A WORLD IN MOTION

Cybersecurity Challenge

SAE International

Acknowledgments

This program is a product of SAE International and supported by contributions to the SAE Foundation, Warrendale, Pennsylvania.

David Schutt, Chief Executive Officer
Mathew M. Miller, Director, SAE Foundation & Pre-College Programs
Christopher M. Ciuca, *A World In Motion* (AWIM) Program Manager

Written and Developed by Education Development Center, Inc.*

Kristen Bjork, Curriculum Developer and Project Director
Kevin Waterman, Curriculum Developer
Kerry Ouellet, Managing Editor
Sophia Mansori, Evaluator
Christopher M. Ciuca, SAE International, AWIM Program Manager

Layout, Design, and Illustrations

Kerry Ouellet, Graphic Designer
Jennifer Davis-Kay, Copyeditor
Lisa Finch, Artist
Michele Shortley, Artist

Other Images

At a Glance icon (glasses) made by Gregar Cresnar from www.flaticon.com

Advisors, Consultants, and Reviewers

Matthew M. Miller, Christopher Ciuca, Julie Nalducci, Kenneth Francis

We would like to thank the following schools and classroom teachers for their participation in the pilot- and field-testing of the curriculum:

Schools

Ashburnham Middle School, Ashburnham, Mass.
Cape Elizabeth Middle School, Cape Elizabeth, Maine
Elizabeth Middle School, Elizabeth, Colo.
Florence Sawyer School, Bolton, Mass.
Indiana Area Junior High, Indiana, Pa.
McLaughlin Middle School, Manchester, N.H.
St. Joseph Academy, Haverhill, Mass.
St. Thomas More School, Centennial, Colo.
Tall Pines STEM Academy, Aiken, S.C.

Classroom Teachers

Yvonne Boyd, Ruth Crowley, Susan Finley, Mary Gasbarro, Kellee McNeill, Katherine Morrison, Lisa Mullins, Stephanie Potito, Hannah Rohner, Rob Stewart

EDC Learning transforms lives.

* Education Development Center, Inc. (EDC), is a global nonprofit organization that develops, delivers, and evaluates innovative programs designed to address challenges in education, health, and economic development.

GM

Development and distribution for the *A World In Motion*® Cybersecurity Challenge has been made possible, in part, through a generous grant from the General Motors Foundation.

Cybersecurity Challenge

Table of Contents

Reproducible masters (RMs) are shown in italics.

OVERVIEW

Introducing *A World in Motion* i
What Is Cybersecurity? ii

INTRODUCING THE UNIT

What Is the Cybersecurity Challenge? iii
Unit Structure iv
Correlation to the Standards vii
Activity Calendar xi
Before You Teach xii
Skills Emphasized in This Unit xiii
Additional Teacher Resources xv

PART I: THE CHALLENGE

1. Introducing the Challenge 1
   RM1: Letter from Jupiter Motors 6
   RM2: Marketing Idea Planner and Checklist 7

PART II: MODELING THE INTERNET

2. Sending a Message: Simulation A 9
3. Different Senders, Different Recipients: Simulations B and C 19
   RM3: Team Reflections on Classroom Internet Model: Simulations B and C 29
4. Testing the Stability of the Model: Simulations D and E 31
   RM4: Team Reflections on Classroom Internet Model: Simulations D and E 41
5. Bringing the Network Together 43
   RM5: Mapping the Path of a Message from Jupiter Motors to a Car 48

PART III: ENCRYPTION

6. Securing Messages: Using a Scytale 49

RM6: Encrypted Message 1 56

7. Securing Messages: Using Cipher Wheels 57

RM7: Secret Messages 65

RM8: Cipher Wheel Template 66

8. Combining Two Methods 67

RM9: Encrypted Message 2 74

PART IV: PRESENTATION

9. Developing Marketing Ideas 75

RM10: Presentation Planner and Checklist 80

RM11: Presentation Rubric 81

10. Presenting Marketing Ideas 83

RM12: Cybersecurity Challenge: Assessment 87

RM13: Cybersecurity Challenge: Assessment Answer Key 88

GLOSSARY 91

OVERVIEW

Introducing *A World in Motion*

Educating Children for Tomorrow's World

To succeed in the society of tomorrow, all children need an education that prepares them to understand and apply concepts in science, technology, engineering, and mathematics (STEM). In addition to becoming literate in these disciplines, students must also learn to solve complex problems, to communicate clearly, to raise and resolve questions, to assimilate information, and to work cooperatively toward common goals.

Today's educators can no longer succeed by presenting students with scientific information and teaching them rote processes. To help students acquire a deep understanding of scientific, technological, engineering, and mathematical phenomena, teachers must provide students with abundant opportunities for direct, hands-on experience with materials and tools. In this way, students become competent and feel confident in their abilities to explore, conjecture, and reason logically, and to gather and manipulate information to arrive at useful knowledge about the world around them. These abilities are nourished and nurtured when school activities grow out of real problem situations, and they are further stimulated and developed through the interactive, cooperative processes of discussing, reading, and writing about direct experiences.

SAE International has developed the *A World in Motion* design challenges as an opportunity for students and teachers to explore STEM.

What Is Cybersecurity?

CYBERSECURITY is the defense of computer systems (including physical hardware, software programs, and data) from attempts to harm, steal, or disrupt them. Common threats include the false acquisition of access to systems (via intercepting over-the-air transmissions, impersonating users, or creating a physical connection within a secure environment) in order to steal information or money or to plant false information, and attacks on networks or machines to cause failure.

Introducing the Unit

What Is the Cybersecurity Challenge?

In this challenge, students deepen their understanding of the architecture of the internet and how it was designed to withstand both physical and electronic attacks. Through modeling, students experience how information moves and its inherent potential to be exposed. Students explore a number of physical models that simulate the movement of information through the internet; they identify problems with each model and test different enhancements to help make the network operate better and faster. They investigate the two basic components of securing data and systems: encryption (changing information from one form to another, especially to hide its meaning), and authentication (proof that something is real, true, or genuine).

After learning about these important attributes of cybersecurity, students work in teams to create marketing materials to inform purchasers of self-driving cars about the important steps implemented by a fictional car company, Jupiter Motors, to keep its car systems safe and secure.

By the end of the unit, students should understand that Jupiter Motors will need to communicate with the driverless cars via the internet for a number of reasons, primarily to perform periodic software updates and to provide map and navigation data. Their final projects will likely focus on these three important aspects of communication via the internet, which must be done securely:

- Critical updates, bug fixes (e.g., fixing a sensor that causes the car to stop running if the sensor is covered by a leaf), and road updates (e.g., changes in speed limits) must be able to get through to the cars quickly and efficiently; hence, the internet needs to be robust.
- The messages received must be authenticated (i.e., the car's onboard computer must be sure that the message came from Jupiter Motors and no one else) so that a hacker cannot introduce bad programming that could cause crashes.

- Any data sent from the car back to Jupiter Motors (e.g., performance information gathered from individual cars, which could contain proprietary secrets, or personal information such as the location of the car) must be kept private.

Unit Structure

Part I: The Challenge

Activity 1 introduces students to the overarching project of the Cybersecurity Challenge.

Part II: Modeling the Internet

Activities 2–4 provide students with hands-on activities that model how information flows through the internet. As each simulation is introduced, students add a small complexity to the model and then adjust how it operates to account for the added feature. Built into each lesson are several runs of the simulation, which allow students to brainstorm how to resolve any issues and test that their solutions work. However, if Part II is taught on successive days, you may not want to run each simulation more than once. Instead, you may find it more efficient to have students test the solution(s) from the previous simulation during the current simulation.

- In Simulation A (Activity 2), students model the general transmission of a message through the internet—how information is split into pieces, transmitted between a chain of computers, and then reassembled at its destination. The concepts of nodes (or routers) and packets are introduced.
- Simulation B (Activity 3) involves multiple messages being transmitted across the network at the same time, which must then be reassembled at one location. The messages need to be distinguished from one another with the inclusion of identifying (header) information on each packet. In this simulation, the header identifies who sent the message and in what order the pieces should be reassembled.
- Simulation C (Activity 3) involves both multiple senders and multiple recipients, emphasizing the need to label each packet not only with information about the sender, but also with information about which recipient is meant to receive it. Some students may have addressed the challenge of Simulation B to include both sender and recipient information on each packet, in which case Simulation C is likely redundant and can be skipped or folded into Simulation B.

- Simulation D (Activity 4) begins testing failures on the internet by shutting down particular nodes and observing how messages continue to flow around outages. Students also reflect on the security of the messages they send, as any node can read any message that's sent (a fact that some students may pick up on during earlier simulations).
- Simulation E (Activity 4) completes the basics of TCP/IP by exploring how systems deal with missing information (if packets are intercepted or otherwise go missing).

The most interesting challenges occur in Simulations D and E, where students model events that can interrupt the flow of information on the internet. These simulations are vital to the overarching project, as they demonstrate how the architecture of the internet leads to its reliability.

The primary connection between these internet simulations and students' Jupiter Motors project is to show how information (including software updates and map data) gets from Jupiter Motors to the self-driving car. Since the operation of each car relies on its ability to communicate with Jupiter Motors, the stability and robustness of the internet is critical.

In Activity 5, students wrap up what they've learned in Activities 2–4 by making a map to show how messages are sent over the internet.

Part III: Encryption

When students model the internet in Part II, they learn that the nodes are able to see messages as they are being transmitted. You can't physically "hide" a message inside an envelope when transmitting it through the internet, since each machine needs to see the information being passed in order to send it along. The only way to overcome this security issue is to encrypt messages before transmitting them. Activities 6–8 address the idea of securing information on the internet. Students explore two different historical methods of encrypting messages.

- Activity 6 explores the scytale, a transposition cipher that was used in ancient Greece. This cipher involves moving letters around in a systematic way that the receiver can reorder if they have the proper tool.
- Activity 7 explores using a Caesar cipher, a substitution cipher used in ancient Rome. This cipher is commonly identified with a decoder ring and involves replacing (substituting) each letter with another one.

- Activity 8 combines the two methods from Activities 6 and 7 to show that while each encrypting method is relatively weak (and fairly easy to crack) on its own, combining the two provides an encrypting that is difficult to decrypt without the keys. Students complete this activity by learning about PKE, the backbone of many advanced security schemes, and the basis for digital signatures—the primary method for ensuring that information transmitted across the internet is authentic.

The activities connect to students' Jupiter Motors project as follows:

- Software updates, map data, and the like are sent from Jupiter Motors to their cars using a digital signature. The cars use this signature to ensure that the information is authentic—it actually came from Jupiter Motors, and it wasn't altered at any point.
- Any information shared between the cars and Jupiter Motors is encrypted, so that no one can intercept it and gain access to it as it is transmitted across the internet.

Part IV: Presentation

In Activity 9, student marketing teams compile all they have learned to create a presentation for potential purchasers of Jupiter Motors' driverless cars. In Activity 10, teams deliver their presentations to the class (and, ideally, invited guests) and complete an assessment to help teachers gauge what students have learned in this challenge.

Correlation to the Standards

Because the Cybersecurity Challenge is inherently interdisciplinary, it addresses content and skills across the curriculum. Objectives for technology, English language arts, and science education are listed here. Correlation of the unit's activities to the standards can be found on the following pages.

Technology Education

- Using models to better understand complex systems
- Demonstrating creative thinking and generating solutions to address challenges
- Creating materials that address the needs of a target audience
- Communicating and working collaboratively using digital media
- Planning and developing a final project
- Using critical-thinking skills

English Language Arts

- Writing convincing claims that are supported by evidence
- Using appropriate vocabulary in written products
- Engaging effectively in discussions
- Posing and responding to questions
- Presenting the work of the team
- Carefully following procedures

Science

- Modeling systems
- Communicating the results of scientific investigation

Standards for Technological Literacy: Content for the Study of Technology
International Technology Education Association (ITEA)

Standards			Activities									
			1	2	3	4	5	6	7	8	9	10
1	Empowered Learner: Students leverage technology to take an active role in choosing, achieving and demonstrating competency in their learning goals, informed by the learning sciences.											
	a	Students articulate and set personal learning goals, develop strategies leveraging technology to achieve them and re ect on the learning process itself to improve learning outcomes.										
	b	Students build networks and customize their learning environments in ways that support the learning process.										
	c	Students use technology to seek feedback that informs and improves their practice and to demonstrate their learning in a variety of ways.										
	d	Students understand the fundamental concepts of technology operations, demonstrate the ability to choose, use and troubleshoot current technologies and are able to transfer their knowledge to explore emerging technologies.		x	x	x	x					
2	Digital Citizen: Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical.											
	a	Students cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world.										
	b	Students engage in positive, safe, legal and ethical behavior when using technology, including social interactions online or when using networked devices.								x		
	c	Students demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property.										
	d	Students manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online.								x		
3	Knowledge Constructor: Students critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts and make meaningful learning experiences for themselves and others.											
	a	Students plan and employ effective research strategies to locate information and other resources for their intellectual or creative pursuits.										
	b	Students evaluate the accuracy, perspective, credibility and relevance of information, media, data or other resources.										
	c	Students curate information from digital resources using a variety of tools and methods to create collections of artifacts that demonstrate meaningful connections or conclusions.										
	d	Students build knowledge by actively exploring real-world issues and problems, developing ideas and theories and pursuing answers and solutions.		x	x	x	x			x	x	x
4	Innovative Designer: Students use a variety of technologies within a design process to identify and solve problems by creating new, useful or imaginative solutions.											
	a	Students know and use a deliberate design process for generating ideas, testing theories, creating innovative artifacts or solving authentic problems.	x	x	x	x						
	b	Students select and use digital tools to plan and manage a design process that considers design constraints and calculated risks.					x				x	
	c	Students develop, test and refine prototypes as part of a cyclical design process.		x	x	x						
	d	Students exhibit a tolerance for ambiguity, perseverance and the capacity to work with open-ended problems.	x	x	x	x	x	x	x	x	x	

Standards for Technological Literacy: Content for the Study of Technology
International Technology Education Association (ITEA)

Standards			Activities									
			1	2	3	4	5	6	7	8	9	10
5	Computational Thinker: Students develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.											
	a	Students formulate problem definitions suited for technology- assisted methods such as data analysis, abstract models and algorithmic thinking in exploring and finding solutions.		x	x	x				x		
	b	Students collect data or identify relevant data sets, use digital tools to analyze them, and represent data in various ways to facilitate problem-solving and decision-making.					x				x	
	c	Students break problems into component parts, extract key information, and develop descriptive models to understand complex systems or facilitate problem-solving.		x	x	x				x		
	d	Students understand how automation works and use algorithmic thinking to develop a sequence of steps to create and test automated solutions.										
6	Creative Communicator: Students communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats and digital media appropriate to their goals.											
	a	Students choose the appropriate platforms and tools for meeting the desired objectives of their creation or communication.									x	
	b	Students create original works or responsibly repurpose or remix digital resources into new creations.									x	x
	c	Students break problems into component parts, extract key information, and develop descriptive models to understand complex systems or facilitate problem-solving.	x	x	x	x					x	x
	d	Students publish or present content that customizes the message and medium for their intended audiences.									x	x
7	Global Collaborator: Students use digital tools to broaden their perspectives and enrich their learning by collaborating with others and working effectively in teams locally and globally.											
	a	Students use digital tools to connect with learners from a variety of backgrounds and cultures, engaging with them in ways that broaden mutual understanding and learning.									x	x
	b	Students use collaborative technologies to work with others, including peers, experts or community members, to examine issues and problems from multiple viewpoints.									x	x
	c	Students contribute constructively to project teams, assuming various roles and responsibilities to work effectively toward a common goal.									x	x
	d	Students explore local and global issues and use collaborative technologies to work with others to investigate solutions.										

Common Core State Standards, Standards for ELA/Literacy (2010)

Standards		Activities									
		1	2	3	4	5	6	7	8	9	10
Writing: Text Types and Purposes											
W.6.1	Write arguments to support claims with clear reasons and relevant evidence.					x				x	x
W.6.1.A	Introduce claim(s) and organize the reasons and evidence clearly.					x				x	x
W.6.1.B	Support claim(s) with clear reasons and relevant evidence, using credible sources and demonstrating an understanding of the topic or text.					x				x	x
W.6.2	Write informative/explanatory texts to examine a topic and convey ideas, concepts, and information through the selection, organization, and analysis of relevant content.					x				x	x
W.6.2.D	Use precise language and domain-specific vocabulary to inform about or explain the topic.					x				x	x
Writing: Production and Distribution of Writing											
W.6.4	Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience.					x				x	x
W.6.5	With some guidance and support from peers and adults, develop and strengthen writing as needed by planning, revising, editing, rewriting, or trying a new approach.					x				x	x
Speaking & Listening: Comprehension and Collaboration											
SL.6.1	Engage effectively in a range of collaborative discussions (one-on-one, in groups, and teacher-led) with diverse partners on grade 6 topics, texts, and issues, building on others' ideas and expressing their own clearly.	x	x	x	x	x	x	x	x	x	x
SL.6.1.B	Follow rules for collegial discussions, set specific goals and deadlines, and define individual roles as needed.	x	x	x	x	x	x	x	x	x	x
SL.6.1.C	Pose and respond to specific questions with elaboration and detail by making comments that contribute to the topic, text, or issue under discussion.	x	x	x	x	x	x	x	x	x	x
Speaking & Listening: Presentation of Knowledge and Ideas											
SL.6.4	Present claims and findings, sequencing ideas logically and using pertinent descriptions, facts, and details to accentuate main ideas or themes; use appropriate eye contact, adequate volume, and clear pronunciation.										x
SL.6.5	Include multimedia components (e.g., graphics, images, music, sound) and visual displays in presentations to clarify information.										x
SL.6.6	Adapt speech to a variety of contexts and tasks, demonstrating command of formal English when indicated or appropriate.										x
Science and Technical Subjects: Key Ideas and Details											
RST.6-8.3	Follow precisely a multistep procedure when carrying out experiments, taking measurements, or performing technical tasks.		x	x	x		x	x	x		

Next Generation Science Standards, NGSS Lead States/Achieve (2013)

Standards		Activities									
		1	2	3	4	5	6	7	8	9	10
MS. Engineering Design											
MS-ETS1-1	Define the criteria and constraints of a design problem with sufficient precision to ensure a successful solution, taking into account relevant scientific principles and potential impacts on people and the natural environment that may limit possible solutions.		x	x		x					
MS-ETS1-4	Develop a model to generate data for iterative testing and modification of a proposed object, tool, or process such that an optimal design can be achieved.		x	x	x						
Science Practices											
Asking Questions	Asking questions and defining problems in 6–8 builds on K–5 experiences and progresses to specifying relationships between variables, and clarifying arguments and models.	x	x	x	x	x	x	x	x	x	x
Developing and Using Models	Modeling in 6–8 builds on K–5 experiences and progresses to developing, using, and revising models to describe, test, and predict more abstract phenomena and design systems.		x	x	x						
Engaging in Argument from Evidence	Engaging in argument from evidence in 6–8 builds on K–5 experiences and progresses to constructing a convincing argument that supports or refutes claims for either explanations or solutions about the natural and designed world(s).	x	x	x	x	x	x	x	x		
Obtaining, Evaluating, and Communicating Information	Obtaining, evaluating, and communicating information in 6–8 builds on K–5 experiences and progresses to evaluating the merit and validity of ideas and methods.	x	x	x	x	x	x	x	x	x	x

Activity Calendar

In most cases, the Cybersecurity Challenge should run between 10 and 12 40-minute sessions. Activity 9 can last from one to four sessions, if you'd like students to have more time to work on their marketing plans in class before presenting them. If you limit presentation times to five minutes, you can likely complete Activity 10 within one session.

Below is a suggestion of how the activities might fall into your school calendar.

Day 1	Day 2	Day 3	Day 4	Day 5	Day 6
Activity 1	Activity 2	Activity 3	Activity 4	Activity 5	Activity 6
Day 7	**Day 8**	**Day 9**	**Day 10**	**Day 11**	**Day 12**
Activity 7	Activity 8	Activity 9	Activity 9	Activity 9	Activity 10

Before You Teach

Activity 2

Give some thought to how you will divide the class into marketing teams of four.[1]

- You can form the teams randomly; however, the resulting groups may lack diversity (i.e., all members have similar backgrounds, experience, and knowledge) and may not comprise a good range of the skills needed for the final project.
- You can allow students to choose with whom they will work, which they generally enjoy doing; however, transitioning "friend" relationships to task-oriented ones can be challenging for some students. This method also doesn't help students learn how to work with people they don't know, and may further isolate those who don't have friendships with or connections to the other students.
- The most successful teams tend to be teacher-formed, with attention given to students' skills, previous experiences, background knowledge, and leadership ability.

Activity 6

- Purchase enough PVC pipes of diameters ½ in., ¾ in., 1 in., and 1¼ in., cut to 12–18 in., for each group of four students to receive one set of each of the four diameters. You can get four 15-in. pieces of pipe from one 5-ft. piece of pipe. Home improvement stores will usually cut the pieces for you.

Activity 10

- Decide whether to invite guests (e.g., other students in the school, an industry volunteer, and/or other teachers) to students' final presentations.
- Decide whether to ask three or four "experts" (teachers or other adults) to make up a panel representing Jupiter Motors. Consider whom to invite, and make arrangements for their participation.
- Arrange to use a gymnasium, a cafeteria, or another large room for students' presentations.

---

[1] Adapted from "Better Group Work Experiences Begin with How the Groups Are Formed" by Maryellen Weimer (*Faculty Focus*, July 31, 2013, http://www.facultyfocus.com/articles/teaching-professor-blog/better-group-work-experiences-begin-with-how-the-groups-are-formed/).

- Borrow or plan to use an overhead LCD projector or document camera so that teams can display their work.
- Decide whether to frame the marketing presentations as a competition. If so,
  - adapt "Presentation Rubric" (Reproducible Master 11) for students to use as a score sheet.
  - choose or create a small prize for the winning marketing team(s).

Skills Emphasized in This Unit

Teamwork

Working as a team gives students a chance to accomplish more than they could as individuals. Throughout the unit, students work in marketing teams of four to discuss what they've observed, come to conclusions, and solve problems. Being able to work well with others—whom students don't know well and those with different backgrounds, experiences, knowledge, and skills—is an important life skill, both in the classroom and in the outside world.

Keeping Records

The importance of keeping detailed records is emphasized throughout the unit. Students are asked to keep records in a number of ways, each of which presents an opportunity for you to assess their learning.

REFLECTIONS: Reproducible Masters 3 and 4 prompt teams with specific questions to answer after they complete each simulation. This helps students reflect on their experiences during the simulations and can also serve as a way to gauge student learning.

SCIENCE NOTEBOOK: Each student should be supplied with a science notebook. It can be a spiral-bound notebook (preferably with pockets), a three-ring binder, or even just a folder. Students should also be provided with a supply of blank or lined paper on which they can write notes and observations and draw diagrams. Although there are many instances during the unit when you will formally ask students to record their thoughts in their notebooks, make it clear that they should add to their notebooks as often as they feel necessary. Students are responsible for bringing their notebooks to each class session. Notebook icons, as shown, appear at locations where opportunities arise for students to write in their notebooks.

TEAM MARKETING RESEARCH PORTFOLIO: Like the science notebook, the team portfolio can take various forms, including a spiral-bound notebook with pockets, three-ring binder, or folder. The team portfolio will be used to store team reproducible masters and any notes and other information they will want to use for their marketing presentations in Activity 10. Teams should be provided with a supply of blank or lined paper. After students share their individual observations with their team, the team will work to find some agreement regarding what they've seen and experienced; a team member will then record this agreed-on information in the team portfolio. You may choose to collect team portfolios after each class period or have students choose a responsible team member to bring it to each class session.

Developing and Using Models

In Activities 2–4, students explore a number of physical models that simulate the movement of information through the internet, thus deepening their understanding of its architecture and how it was designed to withstand both physical and electronic attacks.

In Activity 5, they call on their "classroom internet model" experience to create a map to graphically demonstrate how information flows through the internet.

Problem Solving

After each internet simulation in Activities 2–4, students identify problems with the model, brainstorm how to resolve the issues, test different solutions, and debrief their experiences.

In Activities 6–8, students are challenged with trying to crack the code and decipher messages without keys (or even knowing the encryption method). Many students will struggle when attempting to crack the code, which is a purposeful part of the activity—to show that encryption is made secure primarily by the difficulty of deciphering messages without having a key.

Throughout the unit, students are challenged with the problem of how to translate their growing knowledge of the internet into marketing materials designed to reassure anxious consumers.

Additional Teacher Resources

Teacher Tips

Throughout the unit, you will see sidebars of information called Teacher Tips. Some of these tips were offered by teachers who field-tested the materials; others provide additional information or are items that we think can help ease your way through the activities.

Assessment

Embedded in this unit are opportunities for you to assess student understanding that are marked with check mark icons, as shown. These opportunities range from listening to team discussions to asking students to develop an internet map based on the work they have done so far to their final presentations.

Background Information

As you teach this unit, you might want some additional information for yourself or to share with students about the workings of the internet. Several activities conclude with a Background section offering more information on a specific topic.

Glossary

HIGHLIGHTED VOCABULARY WORDS that appear throughout the unit are defined in the Glossary, which is provided for your convenience. In general, it is not necessary to ensure that students understand or memorize the terms in the glossary—it's more important that students understand the general concepts explored in the activities and can explain them *in their own words.* Use your best judgment as to how explicit you wish to make vocabulary a part of students' projects or any assessment.

Website Resources

During this unit, you are asked to show students a number of video clips. These clips, along with links to additional information on some of the topics covered and demonstrations of how to use some of the materials, can be found on the *A World in Motion* (AWIM) website at

http://awim.sae.org/curriculum/cybersecurity/

1 Introducing the Challenge

Introduction

What Students Do in This Activity

Students are introduced to the overarching project of the Cybersecurity Challenge: developing marketing materials to reassure consumers about major aspects of cybersecurity, including

- how the architecture of the internet safeguards information in case of failure.
- how information is secured—both while stored and while being transmitted through the internet.
- how users are authenticated before access to information or systems is granted.

Students are introduced to science notebooks, in which they can jot down notes and ideas as they need to.

Rationale

This activity sets the context for the work students will do over the course of the unit. Although the challenge comes from a fictional car company, it presents an engaging way for students to see how information is secured over the internet. Students are further motivated by the real-world and hands-on characteristics of this challenge.

The videos suggested during this activity show both real and fictional accounts of hacking and cybersecurity threats. They are intended to punctuate the need for attention to security issues and to motivate student discussion around the problems posed.

ACTIVITY 1 AT A GLANCE

Present the Activity

- Show the cybersecurity video clip(s).
- Discuss depictions of the internet in popular culture.
- Review the "Letter from Jupiter Motors" (Reproducible Master 1).
- Show a video on car-hacking.
- Present Jupiter Motors' concern: Consumers will be afraid to buy self-driving cars.
- Go over the "Marketing Idea Planner and Checklist" (Reproducible Master 2).
- Distribute science notebooks.

During the Activity

- Introduce the Cybersecurity Challenge.
- Students brainstorm and record concerns about cybersecurity.

Share and Interpret

- Discuss what the internet means.
- Go over the next class activity: modeling a "classroom internet."

Reflect and Summarize

- Students share what stood out most from the different video clips they saw.
- Students share their reactions to the Jupiter Motors challenge.

Time

1 class period

Materials

For each student:

- 1 copy of "Letter from Jupiter Motors" (Reproducible Master 1)
- 1 copy of "Marketing Idea Planner and Checklist" (Reproducible Master 2)
- Science notebook

For the teacher:

- Video clips on cybersecurity (see Preparation)
- Video on hacking a smart car (see Preparation)
- Computer with a large-screen monitor or projector
- Whiteboard or chart paper and colored markers

Preparation

- Review the *Introduction to the Unit*.
- Review the video clips on cybersecurity (found on the Activity 1 page of the *A World in Motion* [AWIM] website) to determine which ones are appropriate for your students. Bookmark the clip(s) that you decide to show.

- Bookmark the car-hacking video (found on the Activity 1 page of the AWIM website).
- Arrange for access to a computer with a large-screen monitor or projector on which to show students the videos. Test the equipment before class to ensure adequate volume, playback quality, etc.
- Photocopy Reproducible Masters 1 and 2.

Classroom Activity

Present the Activity

1. **Pique students' interest in the topic by showing the video(s) you chose from the AWIM website.**
2. **Explain that depictions of the internet in popular culture have led many people to fear for the security of their personal information.**

   Tell students that there are legitimate concerns about ensuring that personal and private information is kept secret, and there are many individuals and groups (**HACKERS** and cyber thieves) who are always looking to find illegal access to computers and computer data to use in nefarious ways. However, technology is constantly improving to keep up with these criminals.
3. **Distribute "Letter from Jupiter Motors" (Reproducible Master 1), and have students read it.**

   Jupiter Motors invites students to create marketing materials describing the ways that the company secures all communications related to its self-driving cars.
4. **Discuss the letter with the class.**

   Use some or all of the guiding questions below to spark discussion. Feel free to supplement with your own questions, based on what your students seem especially interested in.

   - What does Jupiter Motors want you to do?
     - Students should recognize that Jupiter Motors wants them to explain the basics of cybersecurity in marketing materials designed to reassure Jupiter Motors' target audience.
   - What requirements does Jupiter Motors have for the presentation?

TEACHER TIP:

Students may not understand why people might be afraid of self-driving cars because today's students are "digital natives," who find such technology exciting. Remind them that Jupiter Motors would also like to sell its cars to people who are less comfortable with (and maybe even slightly afraid of) the latest technology.

The letter mentions the following requirements:

- The presentation should require little prior knowledge.
- It should describe how information flows through the internet.
- It should describe how the architecture of the internet safeguards information in case of failure.
- It should describe how information is kept secure—both where it is stored and while it is being transmitted.
- It should describe how systems decide with whom or what they should share information.

▸ How will we know if the marketing materials are successful?

- Answers will vary, but students should recognize that they must meet all of Jupiter Motors' design criteria in order to be successful.

TEACHER TIP

In the real world, numerous marketing ideas are presented for any particular commercial product, but only one or two are ultimately selected. You can run the presentations as a competition if you think your students would enjoy this.

5. **Distribute "Marketing Idea Planner and Checklist" (Reproducible Master 2) to each student, and have them read it.**

   Explain that this reproducible master will help them keep track of the information they need to gather for their final marketing project.

6. **Show the car-hacking video.**

   Discuss the video, which shows how a smart car can potentially be hacked, as a class.

7. **Explain that Jupiter Motors' executives are very concerned that consumers are seeing similar reports and may, therefore, be afraid to buy Jupiter Motors' self-driving cars.**

8. **Give each student a science notebook. Explain that they will keep notes about the work they are doing in the notebook.**

   Have students add their copies of "Letter from Jupiter Motors" (Reproducible Master 1) and "Marketing Idea Planner and Checklist" (Reproducible Master 2) to their science notebooks. Tell them that they are responsible for bringing their notebooks to each class.

   You can collect students' science notebooks at the end of the unit to assess their progress.

TEACHER TIP

You can help students understand the marketing part of the task by asking them how they would try to convince a parent that they need a new bicycle or should adopt a puppy.

During the Activity

9. Tell students that over the next couple of weeks, they will work in marketing teams to meet the challenge presented by Jupiter Motors. Students will explore the structure of the internet and discover how information is kept safe and private.
10. Ask students, "Based on the videos you watched, what fears do you think people might have about cybersecurity?" Record their responses on a whiteboard or chart paper.

Share and Interpret

11. Discuss with students what they think the **INTERNET** means.
    - What are the parts that make up the internet?
    - How does an email, a Facebook post, or an Instagram photo get delivered from a student's phone to its destination (someone's email inbox, a Facebook newsfeed, an Instagram post)?
    - Can they think of a way that they, as a class, could create a model of how the internet works?

    Give students some time to think, and then ask them to share their ideas with the class.
12. Ask students, "Why is it important that you understand how the internet works before you put together a marketing presentation about a self-driving car?"

    Students should recognize that the car must get information from somewhere about how and where to drive, and that "somewhere" is most likely the internet.
13. Explain that in the next activity, students will model a "classroom internet" to help them understand how information is relayed over the internet and how it can be made more secure.

Reflect and Summarize

14. Ask students what stood out the most from the different video clips they viewed in this session.
15. Ask students to share their reactions to the Jupiter Motors challenge.

    Remind students that they will work in teams to create marketing materials for Jupiter Motors that will help car buyers feel more comfortable and secure about the advances in computerized automotive technologies.

16. Have students note their thoughts in their science notebooks.

Letter from Jupiter Motors

Dear Students:

We need your help! Jupiter Motors, Inc., is developing a new driverless car that will go on the market in the fall of next year. Unfortunately, our user focus groups are expressing some concern about the security of these cars. Because our cars receive information over the internet, potential drivers are afraid that hackers could take over their cars while they are driving, with the intent to sabotage them or drive them off the road.

As super-users of technology, young people have a comfort level and a familiarity with technology that our target market (drivers ages 35–55) does not. That's where you come in!

Our Jupiter Motors marketing team is seeking fresh ideas from young people like you. We need your help to develop marketing materials that will make our target market feel more comfortable about the security of driverless cars.

We suggest that your team takes the following steps to help us:

1. Learn how information moves over the internet.
2. Learn as much as you can about how that information stays safe as it moves over the internet.
3. Think about how you can explain to our intended audience what allows information to stay safe.
4. Decide how you will present your pitch to your audience. You might choose to develop a TV commercial, a website, a podcast, or a series of social media postings (tweets, Instagram posts, etc.). Remember: Choose the medium that you think will work best for the audience you're trying to reach.
5. Make a plan for your marketing materials.
6. Develop your marketing materials, and prepare to present them to an audience.

Your marketing idea should be understandable to someone who has little prior knowledge. It should describe the following:

- How information flows through the internet
- How the internet keeps information flowing in case of failure
- How information is kept secure—both where it is stored and while it is being transmitted
- How systems know what information and data can be trusted

Good luck with your ideas!

I. B. Lock

I. B. Lock
President, Jupiter Motors, Inc.

Reproducible Master 1

Society of Automotive Engineers, Inc. © 2017

Name _____ Date_____

Marketing Idea Planner and Checklist

Use this planner to develop a marketing plan with your team. As you complete each task, put an **X** in the right-hand column to show that this part is ready.

Task	**Ready ☒**
1. Collect all the work you do over the course of the project.	
2. In your science notebook, keep track of any thoughts or ideas you have about how what you've done relates to your Jupiter Motors project.	
3. Make sure that your marketing idea fulfills the following requirements: ▸ Requires little prior knowledge to understand	
▸ Makes people feel safe and secure about Jupiter Motors' self-driving cars	
▸ Is targeted to drivers ages 35–55	
4. Make sure that your marketing idea describes the following to potential customers: ▸ How information flows through the internet	
▸ How the internet keeps information flowing in case of failure	
▸ How information is kept secure—both where it is being stored and while it is being transmitted	
▸ How systems know what information and data can be trusted	

Society of Automotive Engineers, Inc. © 2017

2 Sending a Message

SIMULATION A

Introduction

What Students Do in This Activity

Students model how information flows through the internet and explore how protocols can help resolve issues that intercept or otherwise impact data flow. To help them learn about the internet and how it is secured, students develop a classroom model of the internet in stages (across Activities 2–4) and run many tests to learn how to address the various challenges that arise.

Rationale

The internet was designed to facilitate the flow of information between computers. **TCP (TRANSMISSION CONTROL PROTOCOL)** and **IP (INTERNET PROTOCOL)** are suites of **PROTOCOLS** (rules) that programs use to address and route messages (IP) and to ensure that entire messages are broken into pieces, sent, received, and reassembled (TCP). The hands-on simulations in Activities 2–4 were designed to help students better understand how messages are addressed and routed on the internet and how the internet is able to overcome system failures.

- Simulation A focuses on how information is split into pieces (**PACKETS**), transmitted across **NODES** or **ROUTERS** (any electronic device that serves as a connecting point along routes of internet traffic), and then reassembled at its destination.
- Simulation B demonstrates the need for each packet to contain identifying (**HEADER**) information by adding the challenge of figuring out which packets belong to which message when one individual receives multiple messages that must be reassembled.
- Simulation C emphasizes the need to add additional information to the header of each packet (the identification of both the sender and the recipient) by having students model the transmission of messages from multiple senders to multiple recipients.

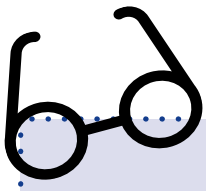
- Simulation D starts testing failures on the internet by shutting down particular nodes and observing how messages continue to flow around outages.
- Simulation E completes the basics of TCP/IP by exploring how systems deal with missing information (if packets are intercepted or otherwise go missing).

The problems presented in the simulations also serve to deepen students' understanding of the complexity of the internet as a whole, and motivate major strands of study presented later in the unit: encryption (Activities 6–8) and authentication (Activity 8).

Connection to the Jupiter Motors Challenge

This activity begins to familiarize students with the different elements of the internet so that they can develop a marketing message that will help Jupiter Motors' customers feel more comfortable about the safety of their self-driving cars.

This simulation explores how information flows from a sender (Jupiter Motors) to a recipient (a self-driving car). It lays the foundation for more varied simulations of information flow over the internet in the following activities.



ACTIVITY 2 AT A GLANCE

Present the Activity

- Review the challenge presented by Jupiter Motors.
- Divide students into marketing teams, and go over their responsibilities in this unit.

During the Activity

- Set up and run Simulation A.
- Have students record their observations.
- (Optional) Repeat the simulation.

Share and Interpret

- Discuss with the whole group how the internet model worked.
- In teams, have students discuss how to address problems in the model.

Reflect and Summarize

- Teams share problems with the simulation that they identified.
- Students reflect on the connection between today's simulation and the Cybersecurity Challenge.

Time

1 class period

Materials

For each student:

- Science notebook

For the "sender":

- 10–15 index cards
- Pen or marker

For each team:

- Team marketing research portfolio
- 1 copy of "Letter from Jupiter Motors" (Reproducible Master 1)
- 1 copy of "Marketing Idea Planner and Checklist (Reproducible Master 2)

For the teacher:

- Chart paper
- Colored markers

Preparation

TEACHER TIP:

You will use this list of rules for the next few activities.

- Determine how you will divide the class into four-person marketing teams. (See *Before You Teach* for more on this.)
- Write the following rules for the simulation on the board or chart paper, and place them where the whole class can see:
  - Each node can hold only one card at a time.
  - Cards should be sent in the general direction of the recipient.
  - No one can move from their spot during the simulation (other than to pass cards, as needed).
- Depending on how organized your students are, you may want to create the messages prior to class. You will need at least two 10- to 15-word messages, with only 1 word per index card.
- Read the Background on TCP/IP at the end of this activity.
- Determine whether or how you will break the class into groups for the simulations.
  - Because the simulations can take a few minutes to complete, and students can become disengaged when they are not involved, the simulations work best when done with groups of 10–15 students.

- If you decide to break the class into groups, make sure that you have enough space for each group to perform the simulation separately.

- Prepare team marketing research portfolios, and include 1 copy each of "Letter from Jupiter Motors" (Reproducible Master 1) and "Marketing Idea Planner and Checklist" (Reproducible Master 2).

Classroom Activity

Present the Activity

1. **Review the request from Jupiter Motors.**
2. **Tell students that they will work in marketing teams throughout this unit. Go over the responsibilities of team members.**

   Make sure students understand that they are each responsible for taking notes on the simulations and activities.

   - Teams will be asked to report to the whole class at certain points.
   - Students will record their individual ideas and reflections and then share them with their team members.
   - Any team member should be able to speak for the whole team, but the team should elect one member to be the primary speaker during each sharing session. (This doesn't need to be the same person each time.)
   - All team members are responsible for knowing what happened during modeling exercises and what conclusions the team reached.
   - All team members will be assessed on their participation in the final project.

During the Activity

3. **Explain that students will make a physical simulation of how a message is sent on the internet.**

   In this simulation, they are sending a message from the person who wrote it to its intended recipient.

4. **Ask students how they think the Jupiter Motors challenge is related to the internet.**

   Prompt students with questions such as the following:

   - Why would the car need to be connected to the internet? *By connecting to the internet, the car can get information*

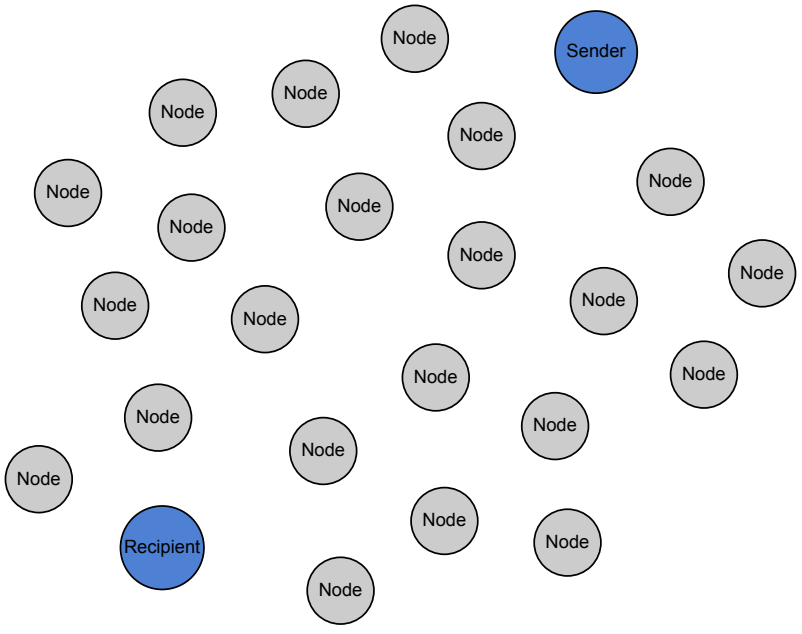
such as software updates, map data, directions, and traffic information. It could also stream music or video.

- What does the car get from Jupiter Motors over the internet?
  The car receives software updates from Jupiter Motors.
- What is a software update? Why do software applications need to be updated?
  A software update is a program, usually free, that provides fixes or new features to an existing application. Applications are updated when programmers need to fix parts of the program that aren't working correctly (bugs), change how the application looks or works, or add new functionality.
- What else might the car get from the internet?
  This question is meant to elicit the idea that the car gets traffic and map information from the internet as well as software updates. If students have no answers, you might ask, "How would the car know where it is?" or "Where does it get its maps and traffic information?" Students might also mention that the car could receive streaming music or audiobook data from the internet.

5. **Set up Simulation A.**

   a. **Select one student to be the "sender" (Jupiter Motors) and one to be the "recipient" (the self-driving car). The rest of the students will be "nodes." The message is a critical software update that needs to get to the car.**

   The diagram below shows one way of arranging students for this exercise.



b. Give the sender the index cards and a pen or marker, and have the sender write a 10- to 15-word message, 1 word per card. (Or, if you prepared the messages in advance, give the sender the prepared cards.)

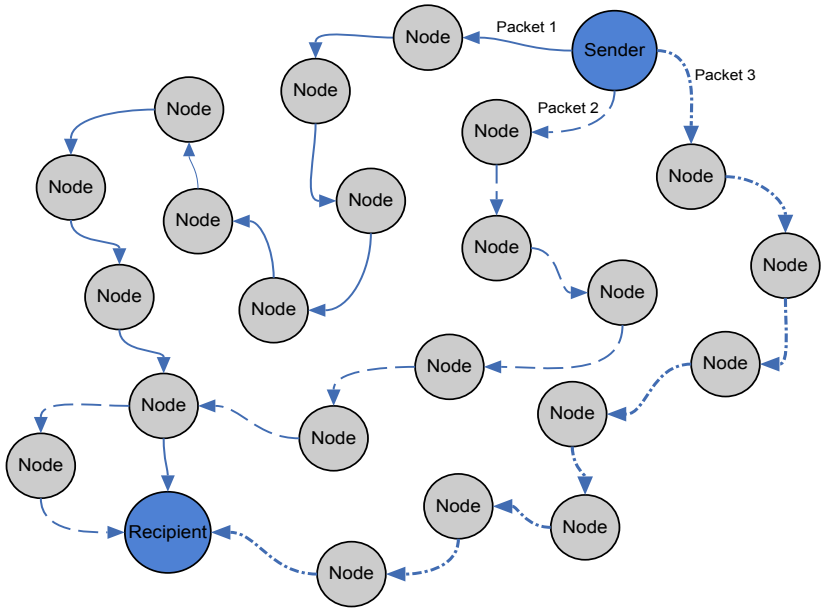
c. Arrange the class as the sender writes the message.

Ideally, have students stand or sit in an open area, positioned randomly, with the sender and recipient along the edge of the group and on opposite ends. The nodes should be between the sender and recipient, more or less evenly spaced.

Try to avoid an arrangement that ends up with an obvious direct path between the sender and recipient. Make sure that there is more than one node within arm's distance of the sender, so the sender can use different paths to transmit the message.

Solution

The diagram below shows a typical path that packets might take during the simulation. Note that students in this diagram aren't arranged in any particular pattern, although the simulation could work fine with students seated at desks arranged in rows provided they're encouraged to mix up how they move packets along.



d. Go over the rules for transmitting messages. Point out where the rules are posted.

6. **Have the sender transmit the message.**

   The sender passes the cards, one at a time, to nearby nodes. The recipient collects the cards, assembles them, and reproduces the message.

7. **Have the recipient read the message aloud.**

   Ask the sender if the message is correct.

8. **Have students record their observations about the simulation in their science notebooks.**

   Ask them to think about and respond to the following questions:

   - How might you make the process of sending messages through your classroom internet better or faster?
   - What problems did you observe or do you predict may happen with the current model?

9. **(Optional) Choose a new sender and recipient, and repeat the simulation.**

10. **Have students record any additional observations in their science notebooks.**

TEACHER TIP:

Repeat the simulation only if you think your students need reinforcement. You also may choose to move directly to Simulation B (Activity 3) before doing the Share and Interpret for Simulation A.

Share and Interpret

11. **Discuss how the classroom internet model worked. Record any problems students note on a piece of chart paper titled "Problems We Identified."**

    Begin by asking the nodes to share their observations, and then ask senders and recipients to contribute. Remind students to keep notes on this discussion in their science notebooks.

SOME COMMON (EXPECTED) RESPONSES:

- All the cards went through the same people. If your class did this, you can add a new rule: Senders and nodes must pass cards to a different node each time.
- The recipient received the cards out of order, and it wasn't easy to reassemble them.
- The recipient wasn't sure when they had received all the cards.
- If none of these responses emerge, don't force them at this point. You will repeat this scenario a number of times in this and the next activity, each time introducing an additional complication, so you need not cover any particular problem exhaustively now or have students come up with the "right" answers.

12. **Have students break into their marketing teams and ask them to write the names of their team members in their science notebooks.**

13. **Introduce and distribute the team marketing research portfolios.**

    Tell students that they will use their team portfolios to collect information about their understanding of the workings of the internet and to record information about their cybersecurity marketing presentation.

14. **Ask teams to discuss how they might address any problems with the "classroom internet model" they have identified.**

    Tell students that sharing their ideas within their teams will allow them to gather the best possible ideas from the whole group.

15. **Circulate and listen in on each team's discussion.**

    Your observations can be a type of embedded assessment. Use the following questions to structure your observations:

    - How are the team members working together?
    - Are they thinking creatively and carefully about how they would alter the design of the simulation to address the problems the class brought up?

Reflect and Summarize

16. **Remind students that the whole class is working together to create the best possible model of the internet.**

    Tell students that scientists and engineers regularly share ideas and experimental data and then use this new information to make further discoveries.

17. **Have each team report on some of the important things they discussed.**

    Add any new responses to the "Problems We Identified" list.

18. **Remind students that they will work in their teams to create marketing materials for Jupiter Motors.**

    Their task is to design materials that will help car buyers feel more comfortable and secure about the advances in computerized automotive technologies. Identifying problems in the transmission of information and brainstorming strategies to address those problems, as they did today, is an important first step in this process.

TEACHER TIP:

Be sure to save the "Problems We Identified" list, as you will use it in the next activity.

19. Have students note any additional thoughts or possible solutions to the problems in their science notebooks.

Background

TCP/IP

TCP/IP, also known as the internet protocol suite, is the set of rules that govern how information moves through the internet. The rules are split into two levels: TCP (transmission control protocol) and IP (internet protocol).

- IP, the lower level, contains the rules that determine what route a message takes. It notes the addresses (not just for the sender and recipient, but of each stop along the way) and determines the best path for messages to take.
- TCP is quality control—it makes sure that the entire message makes it to the destination, puts the message in the right order, and sends requests to the sender if any information is lost along the way.

An important fact to note about TCP/IP is that it deals with public (unprotected) data. The protocols are concerned only with transmitting information, not with securing it. So, packets aren't like envelopes where data sit inside; rather, they are more like postcards, whereby anyone handling the information can read it. Further, the fact that large messages are broken up into smaller pieces to transmit is only done to optimize the transmission (so, for instance, packets can be relayed at the same time, sometimes via different routes), and not as a way to scramble a message, since TCP can easily reassemble the message at any point along the way. For this reason, encryption (changing information from one form to another to hide its meaning) is necessary to encrypt messages and ensure their security during transmission. (Students explore encryption in more detail in Activity 6.)

3 Different Senders, Different Recipients

SIMULATIONS B AND C

Introduction

What Students Do in This Activity

Students build on their model from the previous activity to refine how information flows through the internet. They explore how a recipient receives two messages at the same time, and devise a mechanism for ensuring that the recipient can reassemble the two messages. They continue to refine their model by looking at how multiple messages flow through the internet at the same time—if nodes are handling multiple messages for multiple recipients, they need destination information in order to make sure that messages arrive at the correct recipient.

These simulations add two complexities to the model: how a recipient deals with receiving more than one message at the same time, and how a node passes along messages to two different recipients.

TEACHER TIP:

Depending on the time you have available and the skill level of your class, you may choose to combine the two simulations and address both main goals at once: (1) making sure the recipient receives the multiple messages correctly and (2) making sure the nodes know where and to whom to send each message.

Rationale

Now that teams have successfully completed their first modeling task (simulating the flow of a single message through the internet), they are ready to start to tackle complications of scaling up their model. Simulation B presents a number of problems for students to solve:

- How to provide the recipient with the information needed to distinguish between two separate messages, including how to identify the sender of each message
- How to communicate the order of the parts of a message so the recipient can reassemble it accurately (students may have encountered this issue during Simulation A)
- How to ensure that the entire message has been received

Simulation C, which involves two distinct recipients, adds the following problems:

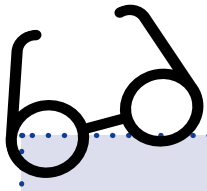
- How a sender can address a message to ensure that it reaches the correct recipient
- How each node can identify the correct destination (recipient) for a packet

The TCP/IP internet protocol suite is the technology that addresses these problems. Each message transmitted through the internet is split into packets, and each packet contains header information, which includes the sender, the recipient, and how the packets fit together so the message may be reassembled. TCP/IP uses this information to find a route from the sender to the recipient, to make sure all the pieces of the message have arrived, and to reassemble the message in the correct order.

Connection to the Jupiter Motors Challenge

The two simulations in this activity help students understand the concept of packets and the fact that each packet needs header information along with the data being sent in order for a message of any size to be sent successfully across the internet.

When Jupiter Motors needs to send information (such as software updates or map data) to a car, Jupiter Motors is the sender and the car is the recipient. Other systems, such as music streaming services, may also be sending information to the car. And both Jupiter Motors and the music service are sending information to multiple cars. Simulation B demonstrates the need for the sender (Jupiter Motors) to identify itself and for pieces of each message to be identified so the computer in the car can put them back together. Simulation C demonstrates the need for the recipient (the car) to be identified, so when Jupiter Motors sends map data, the correct map information gets to the correct car.



ACTIVITY 3 AT A GLANCE

Present the Activity

Review the problems students identified with Simulation A and how the simulation connects to the Jupiter Motors challenge.

During the Activity

- Set up and run Simulation B.
- Have students note their observations in their science notebooks.
- (Optional) Run the simulation again, addressing any problems the students identified.
- Discuss as a class how this classroom internet model worked.
- Introduce the concept of a packet.
- Set up and run Simulation C.

Share and Interpret

- Have students share their notes on the simulation with the class.
- Have teams discuss how to address the problems the class identified and then present their solutions to the class.
- Continue to run Simulation B and/or C until all messages are easily routed and reassembled.

Reflect and Summarize

- In teams, students share their reflections on the simulation.
- Students consider how this activity relates to their overall goal.

TEACHER TIP:

Although teams will compile their responses on just one reproducible master during this activity, students may benefit from having their own copies on which they can follow along with the questions and make notes.

Time

1–2 class periods

Materials

For each student:

- Science notebook

For each team:

- 1 copy of "Team Reflections on Classroom Internet Model: Simulations B and C" (Reproducible Master 3)
- Team marketing research portfolio

For each sender:

- 10–15 index cards
- Pen or marker

For the teacher:

- "Problems We Identified" list from Activity 2
- List of rules for the simulation from Activity 2
- Chart paper
- Colored markers

Preparation

- Display the rules for the simulation where they will be visible to all students:
  - Each node can hold only one card at a time.
  - Cards should be sent in the general direction of the recipient.
  - No one can move from their spot during the simulation (other than to pass cards, as needed).
  - (Optional) Senders and nodes must pass cards to a different node each time.
- Depending on how organized your students are, you may want to create the messages prior to class. You will need at least three 10- to 15-word messages for each simulation, with 1 word per index card.
- Photocopy Reproducible Master 3.

Classroom Activity

Present the Activity

1. **Review the prior activity, including the "Problems We Identified" list, and how the activity connects to the Jupiter Motors challenge.**

   Show students the list. Remind them that this internet simulation is helping them better understand the internet and how it can be secured, which will give them a solid background to create their marketing product for Jupiter Motors. Ask students before the simulation whether they can think of solutions to any of the problems on the list; discuss the solutions and add them to the list, if appropriate.

TEACHER TIP:

These instructions are essentially the same as for Simulation A except that there are now two senders (but still only one recipient).

During the Activity

SIMULATION B: TWO SENDERS, ONE RECIPIENT

2. **Remind students that the self-driving car is receiving information from the internet all the time. Ask students what they think is some of the information that the car might be receiving from the internet.**

   Responses should include much of the following:

   - Software updates from Jupiter Motors
   - GPS data
   - Traffic data
   - Streaming music

3. **Ask students if all of the messages sent to the car will come from Jupiter Motors.**

   Students should recognize that much of the data will come from sources other than Jupiter Motors.

4. **Set up Simulation B.**

   Explain that students will make another physical simulation of how messages are sent on the internet. This time, students will explore how messages sent from two different places (e.g., Jupiter Motors and the traffic data service) get to the self-driving car without getting mixed up.

TEACHER TIP:

Suggest that students mix up the routes of the different cards, making sure that every node gets a chance to pass a card along.

a. **Select two students to be senders (one student will be Jupiter Motors and another will be the traffic data company) and one to be the recipient (the self-driving car). Again, the rest of the students will be nodes.**

   Give the senders the index cards and pens or markers, and have them each write a 10- to 15-word message, 1 word per card. (Or, if you prepared messages in advance, give senders the prepared cards.)

b. **Arrange the class, similar to how they were in Activity 2, as the senders write their messages.**

   The two senders and the recipient should be at the edge of the group, away from one another, with the nodes around and between them, more or less evenly spaced.

   Again, try to avoid an arrangement that ends up with an obvious direct path between the senders and the recipient. Make sure that there is more than one node within arm's distance of each sender so that the senders can easily use different paths to transmit the message.

c. **Remind students of the posted rules for transmitting messages.**

5. **Have the senders transmit their messages.**

   Senders pass their cards, one at a time, to nearby nodes. The recipient collects the cards, assembles them, and reproduces the two messages as best as they can.

6. **Have the recipient read the two messages aloud.**

   Ask the senders if the messages are correct.

TEACHER TIP:

Depending on your class, you may save student reflection time until after Simulation C is completed and have them write about both simulations at the same time.

7. **Have students note their observations of the activity in their science notebooks.**

   Ask them to think about and respond to the following questions:

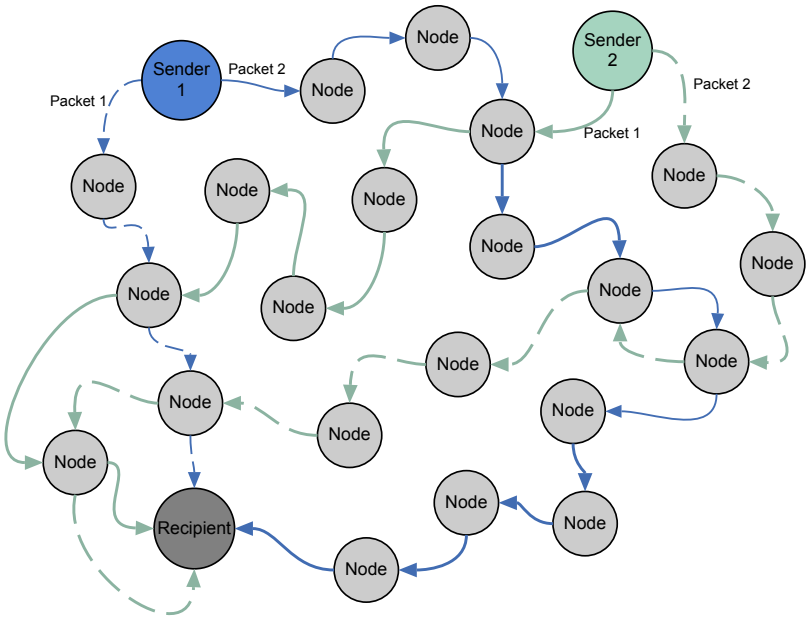
   - What challenges or problems did you discover during the simulation?
   - How might you fix these problems?

8. **(Optional) If students believe they can continue to improve on the model, or if they'd like to test their proposed solutions, choose new students to act as senders and a new student to be the recipient, and repeat the simulation.**

   Again, have students note their observations of the activity in their science notebooks—in particular, how their fixes worked when they tested them.

Solution

The diagram below demonstrates how messages may flow through the classroom internet model. The blue arrows represent two packets (one solid, one dashed) for a message coming from Sender 1, and the two green arrows represent two packets (one solid, one dashed) coming from Sender 2.



9. **Discuss how this new classroom internet model worked.**

Begin by asking the nodes to share their observations, and then ask senders and recipients to contribute. Remind students to keep notes on this discussion in their science notebooks. If you repeated Simulation B, ask students to reflect on the changes they made after the first simulation.

TEACHER TIP:

If none of these responses emerge, don't force them at this point. Future rounds are designed to complicate matters and may prompt responses more directly.

SOME COMMON (EXPECTED) RESPONSES:

- Nodes are able to read the message. This observation exposes the fact that messages are not inherently secure when sent through the internet. While it isn't guaranteed that a particular node will see all pieces of a message, they may see enough sensitive information to compromise security.
- The recipient received the cards out of order, and it wasn't easy to reassemble two mixed-up messages.
- The recipient wasn't sure when they received all the cards for each message.

TEACHER TIP:

Students' solutions should have included some sort of label on each index card indicating both which message the card belonged to and the correct order of the cards in each message. If their solutions include the need to add information about both the sender and the recipient on each packet (the "big reveal" of Simulation C), you may choose to skip this next simulation.

TEACHER TIP:

Some internet simulations use small envelopes to model packets, on which students write the address information and place the message text inside. We avoid this model because it may give the false impression that a message is somehow "protected" or "hidden" by the packet itself. In reality, a packet is more like a postcard than a letter—anyone who touches it can read its information.

10. **Add any problems they note to the "Problems We Identified" list.**
11. **Ask students how they enhanced the design of the model to address these problems.**

    Record students' solutions next to the problems on the list.

SIMULATION C: TWO SENDERS, TWO RECIPIENTS

12. **Introduce the concept of a packet.**

    Tell students that each index card in Simulation C represents a **PACKET**, which is a piece of a message (whether an image, video, file, email—any piece of information sent over the internet), along with information that tells nodes where the message came from, where it's going, and how to reassemble the pieces.

13. **Ask students, "When messages are being sent to the self-driving car, do you think other messages are being sent on the internet?"**

    Students should understand that at any moment, huge numbers of messages are being sent over the internet.

14. **Set up Simulation C.**

    Explain that in this simulation, students will model how two different senders' messages get sent to two different recipients over the internet. In this case, Jupiter Motors (Sender 1) is sending a software update to the car (Recipient 1) while your student's best friend (Sender 2) is sending a video of a grumpy cat to the student (Recipient 2).

    a. **Select two students to be senders and two to be recipients. Again, the rest of the students will be nodes.**

       Give the senders the index cards and pens or markers, and have them each write a 10- to 15-word message, 1 word per card. This time, though, the senders should include additional information—sender, recipient, packet number, and total number of packets—on the back side of each card in their message.

    b. **Arrange the class as the senders write their messages.**

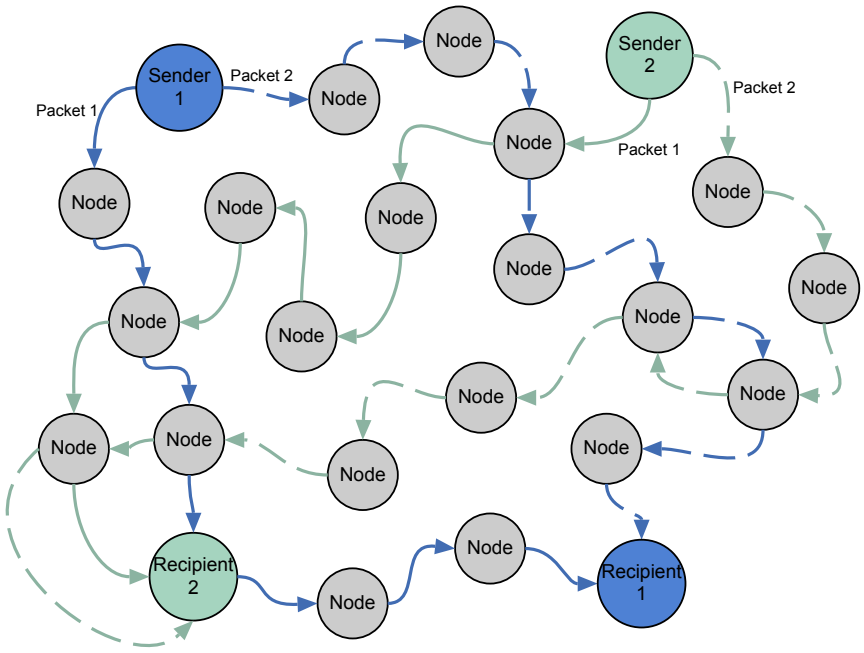
       The nodes should be in the middle, with the senders and recipients evenly spaced around the group.

15. **Have the senders transmit their messages.**

    The senders pass their cards, one at a time, to nearby nodes. The recipients collect the cards, assemble them, and reproduce their message as best they can.

SOLUTION

The diagram below demonstrates how messages may flow through the classroom internet model. The blue sender and recipient represent the software update being sent from Jupiter Motors to the car, and blue arrows show the path of two packets (one solid, one dashed). The green sender and recipient represent the cat video being sent from the best friend to the student, and green arrows show the path of two packets (one solid, one dashed).



16. **Have each recipient read their message aloud.**

    Ask the senders if the messages are correct.

17. **Have students note their observations in their science notebooks.**

    Ask them to think about and respond to the following questions:

    - What challenges or problems did the class have while running the simulation?
    - What changes would you make in order to fix each problem?

18. **(Optional) If you think students would benefit by repeating the scenario to test their proposed fixes, choose new senders and recipients, and repeat the simulation.**

    Have students note their observations of the activity in their science notebooks—in particular, how their fixes worked when they tested them.

TEACHER TIP:

Although not central to this unit, IP addresses could be introduced here as a way for senders to mark their messages. Read the Background on IP addresses at the end of Activity 4 for more information.

19. (Optional) Discuss the second round of the simulation as a class.

    Begin by asking the nodes to share their observations, and then ask senders and recipients to contribute. Remind students to keep notes on this discussion in their science notebooks.

Share and Interpret

20. Ask students to share with the class the problems they noted with Simulation C in their science notebooks.
21. Add the problems they mention to the "Problems We Identified" list.
22. Have students gather in their marketing teams to discuss how they might address these problems.

    Distribute "Team Reflections on Classroom Internet Model: Simulations B and C" (Reproducible Master 3) and team portfolios. Have each team choose a team member to record the main points of the team's discussion on the master..

23. Circulate and listen in on each team's discussion.

    Your observations can be a type of embedded assessment. Use the following questions to structure your observations:

    - How are the team members working together?
    - Are they thinking creatively and carefully about how to alter the simulation to address the problems the class brought up?

TEACHER TIP:

If you've observed that each team has come up with essentially the same solution(s), have a whole-group discussion instead of separate presentations, and point out the minor variations in their solution strategies.

24. When most teams have identified a potential solution for each problem, have each team present its ideas to the whole class.

    Remind students that their larger goal is to create the best possible model of the internet. Point out that although they are working in teams, the purpose of this sharing is to have teams learn from one another so that each team arrives at a working design that gives a consistent performance.

SOME COMMON (EXPECTED) STRATEGIES:

- **Identify the sender on each card.** Senders can write their name or a number on each card, thus ensuring that the recipient can distinguish between the two messages.
- **Number the cards.** This ensures that the recipient can put the words in the proper order.
- **Include the total number of words (cards) in the message.** This ensures that the recipient knows how many cards to expect in each message.

TEACHER TIP:

Keep the "Message Strategies" list, as you may refer to it in the next activity.

25. Record students' strategies on chart paper titled "Message Strategies."
26. To test the proposed enhancements, choose new senders and recipients and repeat Simulation B and/or C, applying the suggested design changes.

    Have students continue to refine the design and repeat the simulations until all messages are easily routed and reassembled. Remind students to note their observations in their science notebooks.

Reflect and Summarize

27. Have team members share their individual reflections from their science notebooks with the rest of their team.

    Have teams choose one team member to record the main points of the team's discussion on Reproducible Master 3. The recorder should place the completed worksheet in their team portfolio.

28. Remind students of how this activity relates to their overall goal.

    Simulating how information flows on the internet helps students better see which parts of the process are open to spying or attack. This will aid them in their task of creating marketing materials for Jupiter Motors that can help car buyers feel more comfortable and secure about the advances in computerized automotive technologies. Continuing to identify problems, brainstorm strategies, and refine their process is an important step in this process.

Name _____ Date_____

Team Reflections on Classroom Internet Model

Simulations B and C

Answer the following questions:

1. How would you explain what a node is to someone who does not understand networks?

2. What challenges or problems did you discover while running the simulations?

3. How might you fix these problems? How did the fixes work when you tested them?

4. Describe how Jupiter Motors would send a software update to a car.

Society of Automotive Engineers, Inc. © 2017

4 Testing the Stability of the Model

SIMULATIONS D AND E

Introduction

What Students Do in This Activity

In Simulations D and E, students test the stability of their network as individual or groups of nodes are identified as "bad." These simulations are important in that they demonstrate the **RELIABILITY** of the internet's architecture: If certain nodes get overwhelmed or are faulty, messages can be rerouted and still continue to flow.

In Simulation D, nodes are turned off and refuse to accept packets, so students must reroute their messages around the bad nodes. Typically, students solve this problem by simply handing packets to another node.

In Simulation E, nodes accept packets but don't send them along. The solution to this problem is less obvious, and students brainstorm possible solutions for dealing with the problem.

Rationale

When designing systems, most engineers start by designing for success: They review their requirements and their goals, and then make sure that each is achieved. The next step, one that is critical for addressing issues of security, is to test and design for failure. This activity introduces situations where parts of the system do not work as designed, and exemplifies how a good design is prepared to handle these less than ideal situations.

Simulation D shows how the architecture of the internet, with its web-like connections between nodes, allows messages to reach their destinations via multiple routes. Should a particular node go offline (via power outage, overloading of messages, or even a hacker attack), packets can find a new route to make it to their destination. This rerouting is a vital activity of the IP part of TCP/IP.

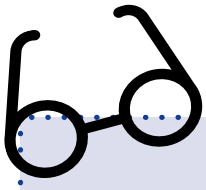
Simulation E has an important distinction from Simulation D in that it tests how the recipient deals with missing information. As stated above,

the solution is less obvious—it isn't "baked in" to the architecture but is an additional feature that needs to be added. The TCP part of TCP/IP deals with this problem by identifying each packet in a message and, upon determining that packets are missing after a specific period of time, requesting that those packets be re-sent.

Connection to the Jupiter Motors Challenge

The two simulations in this activity help students understand how the internet was developed to allow for information to be transmitted even when parts of the internet are not functioning. Because computers are connected in multiple ways, there are a large number of paths that information can follow to get from the sender to the recipient.

When Jupiter Motors needs to send information (such as software updates or map data) to a car, it is vital that the information arrive in a timely manner. If one path is slow or broken (Simulation D), IP will seek a new path to send the packets so they aren't delayed and cause problems. If pieces of a message are missing (Simulation E), TCP will request that it be re-sent so the complete message gets through.



ACTIVITY 4 AT A GLANCE

Present the Activity

- (Optional) Review the prior activities.
- Introduce today's activities as simulations that demonstrate the strength of the internet.
- Remind students of how these simulations relate to their larger goal.

During the Activity

- Set up and run Simulation D, incorporating "bad" nodes into the exercise.
- Have students note their observations in their science notebooks.
- (Optional) Run the simulation again.
- Set up and run Simulation E.

Share and Interpret

- Discuss both simulations as a class, and have students identify any problems they noted.
- Have students work in their teams to identify solutions to these problems and then present their solutions to the class.
- (Optional) Continue to run Simulation E until all messages are easily routed and reassembled.

Reflect and Summarize

- In teams, students share their reflections on the simulation.
- Students consider how this activity relates to their marketing presentations.

Time

1 class period

Materials

For each student:

- Science notebook

For each team:

- 1 copy of "Team Reflections on Classroom Internet Model: Simulations D and E" (Reproducible Master 4)
- Team marketing research portfolio

For each sender:

- 20–30 index cards
- Pen or marker

For the teacher:

- (Optional) "Problems We Identified" list from Activity 3
- (Optional) "Message Strategies" list from Activity 3
- List of rules for simulations
- Chart paper or whiteboard
- Markers

TEACHER TIP:

Although teams will compile their responses on just one reproducible master during this activity, students may benefit from having their own copies on which they can follow along with the questions and make notes.

Preparation

- Display the rules for the simulation where they will be visible to all students:
  - Each node can hold only one card at a time.
  - Cards should be sent in the general direction of the recipient.
  - No one can move from their spot during the simulation (other than to pass cards, as needed).
  - (Optional) Senders and nodes must pass cards to a different node each time.
- For Simulation D, depending on how organized your students are, you may want to create the messages prior to class. You will need at least four 10- to 15-word messages, with 1 word per index card.
- For Simulation E, have the senders create their own messages. When a bad node "swallows" a packet, the recipient will need to ask the sender to rewrite and resend it. Giving the sender multiple copies ahead of time eliminates the "discovery" aspect of this exercise.

TEACHER TIP:

The simulation may evoke more discussion if the "bad" nodes are kept secret. For that reason, using an identifying characteristic, such as hair color or clothing, to choose bad nodes is not the best method since students will be able to identify bad nodes and actively avoid them at the start of the activity.

- Determine a method for identifying bad nodes. You can choose the bad nodes in a number of ways, depending on the size and makeup of your class. You want roughly one-quarter of the nodes to be bad, and it's best to have them dispersed among the group.

  Here are a few ideas for how to identify bad nodes:

  - Randomly distribute cards, some of which are blank and some of which identify bad nodes.
  - If your class is familiar with IP addresses, you can secretly assign a different one to each student. Have several begin with the same first one or two numbers (such as "12.34.xx.xx," which would put them in the same **SUBNET**), and inform those students that they are "bad" nodes. To prepare for multiple runs of the scenario, you may want to clump IP addresses into just three or four subnets.
- Read the Background on IP addresses at the end of this activity.
- Photocopy Reproducible Master 4.

Classroom Activity

Present the Activity

1. **(Optional) Review the prior activities.**

   Remind students that in Activities 2 and 3, they built up their classroom model of the internet, simulating the transmission of messages. As more than one message was sent simultaneously, new features were required to keep the messages from becoming garbled. Review the "Problems We Identified" and "Message Strategies" lists created in the prior activities.

2. **Introduce this activity as a simulation that demonstrates the strength of the internet.**

   Tell students that the internet was specifically designed to be robust (i.e., able to withstand various types of failures). No one central machine is needed to run the internet. The tasks are distributed across a large number of nodes; even if many nodes go down, the internet continues to operate. And if pieces of information go missing, recipients have a mechanism for requesting those pieces to be re-sent.

Today, students will look at two ways that message transmission can be disrupted and how protocols make sure that messages continue to flow.

3. **Remind students of how this activity relates to their larger goal.**

   Continuing to explore the architecture of the internet will help students develop marketing materials for Jupiter Motors. The more familiar they are with the internet, the more able they will be to put customers at ease with this new technology.

During the Activity

SIMULATION D: BAD NODES

4. **Ask students, "Do you think that the speed with which information gets to the car matters? Why or why not?"**

   Students should be able to identify that software updates that fix critical flaws in the car's software will need to get to the car quickly. They should also recognize that traffic and map data are critical.

5. **Set up Simulation D.**

   Explain that this simulation introduces the idea of nodes that are not working. In this simulation, the car (Recipient 1) has requested traffic data from a well-known search engine (Sender 1), while your student's friend (Sender 2) is sending your student (Recipient 2) a different video (this time it is a puppy wearing a sweater). Unfortunately, some of the internet is not working properly.

   a. **Select two students to be senders and two to be recipients. The rest of the students will be nodes.**

      Give the senders the index cards and pens or markers, and have them each write a 10- to 15-word message, 1 word per card. (Or, if you prepared messages in advance, give the senders the prepared cards.) On the back side of each card in their message, have the senders include the name of the recipient, the packet number, and the total number of packets.

   b. As the senders write their messages, arrange the rest of the class.

      The nodes should be in the middle, with the senders and recipients evenly spaced around the group.

   c. **Remind students of the posted rules for transmitting messages.**

6. **Use the method you determined to choose students to be bad nodes.**

   Roughly one-quarter of the students should be bad nodes.

   (Optional) Challenge the bad nodes to keep their identities secret as long as they can.

7. **Add the following to the posted rules for transmitting messages:**
   - Bad nodes cannot touch any cards.
   - Messages cannot be given to a bad node.

8. **Have the senders transmit their messages.**

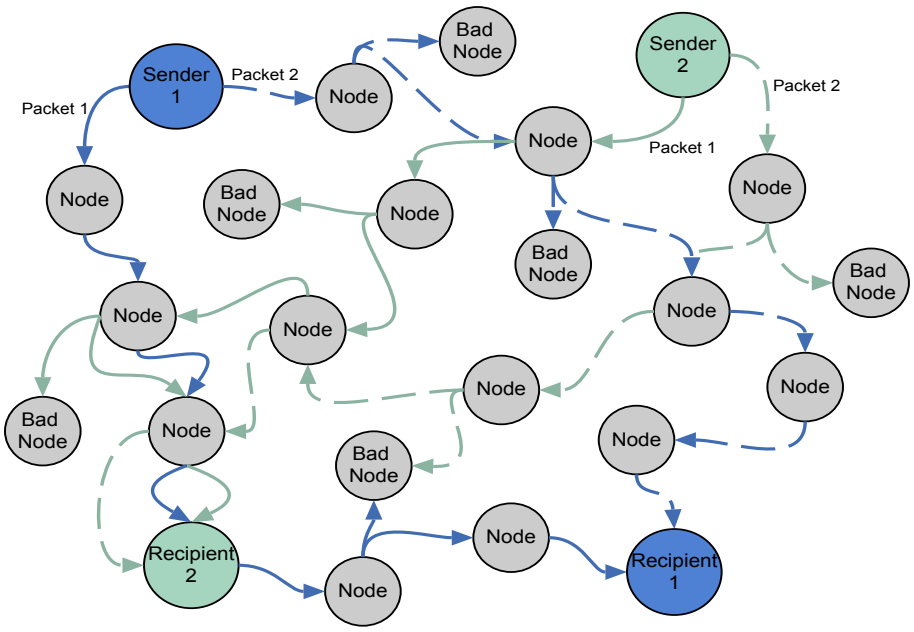
   Senders pass their cards, one at a time, to nearby nodes.

SOLUTION

The diagram below demonstrates how messages may flow through the classroom internet model. When a packet meets a bad node, it is sent again to a nearby node (so two matching lines come out of a single node).

The blue sender and recipient represent the traffic data being sent from Jupiter Motors to the car, and blue arrows show the path of two packets (one solid, one dashed).

The green sender and recipient represent the puppy video being sent from the best friend to the student, and green arrows show the path of two packets (one solid, one dashed).



9. **Remind bad nodes to refuse to accept any cards.**

   Students attempting to pass a card to a bad node must find another node to give the card to.

10. **Have recipients collect their cards, assemble them, reproduce their messages, and read them aloud to the class.**

    Ask the senders if the messages are correct.

11. **Have students note their observations in their science notebooks.**

    Ask them to answer the following:

    - How can you be sure that a software update gets to Jupiter Motors' self-driving car?
    - When parts of the internet fail, how does the internet deal with it?

12. **(Optional) Choose new senders, recipients, and bad nodes, and repeat the simulation.**

    Have students continue to refine the design and repeat the simulation until the messages are easily routed and reassembled.

TEACHER TIP:

You should not expect that students can answer these questions in detail yet.

SIMULATION E: LOST PACKETS

13. **Explain that in this simulation, as with Simulation D, the car (Recipient 1) has requested traffic data from the search engine (Sender 1), while your student's friend (Sender 2) is sending another puppy video to your student (Recipient 2). But this time, the bad nodes are damaged in a different way: They now destroy any packets they come in contact with.**

14. **Set up Simulation E.**

    The setup for this simulation is the same as for Simulation D.

15. **Change the posted rules for bad nodes.**

    Previously, bad nodes could not touch any cards, and senders could not give messages to a bad node. *Replace that rule with the following:*

    - Bad nodes can accept cards but cannot pass them along—they hide any cards they are given.

16. **Have the senders transmit their messages.**

    (Optional) Challenge the bad nodes to keep their identities secret as long as they can.

17. **Ask if either recipient received a complete message. If so, have recipients read their messages aloud to the class.**

    Ask the senders if the messages are correct.

TEACHER TIP:

In most cases, and by design of this simulation, recipients will not receive complete messages, causing students to be confused and not know how to proceed.

Share and Interpret

18. **Discuss both simulations as a class, and have students name the problems that occurred. List their problems on the board or chart paper.**

    Recipients will likely note that packets went missing, but they didn't know how to retrieve them. The challenge is to determine ways for the recipient to request that the sender resend missing cards.

19. **Ask the nodes (including the bad nodes) to share their observations, and then ask senders and recipients to contribute.**

    At this point, a good number of (if not all) students in the class should have had some experience with transmitting cards. Ask them to describe what is going on, what each node is doing, and what they're thinking as they transmit the messages.

20. **Have students record their observations of the activity in their science notebooks.**

21. **Have students work in their marketing teams to brainstorm possible solutions to the problems the class identified.**

SOME COMMON (EXPECTED) RESPONSES:

- Ask the sender to send the packet again. Some students will go "outside the model" and holler across the room to the sender.
- Have the recipient send a packet back to the sender, requesting them to resend the missing packet. That's a mouthful, but it is the most important solution here. Even though in these scenarios, students have been assigned the official titles of "sender" and "recipient," they are not bound to those roles: Any node, including the sender and recipient, can play "sender" or "recipient" in a communication. Using the same method of message exchange, anyone can send a message to the original sender asking that a particular packet be re-sent.
- Some students may note other inefficiencies in the process and will want to brainstorm how to make sure messages flow more easily to avoid bottlenecks.

22. **Circulate and listen in on each team's discussion.**

    Your observations can be a type of embedded assessment. Use the following questions to structure your observations:

    - How are the team members working together?
    - Are they thinking creatively and carefully about how they would alter the design of the simulation to address the problems the class brought up?

TEACHER TIP:

Students may have a hard time resolving the problem presented in Simulation E. Depending on the teams' progress, you may want them to continue to work on resolving the problem, or you may direct them toward the solution: the recipient sends a message back to the original sender requesting that the packet be re-sent.

23. **When most teams have identified a potential solution for each problem, have them present their ideas to the whole class.**

24. **Record students' solution strategies on the board or chart paper.**

    Point out that although they are working in teams, the purpose of this sharing is to have teams learn from one another so that each team arrives at a working design that gives a consistent performance.

25. **(Optional) Choose new senders, recipients, and bad nodes, and repeat Simulation E, applying the suggested design changes.**

    Have students continue to refine the design and repeat the simulation until all messages are routed and reassembled easily.

Reflect and Summarize

26. **Encourage teams to reflect on the revised model.**

    Distribute "Team Reflections on Classroom Internet Model: Simulations D and E" (Reproducible Master 4) and team portfolios. Ask teams to consider how their enhancements throughout the various simulations contributed to the stability of their classroom internet. Have teams choose one team member to record the main points of the team's discussion on Reproducible Master 4. The recorders should place their teams' completed worksheets in their team portfolios.

27. **Note the connections between this activity and the students' marketing presentations.**

    Encourage students to think about how they would present this information as part of their final reports. Have students note their thoughts in their science notebooks.

Background

IP Addresses

An **IP ADDRESS** is a series of four numbers from 1 to 255, separated by periods (e.g., the IP address for google.com is 216.58.217.78). "Google.com" is the **DOMAIN** (or **DOMAIN NAME**); the internet maps domain names to IP addresses using a **DOMAIN NAME SERVER** (a directory of domain names, like an internet address book).

Each domain name ends with a suffix (e.g., ".edu," ".us") called a **TOP-LEVEL DOMAIN**. Historically, top-level domains were three letters long and restricted to a very short list, with the most common being .com, .net, .edu, and .gov. They were meant to identify the type of entity that owned the domain. Other top-level domains included two-letter country codes, such as .uk, .ca, and .us. Top-level domains can be individually governed by bodies that control who can create a domain using that suffix. Recently, the list has expanded to include a great variety of top-level domains of various lengths.

IP addresses are not assigned randomly. Certain companies and internet providers (e.g., Comcast and Verizon) "own" all IP addresses within particular subnets. A SUBNET is a collection of IP addresses that have the same first one, two, or three numbers (e.g., 24.x.x.x or 8.12.172.x).

One type of breach in network security that relates to IP addresses is a DoS attack, where hackers bombard common domain name servers and disrupt communication to them. Since messages and requests sent to a domain address (e.g., "Netflix.com") need to be converted into an IP address for the messages to be sent and received, and if a domain name server cannot be reached, the domain cannot be converted to an IP address and the message cannot be sent.

Name _____ Date_____

Team Reflections on Classroom Internet Model

Simulations D and E

Answer the following questions:

1. How can you be sure that a message gets to its intended recipient intact?

2. Describe how the internet is designed so that when Jupiter Motors needs to send map data to a car, it can be sure the message will get there.

Society of Automotive Engineers, Inc. © 2017

5 Bringing the Network Together

Introduction

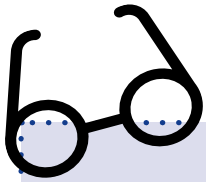
What Students Do in This Activity

Students develop a map that represents what they've learned thus far. They discuss how what they have learned about sending messages via the internet helps them better understand its architecture, and how this understanding impacts their work on the Jupiter Motors marketing materials project.

This activity is a good opportunity to assess student's understanding of how information flows on the internet.

Rationale

Mapping how information is transmitted across the internet helps students more fully understand how information on the internet can be kept secure.



ACTIVITY 5 AT A GLANCE

Present the Activity:

Discuss what students remember about internet Simulations A–E and how these activities relate to their overall goal.

During the Activity:

- Show the video on internet reliability.
- Have teams create a map of how information moves across the internet.

Share and Interpret:

- Have teams share their maps with the class.
- Discuss the similarities and differences between the teams' maps.
- (Optional) Give teams time to revise their maps.

Reflect and Summarize:

Students consider how the internet might be insecure, based on what they've learned so far.

Connection to the Jupiter Motors Challenge

Students integrate what they have learned in the simulations in the previous activities into a map of how information (e.g., a software update) travels from Jupiter Motors to a car over the internet.

Time

1 class period

Materials

For each team:

- 1 copy of "Mapping the Path of a Message from Jupiter Motors to a Car" (Reproducible Master 5)
- Chart paper
- Pencils
- Markers

For the teacher:

- Video on internet reliability (see Preparation)
- Computer with a large-screen monitor or projector
- Chart paper
- Markers

Preparation

- Bookmark the video link for this activity from the Activity 5 page of the AWIM website.
- Arrange for access to a computer with a large-screen monitor or projector on which to show the video. Test the equipment before class to ensure adequate volume, playback quality, etc.
- Photocopy Reproducible Master 5.

Classroom Activity

Present the Activity

1. **As a class, discuss what students recall of the five internet simulations they engaged in.**

   Ask students to share examples of how the internet modeling they have undertaken has helped them better understand how the internet works.

QUICK REVIEW:

In Activities 2–4, students built a model of the internet, simulating how messages flow across the internet. As they made the model more complex, additional features were added to make sure all messages arrived intact:

- Having different senders and recipients prompted students to include sender and recipient information ("From" and "To") in the header.
- Having multiple messages flowing at the same time prompted students to identify different messages and number each packet in order to let the recipient know how to reassemble each message.
- Sending multiple messages also prompted students to include, on each packet, the total number of packets in the message so the recipient can determine whether the message is complete.
- Simulating two ways that nodes could fail demonstrated how the protocols make sure messages continue to flow across the internet and arrive completely.

2. **Remind students of how these activities relate to their larger goal.**

   Familiarity with how the internet works will help them develop marketing materials for Jupiter Motors that put their customers at ease with this new technology.

During the Activity

3. **Show the video clip.**

   The video summarizes what they've learned thus far and will help them with the next task.

4. **Have students get into their marketing teams.**

   Hand out the team portfolios, and then distribute "Mapping the Path of a Message from Jupiter Motors to a Car" (Reproducible Master 5), pencils, markers, and a large piece of chart paper to each team.

5. **Tell students that their task is to create maps that address the question "How does a message get from Jupiter Motors to one of its self-driving cars?"**

Teams will do the following:

a. Work together to develop rough drafts of a map that shows how a message gets from Jupiter Motors to a self-driving car over the internet.

b. Revise and finalize their maps.

c. Prepare to present it to the class.

6. **Circulate among teams as they work.**

   Remind any teams that are having trouble creating a list and/or putting together their maps to consult their science notebooks and team portfolios. If teams continue to struggle, suggest that they think about each simulation they did as a class and what they learned about senders, recipients, packets, lost packets, headers, nodes, and bad nodes.

Share and Interpret

7. **Have teams share and explain their maps.**
8. **After all teams have shared, discuss the similarities and differences between teams' maps.**
9. **(Optional) If any teams would like to revise their maps, give them time to do so.**

Reflect and Summarize

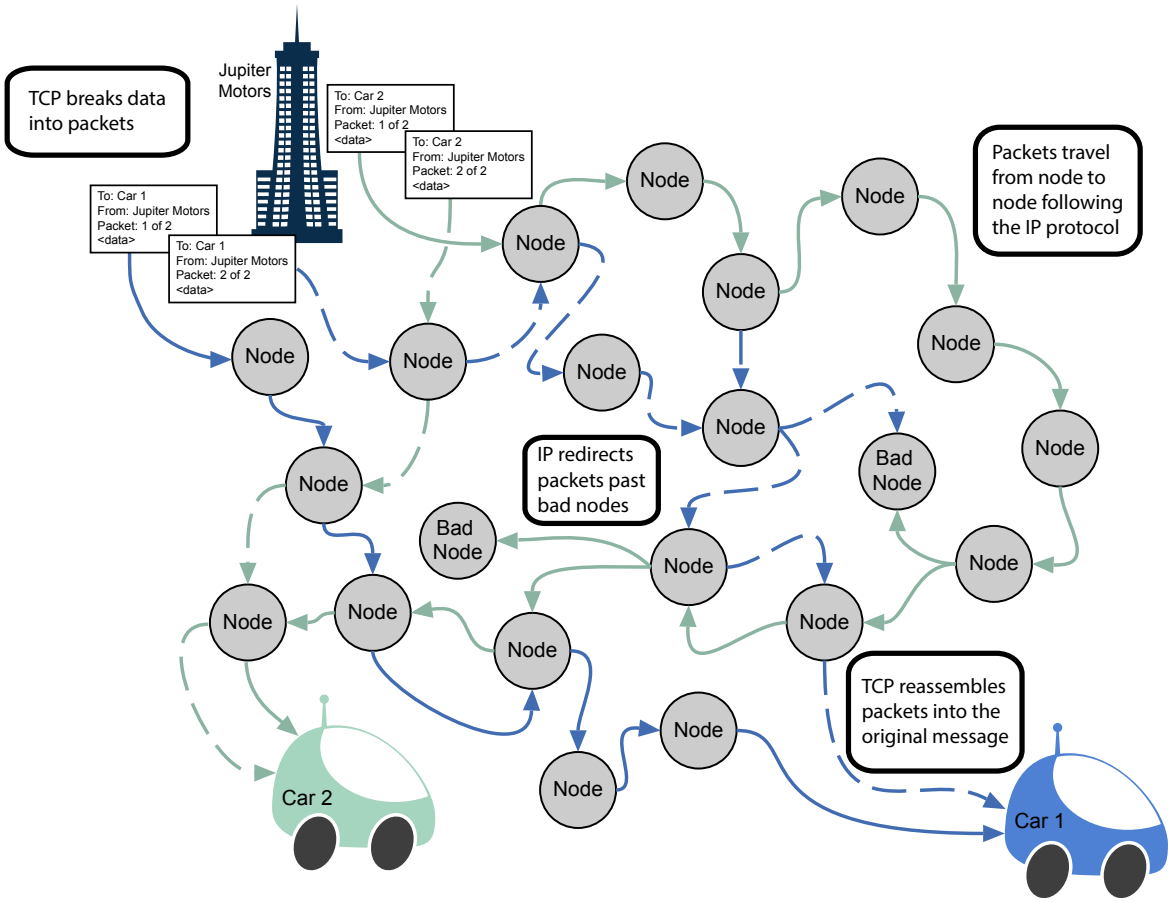
10. **Ask students to think about how the internet might be insecure based on what they've learned so far. Ask, "Where and how easily could information on the internet be intercepted?" Write this question at the top of a piece of chart paper.**
11. **Have students note their thoughts in their science notebooks.**

12. **Have students share their thoughts, and record them on the chart paper.**

    Students should note that while they've learned how the internet can continue to transmit data even if portions of it are non-operational, they have not yet learned about how the information of the internet remains secure. Post this list in the classroom so students can refer to it later.

SOLUTION

This diagram represents one possible map:



Name _____ Date _____

Mapping the Path of a Message from Jupiter Motors to a Car

Create a map that answers the question, "How does a message get from Jupiter Motors to one of its cars?" Draw a rough draft of your map, making sure it accounts for the following:

- The sender (Jupiter Motors)
- The recipient (the car)
- The possible paths a message could take and the parts of that path
- Ways that your message could "go wrong" and how problems are solved

Once you've created your rough draft, talk over the map with your teammates. Make sure you've accounted for everything you've learned about how messages are sent on the internet. Revise and finalize your map, and then draw it on chart paper.

Prepare to present your map to the class.

Society of Automotive Engineers, Inc. © 2017

6 Securing Messages: Using a Scytale

Introduction

What Students Do in This Activity

In Activities 6–8, students explore various methods for encrypting and decrypting messages while learning about how internet messages are made secure. In this activity, they explore a relatively simple method that ancient Greeks used to encrypt their messages called a **SCYTALE** (pronounced "skittle-ee").

Students explore the idea of encryption and learn about **KEYS** (information that details how to decrypt encrypted messages). They discuss how understanding encryption in general can help them complete their Jupiter Motors project.

TEACHER TIP:

Many students may struggle with Activities 6–8. Though it can be difficult, the struggle is part of the learning process, specifically giving students important experience with problem solving and collaborating within a team.

Rationale

Throughout the previous activities, students should have noticed that the information they sent via nodes was not private, as any node could read the messages it passed along. You can't physically "hide" a message inside an envelope when transmitting it through the internet, since each computer needs to see the information being passed in order to send it along. If the message contains sensitive information, such as a password or bank account number, others would be able to read (and thus steal) it. Once students recognize that the architecture of the internet exposes all messages to a large number of potential criminals, the need to hide those messages becomes apparent. The only way to overcome this security issue is to encrypt messages before transmitting them.

Most computer information is hidden by passing it through a set of instructions that alter the messages to make them unreadable. The process of encoding messages in order to keep them secret is called encryption. The instructions include a key that allows the message to be decrypted easily. How difficult it is to crack the code and decrypt a message without that key depends on the encryption method chosen. In Part III, students play with a few simple encryption schemes (or **CIPHERS**).

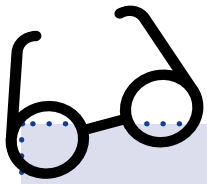
TEACHER TIP:

This activity introduces the general concept of encrypting messages; it does not, however, necessarily represent how messages are encrypted today. Assure students that encryption protocols have advanced rapidly in the internet era!

It's also important for students to understand that no encryption method is entirely secure. Any cipher can be cracked eventually. The goal is to make it take a very, very long time to crack a cipher—so long, in fact, that by the time a message can be read, it is no longer relevant nor needs to be kept secret.

The activities in Part III are structured in a particular way to reinforce that ciphers—even simple ones—take time to decipher when the details of the encryption method are unknown. For both encryption methods, students are asked to decipher messages without having any idea about how they were encrypted. Next, students are shown the basic encryption method while the key remains hidden. Finally, students are given the key (unless they successfully cracked it on their own). This sequence helps to show how the components of encryption—the method in general and the keys that determine the specific cipher—combine to secure messages.

This activity focuses on the scytale, a device that allowed the ancient Greeks to create and send **TRANSPOSITION CIPHERS,** in which letters from the source message are rearranged in a particular pattern (transposed), but each letter keeps its identity (for instance, a "K" still represents a "K"). It is the oldest known ciphering method, primarily used to relay military information.



ACTIVITY 6 AT A GLANCE

Present the Activity:

- Remind students of their overarching task.
- Discuss the security of the messages that were exchanged during internet Simulations A–E.

During the Activity:

- Have students work in their teams to decipher an encrypted message.
- Discuss their observations as a class.
- Give each team a set of scytales, and ask them to document their process in their team portfolios as they work to decipher the message.
- Have teams report their results to the class.
- Have teams encrypt their own messages and then exchange them with other teams.

Share and Interpret:

Discuss this encryption method as a class.

Reflect and Summarize:

Students consider how encryption relates to keeping messages safe on the internet.

TEACHER TIP:

Encode and encrypt have essentially the same definition: "to convert into a coded form." Encrypt more commonly describes codes that are used to keep data confidential, relying on keys to decrypt the data. Encode more broadly refers to coding schemes that maintain usability of the data, and are typically used to change text so that it's easier to transmit or store (e.g., alphabetic characters are encoded as strings of binary digits).

TEACHER TIP:

Code and cipher are synonyms; both mean "a secret or disguised way of writing." In computer science, cipher is most commonly used to describe the type of codes explored in these activities, as the term code has a variety of different uses.

Connection to the Jupiter Motors Challenge

This activity introduces the idea of encrypting messages. While a transposition cipher is uncommon for most computer security, it is historically one of the first methods people used for securing messages, and provides a basic understanding of the concepts of encrypting, decrypting, and keys.

When Jupiter Motors communicates with cars, it is important that the information is secure. If data being sent to the car are intercepted and manipulated, the information could be tainted; incorrect instructions could then be given to the car, causing it to do something unsafe (e.g., drive the wrong way down a one-way street). Understanding the basics of **CRYPTOGRAPHY** can help students assure car owners that their personal information is secure and that they can rely on information they get from Jupiter Motors.

Time

1 class period

Materials

For each student:

- Science notebook

For each team:

- 1 set of four scytales (see Preparation)
- 1 copy of "Encrypted Message 1" (Reproducible Master 6), cut and assembled (see Preparation)
- Team marketing research portfolio
- Several 1-in. strips of paper or ribbon, cut and/or taped together (see Preparation)

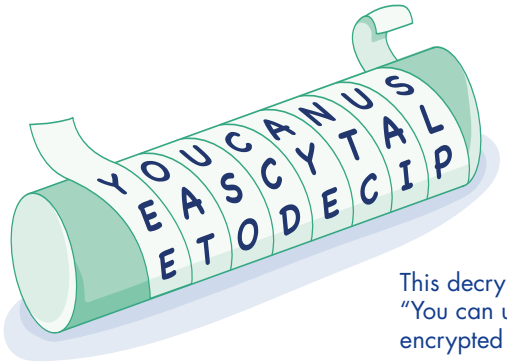
For the teacher:

- Chart paper
- Colored markers

Preparation

- Make your own scytales by cutting PVC pipe of four diameters (½ in., ¾ in., 1 in., and 1¼ in.) into 12- to 18-in. lengths. Each team needs a set of four scytales. If obtaining PVC pipe is difficult, you can use other materials for scytales, such as rolled-up stiff paper, wooden dowels, or cardboard tubes, as long as the resulting cylinders are the correct diameters.

- Photocopy "Encrypted Message 1" (Reproducible Master 6); cut the message into 1-in. strips following the lines on the master, and tape the ends together into one long strip. Assemble one message strip for each team.
- If you prefer, you can encrypt your own message(s) instead of using the reproducible master. To encrypt your own message, wind your paper strip or ribbon around one of the scytales and print your message, one letter per turn of the ribbon, as shown below, ignoring spaces in the message. When you get to the end of the scytale, rotate it and continue on the "line" below.



This decrypted message says, "You can use a scytale to decipher encrypted messages."

  - Create the strips for students' own encrypted messages.
  - If you are using chart paper or other paper, cut it into 1-in. strips and tape strips together end to end so they are around 30 in. long.
  - If you are using 1-in. ribbon, cut pieces around 30 in. long.
- Read the Background on the history of the scytale at the end of this activity.

Classroom Activity

Present the Activity

1. **Remind students that their overarching task is to develop marketing materials for Jupiter Motors.**

   Now that they understand a little more about the internet, they'll begin to explore how information is kept secure as it travels over the internet.

2. Ask students if they thought about the security of the messages they exchanged during the previous simulations.

   Discuss with the class how safe their messages were—if they wanted to keep their information secret, was this a good method for sending it?

During the Activity

3. Have students gather in their marketing teams, and distribute the assembled "Encrypted Message 1" (Reproducible Master 6).
4. Give teams a few minutes to try to decipher the encrypted message before revealing the scytales.
5. Have students record their observations in their science notebooks.

6. Discuss students' observations as a class. Ask, "Were any of you able to crack the code and decipher the message?"

   If any team successfully deciphered the message, have them hold on to their solution until the next part of the activity.
7. Give each team a full set of scytales, and ask them if they can decipher the message. Do not tell them the "key" at this point—ask them if they can "crack the code" on their own.

   Let students play with the pipes and try to figure out the method on their own. You may observe some trying to look through the pipes, slipping the paper through the pipe, or using several pipes in tandem. Ask them to be somewhat careful, as they will reuse the scytales in a later activity.
8. Have teams document the process they use to decipher the message.

   Distribute team portfolios, and ask each team to choose one member to record the main points of the team's discussion in the portfolio.
9. Observe how each team uses the scytales.

   The following prompts may help you guide struggling teams:

   - What if I told you that each scytale could be thought of as a different key for the cipher?
   - What is different about each pipe? How could that relate to the text on the message strip?
10. Have each team report its results.

TEACHER TIP:

Allow teams to struggle a bit at first, but not for too long. The idea is to demonstrate how deciphering a message without knowing the encryption method takes far more time and effort than when the method—and key—are known.

TEACHER TIP:

A video demonstrating how to wrap an encrypted message strip around a scytale is included on the Activity 6 page of the AWIM website.

TEACHER TIP:

You can think of the diameter of the scytale, or the scytale itself, as being the key for the encryption.

SOLUTION

The encrypted message on Reproducible Master 6 is:

SCRSITHTESATHAURETSNTNHTDAPRTETAERRTCEESHEPATESASOBNCUNEOEREN

The ¾-in. diameter scytale correctly decodes this message:

"Start at the bench. Ten paces north. Three paces east. Treasure is under stone."

11. **Have teams encrypt their own messages.**

    Give each team several 1-in. ribbons or strips of paper. Have teams choose a scytale and use it to encrypt their own messages.

12. **Have teams trade messages with other teams and try to decipher them.**

    Depending on the level of your class, you may ask teams to keep the keys secret and have other teams try to crack the code, or teams can share the keys they used so other teams can practice decrypting using a key.

Share and Interpret

13. **As a class, discuss this encryption method.**

    Below are some questions you might pose to prompt discussion:

    - How secure is this method?
    - What would you tell the recipient to let them know how to decipher the message?
    - Why were spaces removed when the message was encrypted?
    - How much time would it take you to crack the code if you had eight different scytales?
    - Once you get the "trick," how could you decipher a message without any scytale?
    - How much time would it take you to crack the code without a scytale?

Reflect and Summarize

14. **Discuss how what they've learned about encryption might relate to keeping messages safe on the internet.**

    Below are some questions you might pose to prompt discussion:

    - Why is it important for messages on the internet to be secure?
    - Do you think that using this type of encryption on the internet would be enough to keep a message safe?

- What types of information are most important to keep safe on the internet?
- What types of information are most important for Jupiter Motors to keep safe?

15. **Have students note their thoughts in their science notebooks.**
16. **Collect the scytales from each team.**

    You will use them again in Activity 8.

Background

History of the Scytale

Throughout history, humans have needed to send secret messages to others near and far. Before motor transportation, phones, and the internet, sending even an ordinary message any distance was challenging—and sending a secret message that others along the way could not decipher was extremely difficult. For instance, during wartime, the ancient Spartans and Greeks needed a form of communication in which their messages to their allies could not be intercepted by the enemy. One way that ancient people did this was by using cryptography, the art of writing and then deciphering codes.

The scytale (rhymes with Italy) is one such form of cryptography. Ancient scytales might use parchment or leather strips that were then wrapped around a wooden cylinder of a certain size. In some cases, once wrapped around the correct cylinder, the message could be read. But in most cases, the message was too important to be read so easily, so it would still need further decoding, using a cipher. (Students have additional opportunities to try decoding messages in Activities 7 and 8.)

For more information about the history and use of scytales, see the Activity 6 page of the AWIM website.

Encrypted Message 1

1.1	1.2	1.3	1.4	1.5	1.6
S	T	H	R	T	E
C	H	T	R	E	O
R	A	D	T	S	E
S	U	A	C	A	R
I	R	P	E	S	E
T	E	R	E	O	N
H	T	T	S	B	
T	S	E	H	N	
E	N	T	E	C	
S	T	A	P	U	
A	N	E	A	N	

Line up the first letter of the next strip here.

Society of Automotive Engineers, Inc. © 2017

Reproducible Master 6

7 Securing Messages: Using Cipher Wheels

Introduction

What Students Do in This Activity

Students explore a different method of encryption: the additive (or Caesar) cipher, an example of a substitution cipher. Unlike the transposition cipher from the previous activity (where the letters stay the same but their position changes), with a substitution cipher, the positions stay the same but the letters change.

As in the previous activity, students will be given encrypted messages without any tools to decipher them. They will initially be challenged to crack the code on their own just by looking at the message. Students will then use a cipher wheel to attempt to discover the key used to encrypt the message, and compare their work with decrypting a message when they know the key. They continue to discuss how understanding encryption will help them complete their Jupiter Motors project.

Rationale

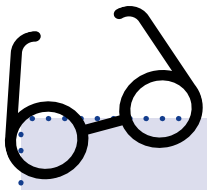
Substitution ciphers are the basis for many encryption schemes used by the internet. This activity gives students more experience with ciphers and increases their understanding of how ciphers work.

As with most encryption methods, there are two key components: the method (the general instructions for how to change the message) and the key (the specific rule or piece of data that completes the instructions). With a cipher wheel, the method is to substitute each letter with another, and the key tells you what specific letters are to be substituted. When students first try to decipher the message, they don't know either the method or the key, so they try to "crack the code" by guessing both. Once they get the cipher wheels and understand how they work, they can "crack the code" by figuring out the key and then use that key to apply the method and decipher the message.

Connection to the Jupiter Motors Challenge

This exploration of a different cipher deepens students' understanding of the concepts of encryption and provides a simple version of methods that are used by computers to secure information.

When Jupiter Motors communicates with cars, that communication needs to be secure. Cryptographic methods based on substitution ciphers are the most common ways to secure information.



ACTIVITY 7 AT A GLANCE

Present the Activity:

- Remind students of their overall goal.
- Review how students used scytales to decrypt messages in the previous activity.

During the Activity:

- Have students work in their marketing teams to decipher three messages.
- Discuss their observations as a class.
- Distribute cipher wheels, and have teams try to use them to decipher the messages, documenting their progress in the team portfolio.
- Have teams report on their results to the class.
- Have teams choose a key, encrypt their own secret messages, and exchange them with another team.

Share and Interpret:

Discuss this encryption method as a class.

Reflect and Summarize:

- Students consider how this activity helps them better understand internet security.
- Students record their observations in their science notebooks.

Time

1 class period

Materials

For each student:

- Science notebook
- 1 copy of "Secret Messages" (Reproducible Master 7)

For each team:

- 2 assembled cipher wheels (see Preparation)
- Team marketing research portfolio

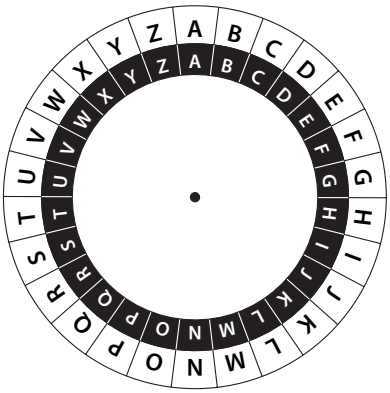
For the teacher:

- "Cipher Wheel Template" (Reproducible Master 8)
- Scissors
- Tape
- Hole punch
- Paper fasteners
- Chart paper
- Colored markers

Paper fasteners

Preparation

- Photocopy Reproducible Master 7.
- Create a cipher wheel for each pair of students:
  - Photocopy "Cipher Wheel Template" (Reproducible Master 8).
  - Cut out the two disks.
  - Punch a hole in the center of each disk.
  - Fasten the smaller disk on top of the larger disk with a paper fastener (see image at right).
- Read the Background on substitution ciphers at the end of this activity.



Assembled, unrotated cipher wheel

TEACHER TIP:

A video demonstrating how to use the cipher wheel is included on the Activity 7 page of the AWIM website.

Classroom Activity

Present the Activity

1. **Remind students of their overall goal.**

   Students are building their understanding of internet security in order to create a marketing presentation for Jupiter Motors that puts their customers at ease with this new technology.

2. **Remind them of how they used scytales to decrypt messages in the previous activity.**

   Explain that they will use a different type of cipher and a new method for deciphering messages in this activity.

During the Activity

3. **Have students gather in their marketing teams.**

   Distribute "Secret Messages" (Reproducible Master 7).

4. **Give students 5–10 minutes to look at the messages and brainstorm possible ways to decipher them by "cracking the code" and figuring out the instructions for how the message was encrypted.**

   Keep the cipher wheels hidden at this point to give the students a chance to recognize the difficulty of deciphering messages when they don't know the method of encryption. Have students record their observations in their science notebooks.

SOLUTION

The deciphered messages read as follows:

Only those who dare to fail greatly can ever achieve greatly.

—Robert F. Kennedy (Key: Encrypted A to J)

It takes a great deal of bravery to stand up to our enemies, but just as much to stand up to our friends.

—J. K. Rowling (Key: Encrypted A to S)

The greatest discovery of all time is that a person can change his future by merely changing his attitude.

—Oprah Winfrey (Key: Encrypted A to Z)

TEACHER TIP:

Teams are not expected to have made much headway here, which is why the time given is limited, so as not to cause too much frustration before moving to the next step.

5. **Discuss their observations as a class. Ask if any teams were able to crack the code and decipher a message.**

   If any team successfully deciphers a message, have them hold on to their solution until the next part of the activity.

6. **Distribute two cipher wheels to each team, and ask teams to use them to decipher the secret messages.**

   Let students play with the cipher wheels and try to figure out the method on their own. Ask them to be careful with their cipher wheels, as they will use them in the next activity. If teams still are struggling with a message, you can offer them the key to decrypt it.

7. **Have teams document the process they use to decipher the message.**

   Distribute team portfolios, and ask each team to choose one person to record the main points of the team's discussion in the portfolio.

8. **Observe how each team uses the cipher wheel.**
9. **Ask each team to report its results to the class.**

10. Have teams choose a key and use it to encrypt their own messages.
11. Have teams trade messages with other teams and try to crack the code and decipher the message.

Share and Interpret

12. As a class, discuss this encryption method.

    Below are some questions you might pose to prompt discussion:

    - How secure is this method?
    - How would you describe the key? What would you tell the recipient about how to decrypt the message?
    - How much time would it take you to crack the code if you did not have a cipher wheel?
    - Once you get the "trick," how could you crack the code without a cipher wheel?

Reflect and Summarize

13. Ask students to think about how this activity helps them better understand internet security.

    Remind them that they will use this information to develop their marketing presentation for Jupiter Motors.

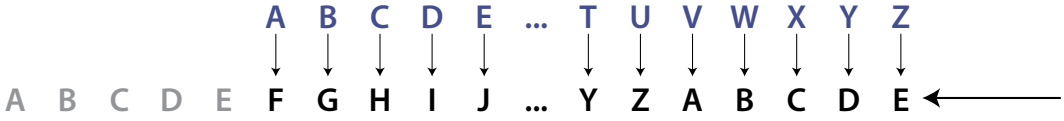
14. Ask students to record their thoughts in their science notebooks.
15. Collect cipher wheels from students before they leave.

    You will use them in the next activity.

Background

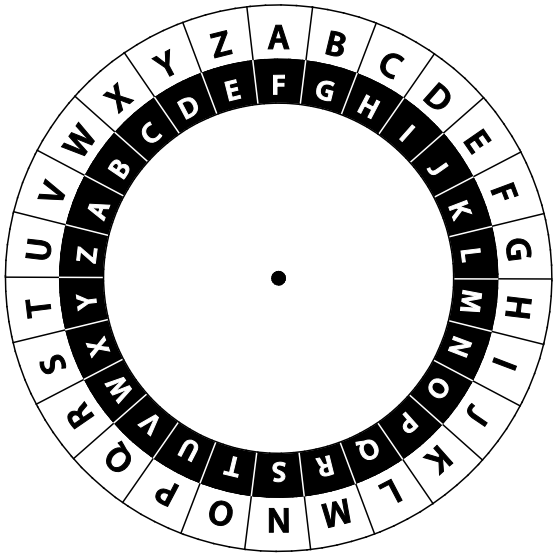
Substitution Ciphers

A **SUBSTITUTION CIPHER** is a set of rules (an algorithm) that allow a message to be encrypted or decrypted. The complexity of the encryption method is based on how letters are substituted. An **ADDITIVE CIPHER** is a specific type of substitution cipher in which each letter is encrypted by shifting it a fixed number of spaces (in effect, "adding" a constant amount to each letter). As illustrated in this diagram, the alphabet is "shifted" a fixed number of spaces; letters at the end of the alphabet "wrap around" to map with letters at the beginning of the alphabet.



Here, the letter A is replaced by F, B by G, C by H, and so forth, until U is replaced by Z. The beginning of the alphabet then "wraps around" so that V is replaced by A, etc. So the key can be described as "A to F."

The cipher wheel included as part of this activity can encrypt and decrypt letters using any additive cipher (of just the 26 letters of the alphabet). For the A to F encryption scheme described above, you would rotate one wheel so that A aligns with F, as shown in the image below:



Rotated cipher wheel (A to F)

Here, the outer ring represents the original letter in the text, and the inner ring represents the encrypted letter. All other letters in the message will be encrypted the same way. (However, you can also decrypt the message with the inner ring representing the original letter in the text, and the outer ring representing the encrypted letter. The important thing is to be consistent—see more on this below.)

The fact that you rotate the wheels to align the original and encrypted letters a number of spaces to encrypt it gives another, more common notation for additive cipher keys: ROT (for rotation). The figure above demonstrates a key of ROT-5, since the alphabet is shifted five spaces (or, in other words, 5 is added to each letter to get the encrypted letter).

For instance, say that you would like to encrypt the message "HAPPY" using ROT-5 as the key. A computer would transform each letter into a number, add 5, and then transform the resulting numbers back to letters. In other words:

- "HAPPY" would become "8 1 16 16 25."
- Adding 5 to each number gives you "13 6 21 21 30."

- Since 30 is past the last number, 26, it wraps around to become 4 (you simply subtract 26 from 30). This gives you "13 6 21 21 4."
- Map those numbers back to letters, and "HAPPY" is now "MFUUD."

(You can also use the cipher wheel to encrypt the message without converting it to numbers, but the number conversion is important to understand for the next step!)

Arithmetic that uses only a range of integers is called modular arithmetic. The most common example is a clock: After 12:00, counting continues back at 1:00. If you want to know what time it is three hours after 11:00, add 3 to 11 to get 14, but then subtract 12 (the biggest number you're using) to get 2, or 2:00. A computer program typically converts the letters to numbers, and uses modular arithmetic (part of a branch of mathematics called number theory) to encrypt and decrypt letters.

You can decrypt a message that was encrypted using ROT-5 in two ways:

- Undo the encryption by subtracting 5 from each encrypted letter. As before, transform the letters to numbers first: "MFUUD" becomes "13 6 21 21 4." Subtract 5 from each to get "8 1 16 16 –1." Since that negative number won't work, wrap it around to become 25 (in other words, add 26, the largest number you're using). Take the final numbers—"8 1 16 16 25"—and turn them back into letters: "HAPPY."
- Re-encrypt the message by making the letters go all the way around. If the original is encrypted using ROT-5, encrypt it again using ROT-21; the letters will come back around to where they started. Try it: "13 6 21 21 4" becomes "34 27 42 42 25." The first four numbers are too big, so subtract 26 from each. The result is "8 1 16 16 25," which, when turned back into letters, is "HAPPY."

It is easy to get confused when using the cipher wheel because you can forget which way you're exchanging letters (outer ring to inner, or inner to outer?). Consistency can help.

For instance, you can treat the wheel so that the outer ring is always original text and the inner ring is always encrypted text. If that's the case, to decrypt a message encrypted using ROT-5 as the key, you would set the cipher wheel as shown in the diagram above, match letters from your encrypted message to the inner wheel, and then write down the corresponding letter from the outer wheel to decrypt. The benefit of this way of thinking is that you set up the wheel the same way whether

you're encrypting or decoding the message—you just have to remember which one you're doing.

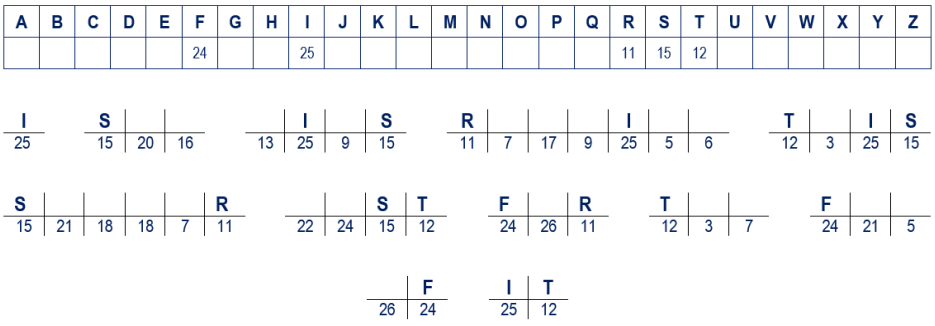
Alternatively, you can choose that the outer ring is always the input and the inner ring the output, so you're always looking for letters in the outer ring and writing down the corresponding message from the inner ring, whether encrypting or decoding a message. This way, you would set the cipher wheel as shown in the diagram to encrypt a message, but you would align the outer A with the inner V to decrypt the message. The benefit of this way of thinking is that you're always going from outside to inside; you just have to figure out the wheel setup to decrypt based on the key used to encrypt the message.

The cipher wheel is an example of an additive cipher. Other substitution ciphers include multiplicative ciphers and exponential ciphers. The latter forms the basis for public key encryption, where extremely large prime numbers are used to determine pairs of exponents that can encrypt and decrypt messages when used together. (Students further explore public key encryption in the next activity.)

Cryptograms, a popular word puzzle, are substitution ciphers that typically follow no particular pattern. Each letter is randomly assigned to a different letter of the alphabet or to a number, so the key needed to decrypt a message would effectively be a complete map of all letters of the alphabet and their corresponding coded letters.

Example of a crytogram. *Solution: I spy kids reading this summer just for the fun of it.*

Source: Texas State Library Commission



Name _____ Date _____

Secret Messages

Decipher the following messages:

1. XWUH CQXBN FQX MJAN CX OJRU PANJCUH

   LJW NENA JLQRNEN PANJCUH

2. AL LSCWK S YJWSL VWSD GX TJSNWJQ LG

   KLSFV MH LG GMJ WFWEAWK, TML BMKL SK

   EMUZ LG KLSFV MH LG GMJ XJAWFVK

3. SGD FQDZSDRS CHRBNUDQX NE ZKK SHLD HR

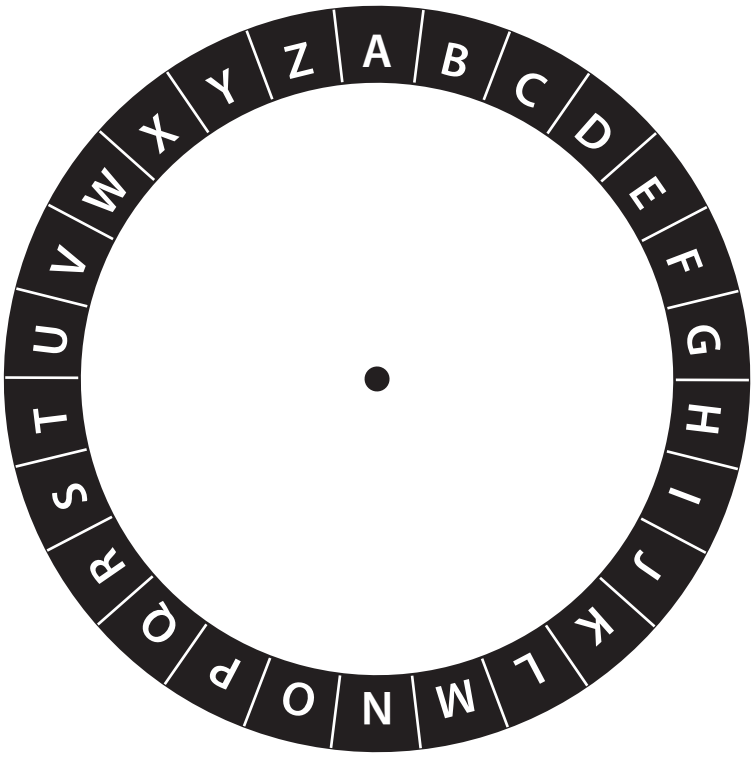
   SGZS Z ODQRNM BZM BGZMFD GHR ETSTQD

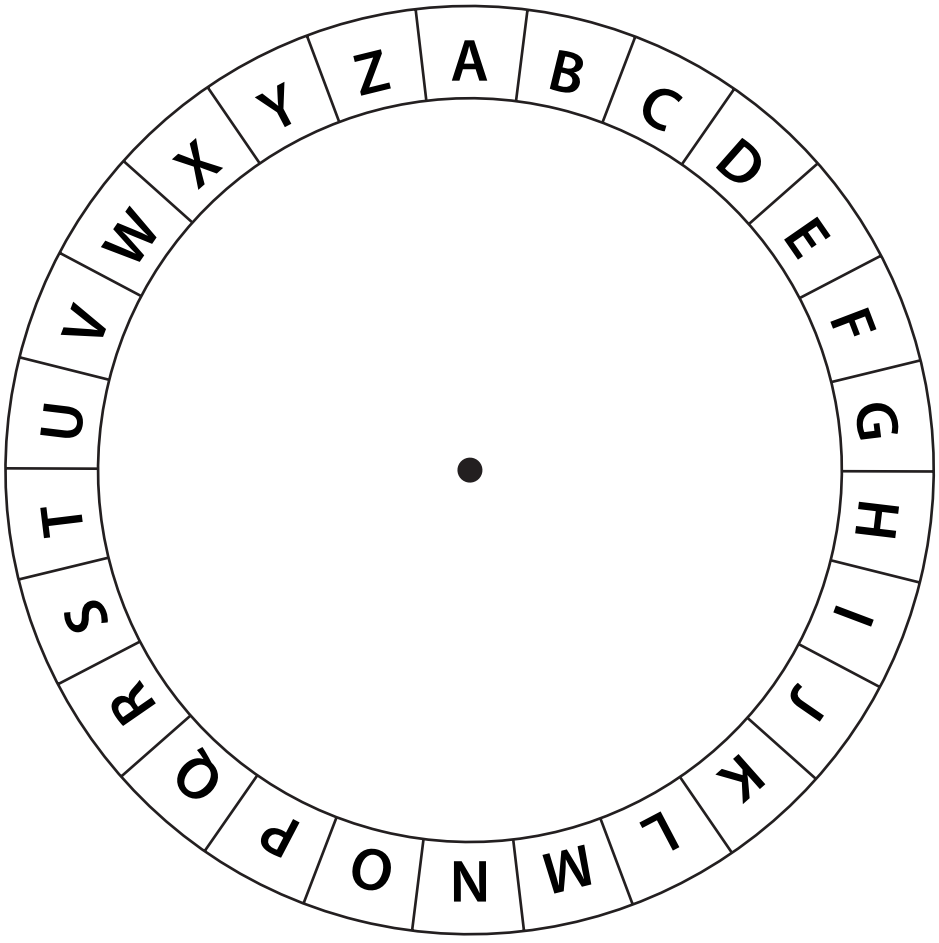
   AX LDQDKX BGZMFHMF GHR ZSSHSTCD

Society of Automotive Engineers, Inc. © 2017

Reproducible Master 7

Cipher Wheel Template





Society of Automotive Engineers, Inc. © 2017

Reproducible Master 8

8 Combining Two Methods

Introduction

What Students Do in This Activity

Students combine the two encryption methods they studied in the previous activities: transposition and substitution ciphers. They attempt to crack messages encrypted using both methods to see how strong even simple ciphers can be when combined. They are given the appropriate keys to decipher messages, which shows them how having a key makes a message easier to decipher.

Students then watch a short video on **PUBLIC KEY ENCRYPTION (PKE)**—a method for securely exchanging keys and providing digital signatures to ensure that a message is authentic.

Rationale

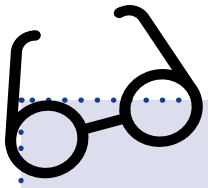
The primary goal of this activity is to show that combining two encryption methods that on their own are relatively simple to crack creates a cipher that is much more difficult to crack. Robust internet encryption often relies on combining more than one encryption method to secure information.

Since security is primarily based on how complicated the cipher is and how long it would take to crack, highly secure encryption techniques (e.g., the Nazi Enigma cipher) are based on a combination of methods. Combining both transposition and substitution ciphers allows students to see that the number of possible combinations is much greater, thus making the cipher much more difficult to crack.

In reality, transposition ciphers are rarely used in computing. Additive ciphers using extremely long keys are most common, with the keys being shared using more complex exponential ciphers.

PKE also provides a mechanism for producing a digital signature. **DIGITAL SIGNATURES** are the primary method for **AUTHENTICATING** messages: they provide the recipient of a message with the assurance that the message actually came from the sender who claims to have sent it, and that the message was not altered during transmission.

The wax seal used many years ago to secure high-level communications is a good analogy for PKE. Kings and other dignitaries rolled or folded the parchment containing their message, melted a small amount of wax over the edge, and then pressed a uniquely carved ring or cylinder into the hot wax to seal the message closed. Upon receipt of the message, the recipient checked the seal to make sure of two things: this was the seal of the person who sent it, and the wax was still holding the parchment closed, indicating that no one had read or altered the message on the parchment.



ACTIVITY 8 AT A GLANCE

Present the Activity:

- Remind students of the larger purpose of their investigation of ciphers.
- Discuss the difference between decrypting a message using a key and cracking a message's code.

During the Activity:

- Have teams attempt to decipher an encrypted message by cracking its code, first without any tools, and then with the set of scytales or cipher wheel.
- Give teams the key used to encrypt the message, and then have them decipher it.
- Have teams encrypt their own messages, trade them with another team, and try to decipher them both by cracking the code and using the key.
- Show students a video on public key encryption, and discuss how this type of encryption makes the internet more secure.
- Discuss all of these encryption methods as a class.

Share and Interpret:

- Have students share their notes on this activity with the rest of their team.
- Have teams share the highlights of their discussion with the class.

Reflect and Summarize:

Students consider how their deepened understanding of internet security will impact their Jupiter Motors project.

Connection to the Jupiter Motors Challenge

By combining the two methods in this simulation, students experience how they can design an encryption scheme that is fairly easy to encrypt and decrypt using the keys but quite difficult without them. This reinforces the notion of cryptography: the desire to secure information that is easy for people to decrypt when they have the keys (and are thus authorized to decrypt it) but difficult to decrypt for those without the keys.

The information on digital signatures is directly connected to the Jupiter Motors challenge because it is through digital signatures that cars can be sure that information (e.g., map data or software updates) originated from Jupiter Motors and was not altered during transmission.

Time

1 class period

Materials

For each student:

- Science notebook

For each team:

- 2 assembled cipher wheels (from Activity 7)
- 1 set of 4 scytales (from Activity 6)
- 1 copy of "Encrypted Message 2" (Reproducible Master 9), cut and assembled (see Preparation)
- Team marketing research portfolio

For the teacher:

- Scissors
- Tape
- Chart paper
- Colored markers
- Video on public key encryption (see Preparation)
- Computer with a large-screen monitor or projector

TEACHER TIP:

Depending on time, you may choose to show an excerpt rather than the entire video.

Preparation

- Photocopy Reproducible Master 9, and cut the messages into 1-in. strips, following the lines on the master. Tape the ends together into one long strip.
- Review the videos on public key encryption (found on the Activity 8 page of the AWIM website), and decide which one you will show to your students. Bookmark your chosen video.
- Arrange for access to a computer with a large-screen monitor or projector. Test the equipment before class to ensure adequate volume, playback quality, etc.
- Read the Background on encryption at the end of this activity.

Classroom Activity

Present the Activity

1. **Remind students of the larger purpose of their investigations of ciphers.**

   Building their understanding of internet security will help students develop a marketing presentation for Jupiter Motors that puts their customers at ease with this new technology.

2. **Discuss the difference between cracking (or hacking) a message and decoding it.**

   You may ask a prompting question, such as, "How can you make a message easy to decrypt but hard to crack?"

During the Activity

3. **Have students gather in their marketing teams.**

   Distribute team portfolios. Give each team a set of scytales and two cipher wheels, and remind them how to use the two encryption methods, or ask for student volunteers to briefly explain how to use each encryption method.

4. **Give each team "Encrypted Message 2" (Reproducible Master 9), and tell them they have five minutes to decipher it.**

   Students will struggle trying to decipher this without keys, since getting the right combination of scytale and letter shift won't be easy. Allowing only a brief amount of time before moving to the next step should keep them from becoming too frustrated.

5. **Give teams the keys used to encrypt the message, and have them try again to decipher it.**

SOLUTION

The message was encrypted using the cipher wheel set at A to M (or ROT-12) and the 1-in. scytale.

The message can be decrypted in either order (using the cipher wheel or the scytale first), since the two methods are independent. For instance, the original encrypted text reads:

E F U R Z Y B U D F P F K Z P T D T U F E Q A Q E T Q E I X E Q M Q R Q U F F O D R F T A A A F

After decoding the message with the 1-in. scytale, the message is:

E B K U E E U F F U Z F T Q F T U D P E Q M F A R F T Q E Q O A Z P D A I R D A Y F T Q X Q R F

Using the cipher wheel set at A to M (or ROT-12), the fully decrypted message is:

Spy is sitting in the third seat of the second row from the left.

6. **Remind students to note their observations in their science notebooks throughout the process.**
7. **Have teams encrypt their own messages.**

   Have teams choose their own combinations of encryption methods with keys and use them to encrypt messages.
8. **Have teams trade messages with other teams and try to decipher them, with or without the keys.**
9. **Introduce PKE, and show the video (or video excerpt) you chose.**
10. **Discuss how PKE works and how it makes the internet more secure.**

    Explain that PKE provides two distinct security mechanisms.

    - It can be used to encrypt messages to keep them hidden and secure during transmission; messages can be opened only by the intended recipient.
    - It can be used to digitally "sign" a message (thus creating a digital signature) so that any recipient can be sure that the message originated from the sender who claimed to send it, that it arrived intact and unchanged, and that the sender cannot deny they sent it in the first place. A digital signature is essentially the process of encrypting a message, except that the keys are in reverse. (See Background for more information.)
11. **Discuss these encryption methods—a combination of ciphers and PKE—as a class.**

    Below are some questions you might pose to prompt discussion:

    - How secure are each of these methods?
    - What would you tell the recipient to let them know how to decrypt the message?
    - How much time would it take you to decrypt the cipher-combination method if you had both keys? only one key? neither key?
    - Would it matter in which order you deciphered the message?

Share and Interpret

12. **Ask students to share their observations of this activity with the rest of their team.**

    Have each team choose one person to record the main points of the team's discussion in the team portfolio.
13. **Have teams report the highlights of their discussion to the class.**

Reflect and Summarize

14. **Discuss how their understanding of encryption helps students more deeply understand internet security and how it will impact their Jupiter Motors project.**

    Students should now have a good understanding of the reliability of the internet, both because of its ability to provide multiple pathways for messages to travel and because of the security provided by encrypting information—all of which can help them reassure Jupiter Motors' customers.

Background

Encryption

Encryption is used not only to secure messages being transmitted but also to secure information stored on any computer. Even laptops may be set up to encrypt all the information that's stored on them, which is only decrypted when the correct password is entered. Information stored in the cloud (music library, files stored on Dropbox, shopping information) is (or should be) encrypted by the company that hosts the data.

On their own, the transposition and substitution ciphers used in this unit are relatively easy to crack—popular word games (e.g., anagrams and cryptograms) are based on both. Students likely saw that even without being told the key, they could relatively quickly decrypt a message that was encrypted using only one of these ciphers; combining two methods made cracking more difficult.

The substitution ciphers students used in this activity are elemental forms of the ciphers predominantly used throughout computing today. They are a form of **SYMMETRIC ENCRYPTION**, where the key used to encrypt a message can also be used to decrypt it. More secure methods rely on long keywords or phrases and on higher-level mathematics too complicated for today's computers to crack in a reasonable time.

PKE is the primary method for securing sensitive information on the internet. It is a form of **ASYMMETRIC ENCRYPTION** that requires two keys: one to encrypt a message and one to decrypt it. Unlike with symmetric ciphers, PKE is designed so that you can't decrypt a message even if you have the key used to encrypt it (or, at least, not quickly or easily, using today's technology). In PKE, one key is designated as the public key, and the other is the private key. Messages encrypted using the public key can only be decrypted using the private key, and vice versa.

When a user wants to send a message to someone else securely using PKE, they would obtain the recipient's public key and use it to encrypt the message. Thus, only those who hold the private key (which the recipient should keep private) can open and read the message. The recipient can make their public key available widely, even posting it on a webpage, since having the public key won't let anyone decrypt messages that were encrypted using it.

PKE can also be used to digitally sign a message. Even if the information itself isn't sensitive, it's often vital for a receiver to be sure that the information or program they received really did come from a specific source and not from someone trying to spoof them and insert viruses or malware onto their computer. In this case, the sender would encrypt the message using their private key. Anyone who receives it can obtain the public key and decrypt it. The contents of the message aren't kept secret, since anyone can get the public key to decrypt it. But the very fact that the public key decrypted the message ensures that the only one who could have encrypted it is the person holding the private key. Thus, this digital signature provides security that the message originated from the person with the private key and that it was unchanged during transmission (since changing it would require decrypting it, changing the contents, and re-encrypting it using the private key).

A primary use of digital signatures, and the use most related to the Jupiter Motors challenge, is to authenticate software updates to any computer, including tablets, smart phones, or the computer built into cars. When a device receives an update, it first checks the digital signature to make sure the update is authorized before installing it.

Since encrypting large documents using PKE can be costly, this method is typically reserved for highly sensitive information. In most cases, large pieces of text are encrypted using a slightly simpler method, and the keys are encrypted using PKE or another super-strong method.

A user password is the primary piece of information that secures most keys, so it is important to choose one that isn't easy to guess. Most systems now require passwords to contain both upper- and lowercase letters, numbers, and even symbols. And to be truly secure, it is recommended that a different password be used for each site.

For more information about encryption, see the AWIM website.

Encrypted Message 2

2.1	2.2	2.3	2.4	2.5
E	P	E	E	D
F	F	Q	Q	R
U	K	A	M	F
R	Z	Q	Q	T
Z	P	E	R	A
Y	T	T	Q	A
B	D	Q	U	A
U	T	E	F	F
D	U	I	F	
F	F	X	O	

Line up the first letter of the next strip here.

Society of Automotive Engineers, Inc. © 2017

Reproducible Master 9

9 Developing Marketing Ideas

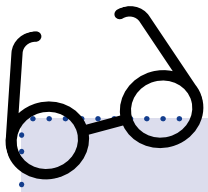
Introduction

What Students Do in This Activity

Building on the simulations and activities they have carried out thus far, teams begin developing their marketing plans for Jupiter Motors.

Rationale

This activity is an opportunity for students to synthesize all the information they have explored in this challenge. It also offers you an opportunity to continue to assess both individual and team learning.



ACTIVITY 9 AT A GLANCE

Present the Activity:

- Review the reason that Jupiter Motors came to the students for help.
- Show the car-hacking video first shown during Activity 1, and ask students how their understanding of internet security has changed since then.
- Discuss as a class what people's fears regarding internet-accessible cars might be.
- Ask students what they have learned that could help reassure potential customers.

During the Activity:

- Review the expectations for students' final presentations.
- Have teams work on their presentations.

TEACHER TIP:

This activity is designed for teams to plan a marketing idea but not to execute it. If time allows, you may wish to have students develop their marketing ideas into final products.

Time

1–4 class periods

Materials

For each student:

- Science notebook

For each team:

- 1 copy of "Presentation Planner and Checklist" (Reproducible Master 10)
- 1 copy of "Presentation Rubric" (Reproducible Master 11)
- Chart paper
- Markers
- Team marketing research portfolio

For the teacher:

- Video on hacking a smart car from Activity 1 (see Preparation)
- Computer with a large-screen monitor or projector

Preparation

- Make sure that you can access the video for this activity (found on the Activity 9 page of the AWIM website).
- Arrange for access to a computer with a large-screen monitor or projector on which to show students the videos. Test the equipment before class to ensure adequate volume, playback quality, etc.

Classroom Activity

Present the Activity

1. **Review the reason that Jupiter Motors came to the students for help.**

   Ask students to get out "Letter from Jupiter Motors" (Reproducible Master 1) from their science notebooks.

   Revisit some of the questions you asked in Activity 1 to spark discussion. Feel free to supplement with your own questions:

   - What does Jupiter Motors want you to do?

- Students should recognize that Jupiter Motors wants them to explain the basics of cybersecurity in marketing materials designed to reach Jupiter Motors' target audience.

- What requirements does Jupiter Motors have for the presentation?

  The letter mentions the following requirements:

  - The presentation should require little prior knowledge.
  - It should describe how information flows through the internet.
  - It should describe how the architecture of the internet safeguards information in case of failure.
  - It should describe how information is kept secure—both where it is stored and while it is being transmitted.
  - It should describe how systems decide with whom or what they should share information.

- How will you know if the marketing materials are successful?

  Answers will vary, but students should recognize that they must meet all of Jupiter Motors' design criteria in order to be successful.

2. **Show the video clip.**

   Remind students that they saw this video in the very first activity. Ask them to keep in mind everything they now know about the internet and internet security as they watch it a second time.

3. **Discuss what students think people's fears might be.**

   Students should recognize that people might fear that internet-accessible cars could be hacked and that people outside of their car might take control of it for nefarious purposes.

4. **Ask students, "What have we learned so far that could help us make people feel less afraid about internet-accessible cars?"**

   Students should mention the following:

   - The internet was constructed to make sure that messages can get through, even if parts of the internet go down.
   - Longer messages are labeled, so they can be easily reassembled.
   - If they aren't encrypted, messages can be read by any machine. Encryption allows messages to be encrypted before they are sent, so they are hard to read without a key.

TEACHER TIP:

For examples of marketing presentations, see the Activity 9 page of the AWIM website.

TEACHER TIP:

It may be necessary to explain to students that a storyboard is a visual outline—a squence of simple drawings, typically with some directions and dialogue, representing each element of a presentation.

TEACHER TIP:

If you've decided to run the preesentation as a competition, present this idea now.

- PKE allows messages to be sent easily but read only by people who hold the right key.
- Digital signatures provide confirmation that a message came from the person who claims to have sent it.

During the Activity

5. **Have students gather in their marketing teams, and distribute "Presentation Planner and Checklist" (Reproducible Master 10) and "Presentation Rubric" (Reproducible Master 11).**

   Ask teams to retrieve "Marketing Idea Planner and Checklist" (Reproducible Master 2) from their team portfolios. Teams should use all of these worksheets as guides as they prepare their presentations. Give each team a pad of chart paper, some colored markers, and its team portfolio.

6. **Tell teams that their presentations should be about five minutes long.**

   Let teams know that their presentations should include the following:

   - An explanation of the medium that was chosen for the marketing campaign
   - An overview of the script and/or a storyboard of the campaign
   - A reasoned argument for why the presentation was developed as it was
   - A discussion of how the team's work over the course of the unit factored into the development of the campaign

7. **Tell students that the presentations will conclude with an opportunity for the audience to ask teams questions about their work.**

   The audience will likely ask questions concerning the presenters' understanding of cybersecurity and how and why the team made their particular decisions (e.g., "Why did you select a brochure/video/PowerPoint presentation to communicate your message?").

8. **Ask teams to decide which member will be responsible for presenting each part of the presentation and in what order, and to record the order on a piece of chart paper.**

   This will help their presentations flow more smoothly.

9. **Explain how the presentations will be assessed.**

   Go over "Presentation Rubric" (Reproducible Master 11), and tell students how they will receive feedback on their presentations beyond the immediate feedback they will get from the audience.

TEACHER TIP:

It will likely take more than a single class session for teams to create their presentations. Further work can be done outside of class or in subsequent classes.

Remind students that after they have made their presentations, they will be asked questions concerning how and why they made their particular decisions. Emphasize that this means that all members of the team must be equally ready to answer questions. Suggest that they brainstorm some questions they might get, and agree as a team on the best responses.

10. Give teams time to work on their presentations.

Name _____ Date _____

Presentation Planner and Checklist

Use this planner to develop a marketing presentation for your classmates. Your presentation can include visual aids, such as posters, illustrations, or projections from a computer. As your team completes each task, put an **X** in the right-hand column to show that this part is ready.

Task	**Ready ☒**
1. Discuss the important things you learned and what you think you need to include in your marketing idea. Make a list of those things below (use the back of this worksheet, if necessary):	
2. Determine the form that your marketing idea will take (a website, podcast, video, newspaper ad, or something else). We chose to create a _____	
3. Create a script or storyboard for your idea. Make sure that you include: ▸ An explanation of why you chose this medium (poster, brochure, podcast, video, website, etc.) for your marketing campaign	
▸ What your marketing idea is and why you chose it	
▸ A reasoned argument for why you developed the presentation as you did	
▸ A discussion of how the team's work over the course of the unit factored into the development of the campaign	
4. Decide who will present each part of your presentation.	
5. Revise your script or storyborad to match your final plan.	
6. Think about the types of questions that your audience might have, and consider how your team would answer those questions.	
7. (Optional) Create visuals to support your presentation.	

Society of Automotive Engineers, Inc. © 2017

Reproducible Master 10

Name _____ Date _____

Presentation Rubric

For each evaluation criterion, circle a number to indicate the score.

	4	3	2	1
Written Reflections on the Activities Carried Out in the Challenge	Reflections are thorough and legible.	Reflections are thorough but not legible.	Reflections are not thorough or legible.	Few reflections are completed.
Presentation Content: Level of Prior Knowledge Required	Requires little prior knowledge to understand.	Requires some prior knowledge to understand.	Requires a fair amount of prior knowledge to understand.	Audience must have a background in internet security to understand.
Presentation Content: Internet Architecture	Clearly explains the architecture of internet safeguards in case of failure.	Explains the architecture of internet safeguards in case of failure.	Does not give a clear explanation of the architecture of the internet.	Does not include an explanation of the architecture of the internet.
Presentation Content: Important Information	Thoroughly describes the following: ■ How information flows through the internet ■ How information is kept secure—both where it is stored and while it is being transmitted ■ How systems decide with whom or what they should share information	Adequately describes the following: ■ How information flows through the internet ■ How information is kept secure—both where it is stored and while it is being transmitted ■ How systems decide with whom or what they should share information	Describes the following, but with little or no detail: ■ How information flows through the internet ■ How information is kept secure—both where it is stored and while it is being transmitted ■ How systems decide with whom or what they should share information	Includes little information about the following: ■ How information flows through the internet ■ How information is kept secure—both where it is stored and while it is being transmitted ■ How systems decide with whom or what they should share information
Presentation Content: Safety and Security	Helps people feel safe and secure about Jupiter Motors' cars.	Helps people feel relatively safe and secure about Jupiter Motors' cars.	Does not really address people's fears about self-driving cars.	Makes people feel less safe about self-driving cars.

	4	3	2	1
Organization	Team presents information in a logical, interesting sequence that the audience can follow.	Team presents information in a logical sequence that the audience can follow.	Audience has difficulty following the presentation because the flow is not completely logical.	Audience cannot understand the presentation because it is disjointed.
Team Dynamics	Students work together respectfully, and all team members participate.	Students mostly work together respectfully, and all team members participate.	Students mostly work together respectfully, and some team members participate.	Students do not work together respectfully, and only some team members participate.
Delivery	Students use clear voices and pronounce terms correctly and precisely.	Students' voices are clear. Students pronounce most words correctly.	Students incorrectly pronounce some vocabulary. Audience members have difficulty hearing the presentation.	Students mumble, pronounce words incorrectly, and/or speak too quietly or quickly for audience members in the back of class to hear.

Comments:

Society of Automotive Engineers, Inc. © 2017

10 Presenting Marketing Ideas

Introduction

What Students Do in This Activity

Student teams share their final cybersecurity marketing ideas with the class and, ideally, invited guests. Each team presents its idea and discusses how it thinks its marketing pitch would help the target audience feel more comfortable with the security of Jupiter Motors' self-driving car. Audience members may ask questions of any team member concerning their marketing idea.

Students reflect on how their understanding of cybersecurity has grown since they began the challenge and complete a unit assessment. They turn in their completed science notebooks and team marketing research portfolios.

TEACHER TIP:

Each team needs to bring a completed copy of "Marketing Idea Planner and Checklist" (Reproducible Master 2) and "Presentation Planner and Checklist" (Reproducible Master 10), their cybersecurity marketing script or storyboard, and a list of which member will present each component of the plan and in what order.

Rationale

This activity is an opportunity for students to demonstrate the skills and understanding they have gained from the activities in this unit. It also gives them experience in presenting information to a large group. By considering each item in the rubric, they gain awareness of the elements of an effective presentation. The team presentations offer another opportunity to assess students' learning and teamwork.

Time

1–2 class periods

Materials

For each student:

- 1 copy of "Cybersecurity Challenge: Assessment" (Reproducible Master 12)

ACTIVITY 10 AT A GLANCE

Present the Activity:

(Optional) Introduce the expert panel.

During the Activity:

Have each team give its presentation.

Share and Interpret:

- After each presentation, ask follow-up questions to probe students' understanding.
- Encourage other students to ask questions and offer feedback.
- (Optional) Have expert panelists ask questions and offer feedback.
- Score each team's presentation using a rubric.

Reflect and Summarize:

- Discuss how students' understanding of cybersecurity has changed throughout this unit.
- Have students complete an assessment and turn in their science notebooks and team portfolios.

TEACHER TIP:

If you chose to run the presentations as a competition, you will need to create a modified version of "Presentation Rubric" (Reproducible Master 11) for students and other audience members to use as a scoring sheet. You might also purchase or make a small prize for the winning team(s).

For the teacher:

- 1 copy of "Presentation Rubric" (Reproducible Master 11) for each team
- (Optional) Document camera or overhead projector
- 1 copy of "Cybersecurity Challenge: Assessment Answer Key" (Reproducible Master 13)

(Optional) For each panel member:

- 1 copy of each team's marketing presentation script or storyboard
- 1 copy of "Presentation Rubric" (Reproducible Master 11)

Preparation

- Photocopy Reproducible Masters 11 and 12.
- (Optional) Remind any invited guests of the date, time, and location of the final presentations.
- (Optional) Photocopy teams' marketing scripts or storyboards for each expert panel member.
- Prepare the presentation area.

Classroom Activity

Present the Activity

1. (Optional) Introduce the expert panel.

   Explain that these "experts" represent Jupiter Motors and will give feedback on the teams' presentations.

During the Activity

2. Have each team give its presentation.

   Before each presentation, collect the chart paper listing which member will present each component of the plan and in what order. If one is available, allow teams to use a document camera or overhead projector to display their work.

Share and Interpret

3. After each presentation, ask follow-up questions to probe team members' understanding of cybersecurity.
4. Encourage other students to ask questions and share their reactions to each presentation.

   Allow three to five minutes after each presentation for this discussion.

5. (Optional) Invite the expert panelists to ask questions and provide feedback to teams.
6. Use the "Cybersecurity Challenge Presentation Rubric" (Reproducible Master 11) to score each team's presentation.

   You may want to give teams formal written comments in addition to a score that reflects your regular assessment system.

7. (Optional) If you chose to run the presentations as a competition, have the audience turn in their completed scoring sheets. Calculate the final scores, and announce the winning team(s)!

Reflect and Summarize

8. Wrap up the activity with a whole-group discussion on cybersecurity.

TEACHER TIP:

It is possible that each team will present basically the same information, and classmates will have no new questions after the first couple of presentations. Encourage students to ask not only about the presenters' understanding of cybersecurity but also the presentation itself (e.g., "Why did you select a brochure/video/ PowerPoint presentation to communicate your message?")

You might also want to have ready some questions that students might not think to ask (e.g., "Would you drive one of these cars yourself? Would you let your grandmother drive one? Is there anyone who shouldn't drive one of these cars?"). Write the questions on slips of paper, and give them to students if the Q&A seems to have stalled.

Pose some or all of the following questions to help students reflect on how their understanding of cybersecurity has grown since they began the challenge:

- How does the design of the internet make it more reliable?

  Because of its distributed nature (there is no one central server running the internet), messages continue to flow even if some parts are out of commission. Protocols account for any missing packets, and automatically redirect and resend them.

- Why is it important to encrypt information before transmitting it through the internet?

  The internet can only send text. Even though we use metaphors, such as "packets," "envelopes," and such, all text is readable by any machine along the way. Encryption scrambles messages so that it is extremely difficult to unscramble them without being given a key.

- What is a digital signature? Why is it important for Jupiter Motors to use a digital signature when sending updates to a car?

  Digital signatures are a sort of encryption that provides confirmation that a message truly originated from the person identified as the sender. Jupiter Motors uses digital signatures so that any updates can be guaranteed to come from Jupiter Motors, not from a hacker or someone else who might tamper with the car's software.

- How does a strong password help secure information on the internet?

  A strong password makes it difficult for hackers to gain access to your personal information, including any keys used in encryption.

9. **Distribute "Cybersecurity Challenge: Assessment" (Reproducible Master 12).**

   Have students complete the assessment. "Cybersecurity Challenge: Assessment Answer Key" (Reproducible Master 13) offers possible responses.

10. **Collect the completed science notebooks and team portfolios.**

    The science notebooks and team portfolios should also be used as part of the final assessment of student work in this challenge.

Name _____ Date_____

Cybersecurity Challenge: Assessment

1. Draw a map of how you would send information across the internet. Mark yourself (or your device) on the map. (Use the back of this sheet.)

2. Why is it important to protect personal information on the internet? What steps can you take to make sure that your personal information is protected on the internet?

3. (a) What is a digital signature? (b) How is it related to encryption? (c) Why are digital signatures important?

4. (a) Describe an event that could "bring down" the internet. (b) How does the design of the internet make sure that as many messages as possible can still be transmitted?

Society of Automotive Engineers, Inc. © 2017

Name _____ Date_____

Cybersecurity Challenge: Assessment

Answer Key

1. Draw a map of how you would send information across the internet. Mark yourself (or your device) on the map. (Use the back of this sheet.)

   Answers will vary. Maps should include nodes, sender(s), recipient(s), packets, and bad nodes (with alternative routing of packets).

2. Why is it important to protect personal information on the internet? What steps can you take to make sure that your personal information is protected on the internet?

   Students should mention that there are people who might want to use their passwords to connect to websites to either maliciously post information under their names, steal their parents' credit card or bank information, or steal their or their parents' other personal information.

   Students should mention some of the following steps to protect their information:

   - *Use a secure password that isn't easy to guess.*
   - *Use a different password for each website.*
   - *Make sure that you are connected securely.*
   - *Don't perform sensitive tasks (such as banking or purchases) when connected to public networks.*
   - *Use encryption to secure your home network and information on your computer's hard drive.*
   - *Don't use standard email or text messaging to send passwords or any other sensitive information.*

Society of Automotive Engineers, Inc. © 2017

3. (a) What is a digital signature? (b) How is it related to encryption? (c) Why are digital signatures important?

   (a) A digital signature is a way for a person or company to show that a message actually came from them and wasn't changed. Using a digital signature allows the recipient to feel confident that the message came from the sender.

   (b) Digital signatures use a "backward" form of public key encryption: The sender encrypts a message using their private key, and the recipient decrypts it using the sender's public key. The only way the message can be decrypted using the sender's public key is if it were encrypted using the corresponding private key, and only the sender has access to that private key.

   (c) Digital signatures ensure that a message comes from the person who claims to have sent it. In the Jupiter Motors example, the company may send software updates to its self-driving car; if the update is digitally signed, the recipient can be sure that it came from Jupiter Motors and is safe to install. Otherwise, someone can impersonate the car company and send a malicious update that could cause the car to do bad things.

4. (a) Describe an event that could "bring down" the internet. (b) How does the design of the internet make sure that as many messages as possible can still be transmitted?

   (a) To "bring down" the internet, one could attack it physically by taking servers (nodes) offline. Their power can be interrupted, the cables can be physically disconnected, or an attacker can send lots of messages to them, overwhelming them and preventing good messages from getting through.

   (b) The internet is designed as a large "web," so even if large parts are brought down, messages can find alternate paths around the outage and continue to flow. A message can follow a number of paths to get from one server to another, so even if many are disrupted, messages likely can still get through. (Of course, some messages may be lost, and some users may be in the outage area, but the distributed nature of the internet means that other areas will continue to function.)

Society of Automotive Engineers, Inc. © 2017

Glossary

Important: Students will learn many of these words as the module progresses, but they are not expected to know them, nor are they assessed on whether they know them. The terms are listed here in one place for the convenience of the classroom teacher.

ADDITIVE CIPHER a specific type of substitution cipher in which each letter is replaced by the letter a fixed number of spaces after it (in effect, "adding" a constant amount to each letter and "shifting" the entire alphabet some number of spaces).

ASYMMETRIC ENCRYPTION a kind of encryption in which two different keys are used: one key encrypts a message, and a second key decrypts it (unlike symmetric encryption, where the same key is used to encrypt *and* decrypt a message). While the two keys are typically related mathematically, it is by design nearly impossible to decrypt a message using the key that encrypted it. (See public key encryption.)

AUTHENTICATING proving that something is real or valid.

CIPHER a system for disguising text, in which strings of characters, usually letters, are changed according to a particular coding scheme.

CRYPTOGRAPHY the art of writing and then deciphering ciphers.

CYBERSECURITY the defense of computer systems, including physical hardware, software programs, and data, from attempts to harm, steal, or disrupt them.

DIGITAL SIGNATURE a type of encryption that provides confirmation that a message truly originates from the person identified as the sender.

DOMAIN a group of online resources controlled by a single entity, usually part of a particular company, institution, or group, that share a unique internet address.

DOMAIN NAME a string of characters consisting of letters, numbers, and hyphens, separated by periods, that specify a particular domain. Each domain name ends with a suffix (e.g., ".edu" or ".us") called a top-level domain.

DOMAIN NAME SERVER a specially identified server that is like an internet address book; what the internet uses to map domain names to IP addresses.

ENCRYPTION the process of encoding or disguising messages to hide their meaning.

HACKERS those who use computers to gain unauthorized access to data.

HEADER part of a packet that includes the sender information, the recipient information, and how the packets fit together in order to reassemble the message.

INTERNET a global system of communications networks that connect computer networks around the world.

IP (INTERNAL PROTOCOL) a set of rules that determine how information is sent from one computer to another on the internet, including addresses (see IP address) and routes (overall path of connections between nodes on the internet).

IP ADDRESS a series of four numbers from 1 to 255, separated by periods (for instance, an IP address for google.com is 216.58.217.78). Each device on the internet, including servers, nodes, routers, computers, phones, and any internet-connected widget, has a unique IP address.

KEY a piece of information that identifies how a message is encrypted. For symmetric encryption, the key can also be used to decrypt the message; for asymmetric encryption, a second key is needed to decrypt the message.

NODE a computer, server, router, or other electronic device that serves as a connecting point along routes of internet traffic.

PACKET a piece of a message (whether an image, video, file, email—any piece of information sent over the internet), along with information that tells nodes where the message came from, where it's going, and how to reassemble the pieces.

PROTOCOL a set of rules regarding how data are transmitted electronically.

PUBLIC KEY ENCRYPTION (PKE) also called asymmetric encryption, PKE is a kind of encryption involving two keys: a public key that is shared with the public and a private key that only the user has. Messages encrypted using the public key can only be decrypted with the private key, and vice versa. The two keys are generated using a pair of extremely large prime numbers and their product. It is nearly impossible using current computing power to generate a private key simply from the public key, which makes this encryption method very secure.

RELIABILITY the quality of being dependable, sturdy, trustworthy, and consistent.

ROUTER a node that primarily joins two or more computer networks via either wired or wireless connections.

SCYTALE a tool used by the ancient Greeks to encrypt messages; a strip of parchment or other material is wound around a cylinder of a specific diameter, and the message is written on it. It can only be read (decrypted) with a cylinder of the same diameter.

SERVER a computer that performs particular services (e.g., allowing access to data files or programs) for all the computers in a network.

SUBNET a collection of IP addresses that have the same first one, two, or three numbers (e.g., 24.x.x.x or 8.12.172.x).

SUBSTITUTION CIPHER a way to encrypt messages using the basic concept of letter (or character) substitution—every occurrence of a letter is substituted with another letter (or number or symbol), but letters stay in the same position.

SYMMETRIC ENCRYPTION a kind of encryption where the same key is used to both encrypt and decrypt a message.

TOP-LEVEL DOMAIN the last segment of a domain name. Common top-level domains in the United States are .com, .net, .edu, and .gov.

TCP (TRANSMISSION CONTROL PROTOCOL) a set of rules that control how data are sent through the internet. This protocol is responsible for making sure that all packets in a message are received and then assembled in the correct order.

TRANSPOSITION CIPHER a code in which letters from the source message are scrambled (transposed) in a particular pattern, but each letter keeps its identity (e.g., “K” still means “K”).