(http://csmatters.org) 3 - 12

0b11 - 0b1100

Cryptography: Public Key Encryption, Certificate Authorities, and Open Standards

Unit 3. Information and the Internet

Revision Date: Jul 22, 2019
Duration: 2 50-minute sessions

Lesson Summary

Summary

In this lesson, students will learn two solutions to the key distribution problem and the mathematical foundations behind these solutions. They will make connections between encryption, the use of SSL/TLS in web browsers, and the use of digital certificates. Students will recognize the value of open standards used in modern cryptography.

Outcomes

- Students will understand the impact of the key distribution problem on secure communication.
- Students will understand that a carefully designed one-way mathematical function allows people to exchange keys or use public keys to solve the key distribution problem.
- Students will understand that digital certificates are used for authentication, and that these certificates rely on the trust model: the certificate authorities are being *trusted* to provide accurate information.

Overview

Session 1

1. Getting Started (5 min) - Students journal on the safety of transactions made online and the role of cryptography,
2. Introduction to Content (15 min) - The Key Distribution problem and mathematical modulus are presented and discussed.
3. Guided Activities (25 min) - Students learn about double encryption through analogies and a group activity.
4. Wrap Up (5 min) - Journaling on sharing secrets.

Session 2

1. Getting Started (5 min) - Students journal on how Diffie's solution benefits them.
2. Introduction to Content (5 min) - Students discuss Diffie's solution to the Key Distribution problem
3. Guided Activities (35 min) - Students Role Play and Journal about Public Key Encryption.
4. Wrap Up (5 min) - Journaling about the positive/negative aspects of Public Key Encryption

Learning Objectives

CSP Objectives

- *EU DAT-1 - The way a computer represents data internally is different from the way the data is interpreted and displayed for the user. Programs are used to translate data into a representation more easily understood by people.*
  - LO DAT-1.A - Explain how data can be represented using bits.
- *EU AAP-2 - The way statements are sequenced and combined in a program determines the computed result. Programs incorporate iteration and selection constructs to represent repetition and make decisions to handle varied input values.*
  - LO AAP-2.C - Evaluate expressions that use arithmetic operators.
- *EU AAP-4 - There exist problems that computers cannot solve, and even when a computer can solve a problem, it may not be able to do so in a reasonable amount of time.*
  - LO AAP-4.A - For determining the efficiency of an algorithm: a. Explain the difference between algorithms that run in reasonable time and those that do not. b. Identify situations where a heuristic solution may be more appropriate.
- *EU IOC-2 - The use of computing innovations may involve risks to your personal safety and identity.*
  - LO IOC-2.B - Explain how computing resources can be protected and can be misused.

Essential Questions

- How are programs developed to help people, organizations or society solve problems?
- How is cybersecurity impacting the ever increasing number of Internet users?

Teacher Resources

Student computer usage for this lesson is: **optional**

In the Lesson Resources folder:

- Lesson slides
- Worksheet for Key Exchange Activity
- Script for Public Key Encryption 3 Act Play

Lesson Plan

Session 1

Getting Started (5 min)

Students should answer the following questions in their journals:

- What types of online activities require information to be kept secret when it is transmitted?
- How does cryptography allow for information to be kept secret when it is transmitted?

Introduction to Content (15 min)

Suggested Review

- Have students present their solutions to the "Computer Encryption" homework from Lesson 2-12 and/or connect back to the previous lesson by posing the question: "Do you think computers actually use the encryption algorithms we learned last class?"
  - This discussion should lead to the question of what algorithms computers actually use. In the 1970s, the US government chose DES as the standard encryption algorithm that everybody could use. It has been updated to AES, which is a stronger algorithm, but DES and AES are very similar.
  - The teacher should make the point that at a high level, DES/AES are symmetric encryption algorithms that work on the same basic principle of the simple algorithms we looked at in the previous lesson.
  - The teacher can leave it at that, or optionally present some brief details on DES/AES. One option is to show the first minute or two of this visualization video and talk over it: http://youtu.be/mlzxpkdXP58 (http://youtu.be/mlzxpkdXP58)

Motivation: Present the Key Distribution Problem:

Introduce the following topic. Allow for discussion among the class about possible solutions to the problem presented.

- Alice wants to send Li some secret information over the Internet. We know that she can encrypt the information before sending it, but how will Li know what key Alice used to encrypt the message?
- This is called the **Key Distribution Problem** and it has been around as long as encryption has. A whole business was developed around this challenge: people were paid to go around the world delivering briefcases full of encryption keys. This distribution process obviously can be very expensive and is completely unpractical for the average person. For a long time, nobody thought that the key distribution problem could be solved algorithmically.

After the class has come up with some ideas, reveal a solution to the problem that was found using math.

Present Key Information: Dreamers to the Rescue – Two men, two solutions, one important mathematical idea.

- Despite everybody telling them they were crazy and hopeless, Martin Hellman and Whitfield Diffie teamed up to try to solve the Key Distribution Problem. Amazingly, they each came up

with a solution, both of which can be used to solve the problem.

- **Introduce One-Way Functions**: Both solutions use a mathematical concept called “one-way functions”. Most functions we are familiar with are “two-way": that is, they can easily be applied in either a forward or a reverse direction. For example, if f(x) = 2x, then it is easy to see that f(5) would be 2(5) or 10. It is also easy to see that if f(x) = 10, then 2x = 10, so x must be 5. One-way functions are different in that they are easy to use in one direction, but are very hard to reverse.
- Key Distribution – Solution #1 – Hellman’s Idea – Key Exchange Protocol

Guided Activities (25 min)

Analogy (10 min)

1. To help with the explanation of the topic, start with an analogy that uses different colors of paint.
    - Show video https://www.youtube.com/watch?v=YEBfamv-_do (https://www.youtube.com/watch?v=YEBfamv-_do) [2:25 - 4:20]
    - Alternatively, use paint to demonstrate the process live in the classroom!
2. The real system relies on a mathematical operation called *modulus* (or *clock arithmetic*), which is when you divide two numbers and find the remainder.
    - Use a clock to visually demonstrate the operation. (The number mod 12 gives you the time)
    - Show how to do modulus by using either long division, a calculator, or Google. (Consider this: If you know the number you divided by, and you know the remainder, can you easily figure out what the original number was?)
    - Alternatively, show the next section of the video: https://www.youtube.com/watch?v=YEBfamv-_do (https://www.youtube.com/watch?v=YEBfamv-_do) [4:20 - 6:18]

The system also uses powers (base/exponent). Very briefly review power notation.

Group Activity (15 min)

1. Students are paired up, and then join another pair to form a group of four.
2. Using either a set of clear directions or an online widget, one pair performs the key exchange using the Y^X(mod P) expression, while the other pair listens in. They then switch roles. They should see that the key is established while sharing information publicly, but the key itself is kept secret.

Wrap Up (5 min)

Students should answer this question in their journals:

- How can two people establish a shared secret in public?

Suggested Homework:

Research Hellman and Diffie’s work on public-key exchange, identify the big ideas of CS Principles that show up, and provide specific examples of how they are related to what you find out about Hellman and Diffie's work. Alternately, read about the British group that developed the same solution as Hellman and Diffie's to public key encryption in secrecy (http://cryptome.org/ukpk-alt.htm (http://cryptome.org/ukpk-alt.htm)).

Session 2

Getting Started (5 min)

Students will read the following question and record their thoughts in their journals:

- Whitfield Diffie said that he wanted to solve the key distribution problem for benefit of "ordinary people," as opposed to just governments and corporations. How do you and I benefit from his team's solutions to the Key Distribution Problem?

Have students present ideas from their journal entries. Use this as a way to review the Key Distribution Problem, and the team that tackled the problem.

Introduction to Content (5 min)

Present Diffie's Solution - Public Key Cryptography

- **The Idea**: Encrypt with one key (public key), decrypt with a second key (private key)
- For further clarification, use this analogy:
  - Analogy with Physical Locks – Person B gives out open padlocks (public key) to anybody who wants to send him or her something secret. Person A just puts the secret in a box, and shuts the padlock (easy to do!). When Person B receives the box, they use the combination (private key) to unlock it.
- This is called "**Asymmetric Encryption**" since it uses two different keys.
- Consider what happens when you go to a "secure" website to check out when you are finished shopping at an online store. Your browser says "https" and some show a picture of a lock. The system, called SSL (Secure Sockets Layer) or the updated version TLS (Transport Layer Security) takes advantage of Diffie's system.

Guided Activities (35 min)

Part 1 (20 min) - Role Play

Have students act out three short scenes (see "Public Key Encryption Plays") in order to illustrate how the system works. (It is advisable to select "dramatic" students to fill the four roles.)

Roles

- Customer
- Store
- Store Impersonator
- Certificate Authority

Overview

- Act 1: The customer and store use public key encryption to complete an online purchase using a credit card. (All seems well, but the next act will have a twist!)
- Act 2: The store impersonator distracts the store and jumps in, steals the credit card info. (After this, stop for a minute and ask the students to explain what the problem is)
- Act 3: Repeat Act 2, except that now the customer asks the Certificate Authority to verify the public key. The impersonator is revealed as a fraud, then the real store completes the transaction with the CA verifying.

Follow Up question to ask the students: Who do you have to trust for this system to work? (2 min)

- Sample Answer: The Certificate Authority. You are trusting that they are giving you valid information so you can verify the identity of others. (A student may ask how you know the certificate authority is not being impersonated. The answer is that the public key of the certificate authority is saved in your browser so you can verify their identify yourself.)

Optional Section on Mathematical Foundation

What are the mathematical details that enable this idea of work? (Don't worry, we are not going to fully answer this!)

- Diffie didn't actually figure out the math to make this actually work, he just had the key idea (Example of Abstraction!) He put the idea out there for others to figure out the details of the math that would make it work (Example of Collaboration!)
- One system (RSA) multiplies prime numbers as part of the one way function. It is easy to multiply two prime numbers, but it is very hard to determine the factors of the product (if you didn't already know them).
    - Give the students a couple of problems to illustrate this.
    - The two primes that you multiply are essentially the "private key". The product is the "public key".
    - This works in practice because the numbers used are huge, making the factoring process extremely difficult and time consuming, even with a large amount of computational power.

Discussion: Do "Open Standards" make sense in the world of Cryptography?

The systems of encryption used on the web have been "standardized" (meaning that everyone agrees to use the same systems) so that computers all over the world can communicate with each other. These standardized systems could be "proprietary" (meaning the details are kept secret), or they can be "open" (meaning the details are shared for anybody to see).

Part 2 (15 min) - Think-Pair-Share

Students will Think-Pair-Share about the following prompts:

- If cryptography is all about secrecy, then does it make sense to have open standards of encryption? List all the pros and cons that you can think of for open standards.
- Open standards fuel the growth of the Internet. Why? (consider both hardware and software)

Possible responses

Benefits of open encryption

- People can independently verify that the algorithm is strong, secure, and doesn't have vulnerabilities.
- People can make sure there are no "back doors" in the algorithm that let certain people spy on them even without the key.

Benefits of open standards

- The bigger picture: Open Internet standards are the cornerstone of the Internet's success. They enable its existence, facilitate its growth, and provide a platform that supports creativity, as well as social and economic opportunity for its billions of users. Open standards are implemented around the world in all kinds of Internet products and services.
https://www.internetsociety.org/policybriefs/openstandards
(https://www.internetsociety.org/policybriefs/openstandards)

Note: Heartbleed vulnerability is a good example of something that was eventually caught because of open standards. (This could be a homework assignment to read about it)

Drawbacks

- Any cyber-criminal can look at the algorithm and try to find a vulnerability to exploit.
- People may assume that because it is open, all the vulnerabilities have been found and plugged when that is not necessarily true.

Wrap Up (5 min)

Students should read this question and record their thoughts in their journals:

- "Open standards result in strong security". Do you agree or disagree with this statement? Give specific reasons to back up your position.

Optional Homework:

Read about Heartbleed vulnerability in SSL. Reflect on how open standards relate to this.

Extensions:

RSA Encryption Algorithm Video: http://youtu.be/M7kEpw1tn50 (http://youtu.be/M7kEpw1tn50)

Evidence of Learning

Formative Assessment

The teacher will observe and evaluate student responses to journal entries, class discussion questions, and class activities.

 (http://www.umbc.edu/)  (http://www.umd.edu/) 

(http://www.nsf.gov/)

Authored by: CS Matters in Maryland
Website: csmatters.org (http://csmatters.org)
Email: csmattersinmaryland@gmail.com (mailto:csmattersinmaryland@gmail.com)