

CS 51 Computer Science Principles

APCSP Module 3: Data, Internet, Computer and Programming

Unit 5: Global Impacts



LECTURE 8 SECURITY

DR. ERIC CHOU

IEEE SENIOR MEMBER

Objectives

- Safe Computing
 - Issues
 - Authentication
 - Encryption
 - Additional Measures for Safe Computing



Data Security

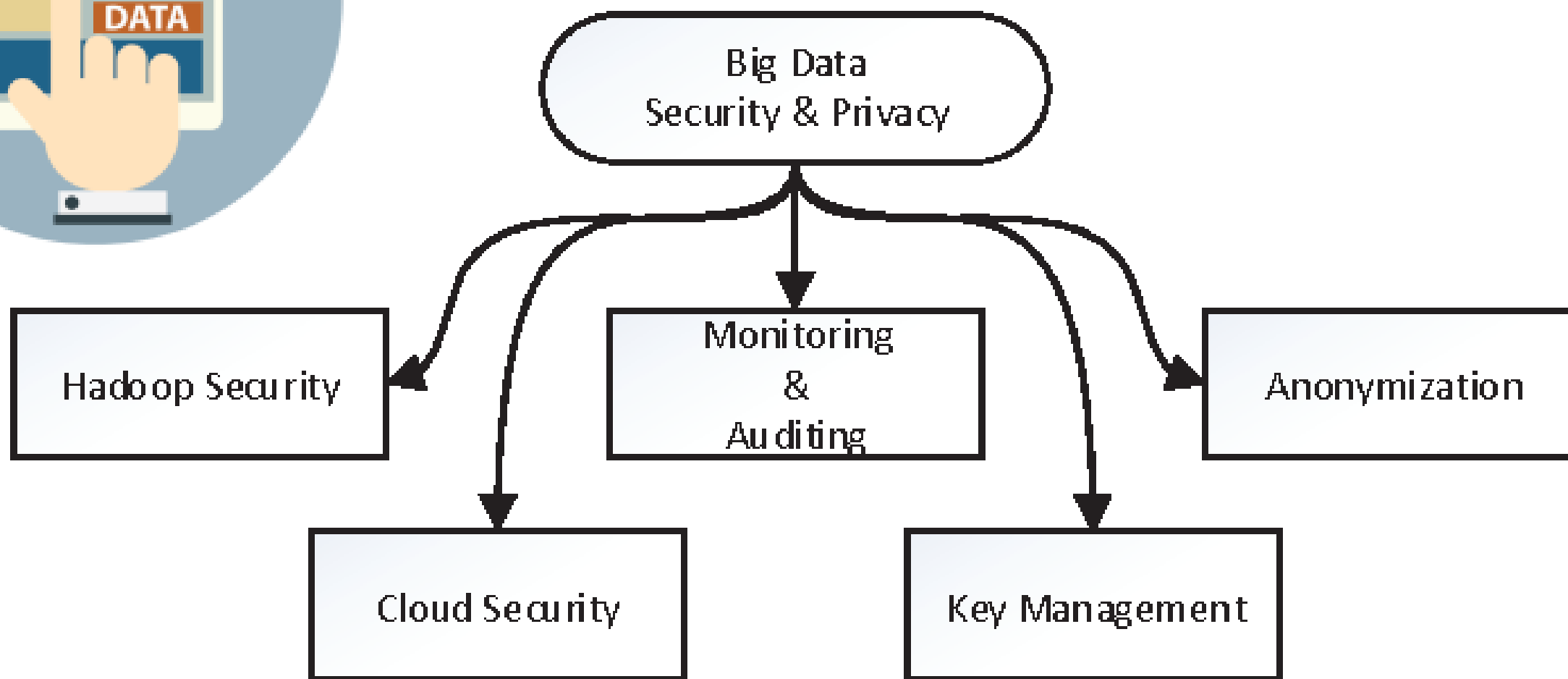
LECTURE 1

Data Security

- We've spent a lot of time looking at potential benefits of collecting and analyzing data. As we've already seen today, however, there are some risks associated with collecting all of this information.
- If it falls into the wrong hands or is used in ways we didn't intend, there may be serious risks imposed on our privacy or security. We're going to start looking more deeply at this problem.

Data Security

- In the **data breaches** we just looked at, some fairly important pieces of information were stolen. Credit card numbers, passport information, or government security clearances are obviously not something we'd like to fall into the wrong hands.
- Other pieces of information, however, don't seem that bad. So what if people know your ZIP code? So what if people know your birthday? This is information we usually share without a second thought.





The Cost of Free

ACTIVITY

Objectives

- Explain **privacy concerns** that arise through the mass collection of data
- Use online search tools to find and connect information about a person or topic of interest.
- Explain how multiple sources of data can be combined in order to uncover new knowledge or information.
- Analyze the **personal privacy and security concerns** that arise with any use of computational systems.



Brightest Flashlight Free ®

Version 2.4.2 can access



Location

- approximate location (network-based)
- precise location (GPS and network-based)



Photos/Media/Files

- read the contents of your USB storage
- modify or delete the contents of your USB storage



Camera/Microphone

- take pictures and videos



Wi-Fi connection information

- view Wi-Fi connections



Device ID & call information

- read phone status and identity

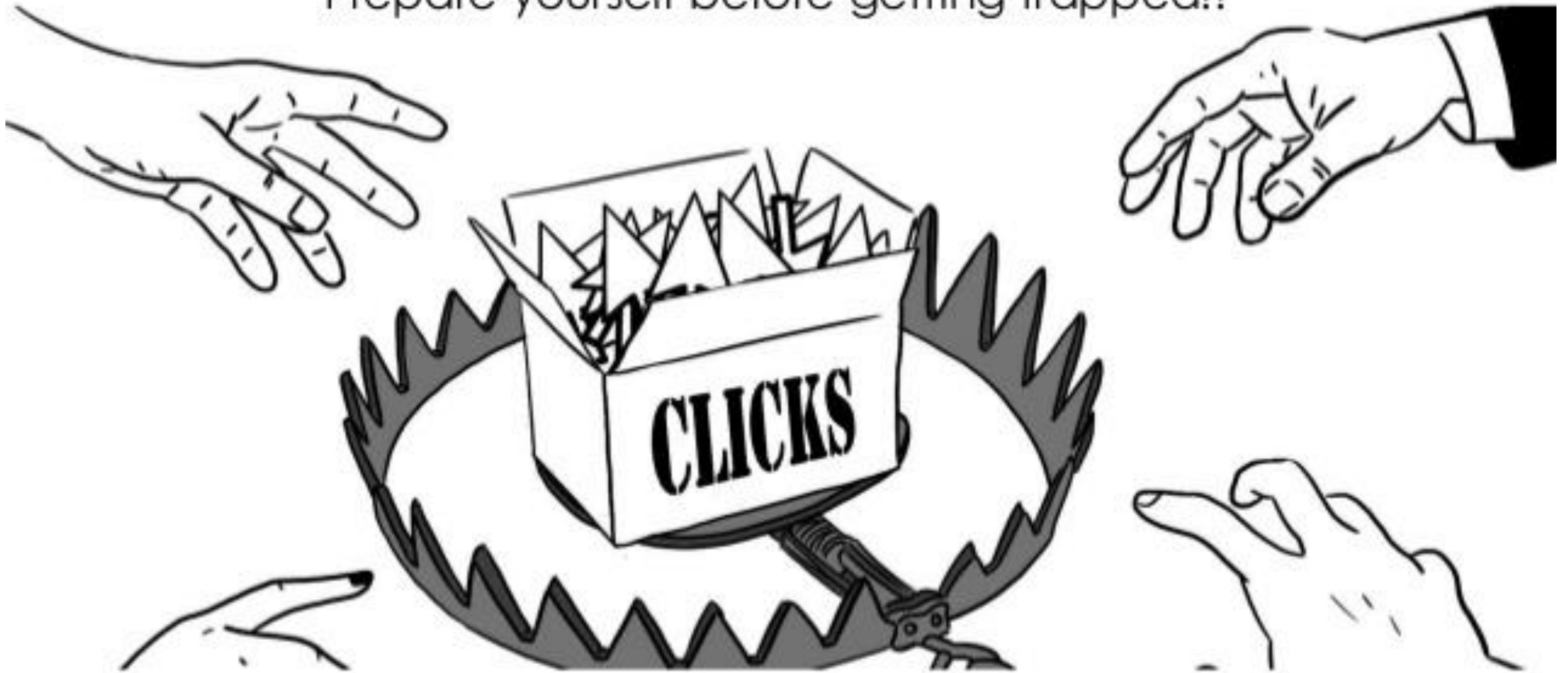
Updates to Brightest Flashlight Free ® may automatically add additional capabilities within each group. [Learn more](#)

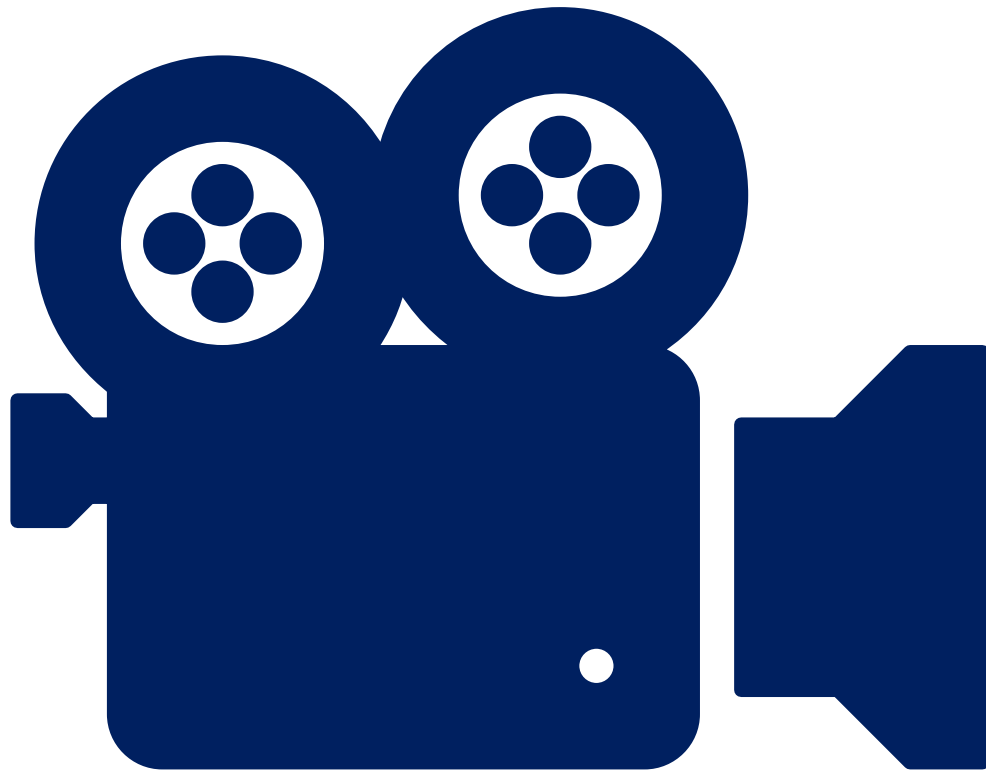


The Cost of Free

Do You know well on Digital Marketing??

Prepare yourself before getting trapped!!





Program or be Programmed

VIDEO -

[HTTPS://WWW.YOUTUBE.COM/WAT
CH?V=F8YTWOXJNTY](https://www.youtube.com/watch?v=F8YTWOXJNTY)

Discussion

- What do you know about data collected about you every day?

Get out some paper and a pen/pencil

- Write down 2 or 3 websites, web services, or apps that you use the most or rely on the most to stay connected to friends and family, or use for “productivity” like school work.

- **Education:** Code.org, Khan Academy, Codecademy.com
- **Social media:** Facebook, Twitter, Instagram, Snapchat
- **Online store:** Amazon, Target, Walmart
- **Search:** Google, Bing
- **Maps:** MapQuest, Yahoo Maps, Google Maps
- **Productivity:** MS Office Online, Google Docs
- **Mail & communication:** Gmail, Hotmail, Yahoo Mail, Skype, Google Hangouts
- **Streaming sites:** Netflix, Spotify, Pandora
- **Gaming sites:** Steam, Xbox Live
- **Banks and financial institutions:** Chase, Citibank

Does this help
jog your
memory?

Digital Traps

- Make a little table to compare side-by-side
- **Name of Website / Service**
 - Do you have an account, or need to login?
What kinds of data does (or could) this site potentially collect about you?
 - Do you know if this data is shared with other people, companies or organizations? (If so, which ones?)
 - Do you know how you would find out what data is collected or how it's shared?

Activity Guide - Privacy Policies

Choose a Website and Find the Data Privacy Policy

Choose an app, website, or other online service you are familiar with to research their privacy policy. The easiest way to find a data policy, if it exists, is to search for the company name followed by the terms “data policy” or “privacy policy.”

Your website: _____

Activity Guide - Privacy Policies

What Is Their Data Policy?

Respond to the questions below. Even if you can't find information, you should record where you looked and the fact that you can't find it. If there isn't a policy or it's hard to find, that can be just as interesting as seeing the policy itself.

- **What kinds of data are being collected? How many different kinds of data?**
- **What service or feature is enabled by the data they are collecting? Why are they collecting it in the first place?**
- **Who else is given access to that data? How are they using it?**
- **Can you get access to your own data? Can you modify what is collected or used, or delete your data if you wish?**

Activity Guide - Privacy Policies

Bottom Line: on a scale of 1-4, rate how comfortable you are with this company's data policy? Give your rating (no going halfway - no 2.5 or 1.5 - make a choice!) and then justify your choice.

1

very uncomfortable

2

uncomfortable
(but maybe fixable)

3

comfortable
(maybe minor
concerns)

4

very comfortable

Articles in the news

Leaning Pro-Utility	Leaning Pro-Privacy
1. <u>Wall Street Journal: It's Modern Trade: Web Users Get as Much as They Give</u>	1. <u>Apple: A Message to Our Customers (Apple challenges order to give government data about terrorist shooter)</u>
2. <u>CNN: Despite Facebook, privacy is far from dead</u>	2. <u>CNN: The Internet is a surveillance state</u>
3. <u>ZDNet: A case against online privacy</u>	3. <u>CNN: Google knows too much about you</u>
4. <u>U.S. News: The Case for Internet Surveillance</u>	4. <u>TechRepublic: Why "Nothing to Hide" misrepresents online privacy</u>
5. <u>Kaspersky: 10 Cool Big Data Projects</u>	5. <u>Huffington Post: The Case Against Monitoring Teens Online</u>
6. <u>Fortune: Boston is using big data to solve traffic jams</u>	6. <u>Politico: We Are All Big Brother Now</u>
7. <u>Maclean's: The real reason crime is falling so fast</u>	
8. <u>U.S. News: Relax and Learn to Love Big Data</u>	
9. <u>LinkedIn: The Ethics of Privacy: The Benefits of Data Gathering</u>	

Personally Identifiable Information

A key tenet of safe computing is protecting your **personally identifiable information**, or (PII). This is information that can be used to identify you and includes your:

- Age
- Race
- Phone Numbers
- Medical information and biometric data (fingerprints, eye scans)
- Financial Information
- Social Security number

Various other pieces of personal data, such as your location, cookies, and browsing history, can also be used to find your personal information.

Other Ways of Getting Info

- Search engines can track your search history and use it to suggest websites and search phrases. They can also show you ads based on your search history, part of a process known as **targeted marketing**.
- Devices, websites, and networks can collect information about a user's location, such as recording the **IP address** of the devices they use.



Safe Computing

LECTURE 3

Objectives

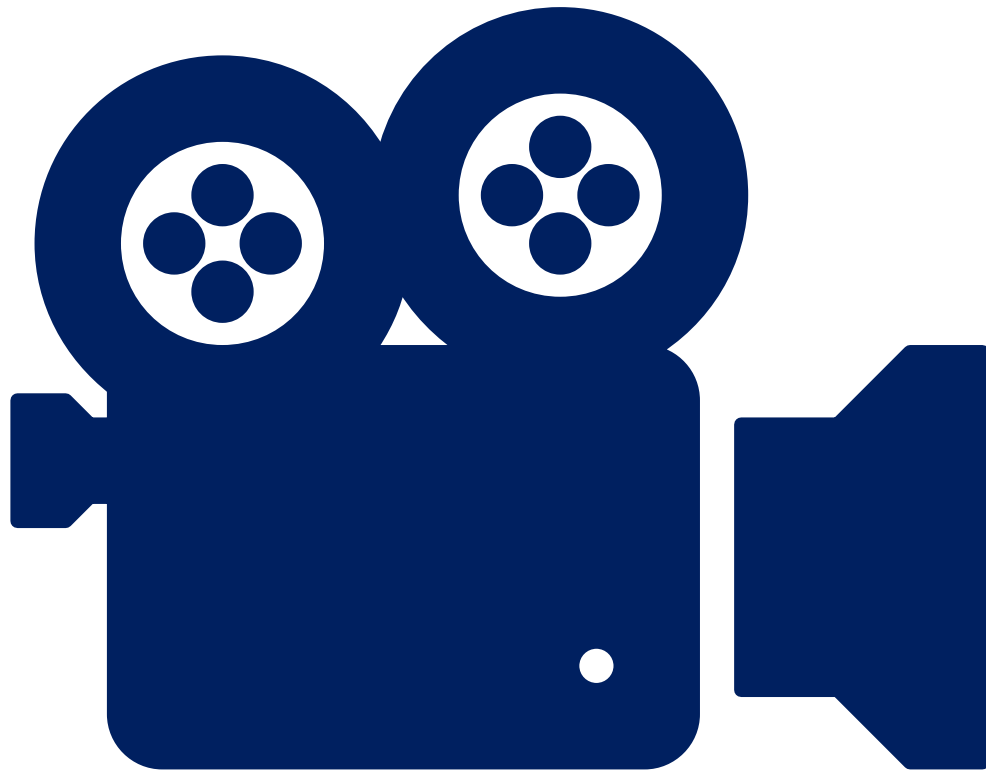
- Explain the characteristics of a phishing attack
- Explain how a DDoS attack works
- Describe how one computer virus works
- Research and describe a cyber attack found in the news
- Reason about the threats posed by, and methods of recourse for, various types of cyber attacks
- Describe plausible storage, security, or privacy concerns for particular pieces of data

Vocabulary

- **Antivirus Software** - usually keeps big lists of known viruses and scans your computer looking for the virus programs in order to get rid of them.
- **DDoS Attack** - Distributed Denial of Service Attack. Typically a virus installed on many computers (thousands) activate at the same time and flood a target with traffic to the point the server becomes overwhelmed.
- **Firewall** - software that runs on servers (often routers) that only allows traffic through according to some set of security rules.

Vocabulary

- **Phishing Scam** - a thief trying to trick you into sending them sensitive information. Typically these include emails about system updates asking you send your username and password, social security number or other things.
- **SSL/TLS** - Secure Sockets layer / Transport Layer Security - An encryption layer of HTTP that uses public key cryptography to establish a secure connection.
- **Virus** - a program that runs on a computer to do something the owner of the computer does not intend.



The Internet: Cybersecurity and Crime

VIDEO -

[HTTPS://YOUTU.BE/AUYNXGO_F3Y](https://youtu.be/AUYNXGO_F3Y)

Topics

You are going to watch a video touches on a number of topics that you might choose to research later:

- DDoS Attacks (and Bot Nets)
- Cyber warfare
- Viruses and Anti Virus Software
- Phishing Scams
- Credit Card theft
- Types of people who commit cybercrimes



Malware and Virus

LECTURE 4

Virus

- Your computer might become infected with a **virus** or a **worm**. A virus is a malicious program. It's called a virus because, like a real virus, it can gain unauthorized access to something and then copy itself. Viruses are attached to infected files and must be activated by the user while worms can operate independently.
- In 2000, the ILOVEYOU virus, named for the fake love-letter email it attached itself to, caused over ten billion dollars of damage across the world. In 2017, the WannaCry worm attack caused a similar amount of damage by encrypting hard drive files and holding them for ransom.

Malware

- Computer viruses are a type of malware. **Malware**, short for malicious software, is intended to damage or take partial control over a computing system. It also includes ransomware and adware.

Phishing

- Scammers online can take advantage of human error to gain potentially harmful information. **Phishing**, for example, works by tricking users into providing their personal information by posing as a trustworthy group.
- For example, you might get a fake email from someone pretending to be your bank that says your credit card or bank account has an issue and they need your username and password to fix it. This information can then be used for a variety of misdeeds.

Keylogging Technology

- Scammers can also take advantage of **keylogging technology**, recording your keystrokes to gain access to sensitive information like passwords.

Rogue Access Point

- The information you send over public networks, like the Wifi network at a coffee store, has the potential to be intercepted by those with harmful ends. One of the ways this can happen is through a **rogue access point**, which gives unauthorized access to a secure network.

Practice Safe Computing

- A key way to practice safe computing is to be wary. You never want to open or click any links in an email that you don't recognize the sender of. (Hackers can also gain access to people's accounts, so also **be wary** if you get a strange message from a friend.) Furthermore, be careful about what you download onto your devices; only download from websites you trust.
- Fortunately, these concerns haven't gone unnoticed, and today there are many systems in place to help protect you on the internet.



Authentication

LECTURE 5

Authentication Measures

- **Authentication measures** keep people from gaining unauthorized access to your accounts. We're going to look at two of them here: making a strong password and implementing a multi-factor authentication method.

Passwords

- A **strong password** is a password that's easy for you to remember but difficult for someone else to guess, regardless of how well they know you. You don't want to use a generic phrase to create your password ("password," "12345,") or something that could be easily guessed at (your name, the name of your family members, etc.) Strong passwords often use a variety of characters, such as uppercase letters, numbers, and symbols (M4r13_cur13).
- [This website](#) can help you determine how strong your password is, and also highlights what makes a password weak or strong.
- You're mostly in charge of creating your own strong passwords, although many companies have implemented requirements for passwords to make them stronger. (They may require you to have a capital letter in your password, for example, or a symbol).

Multifactor Authentication

On the other hand, **multifactor authentication** is provided by the website you're using, although you can generally choose to opt in or out of it. Multifactor authentication is a way to control who gets access to your accounts by requiring *multiple* (at least two) methods of verification.

Typically, these proofs will fall into one of three categories, and they'll usually be in two separate categories.

- **Knowledge:** this is something you know, like a password or PIN number. This can also include verification questions. (What's your favorite food? Where were you born?)
- **Possession:** this is something that you have or own, such as a USB drive or an access badge. This can also include one-time passwords sent to a different device like your cell-phone.
- **Inheritance:** this is something that you own *intrinsically*, like your fingerprints or voice.

Multifactor Authentication

- A multifactor authentication system can provide multiple verification options for user convenience, as well as security. For example, a multifactor login method used for your email account might let you choose between sending a verification code to another email or to your phone in order to get in. That way, if you don't have your phone on-hand, you can still get into your account.
- The more layers of verification you have, the more secure your account generally is, although there are limits and exceptions to the rule.

Authentication

- Password
- Captcha
- Fingerprint recognition
- Facial Recognition
- Eye Iris Recognition

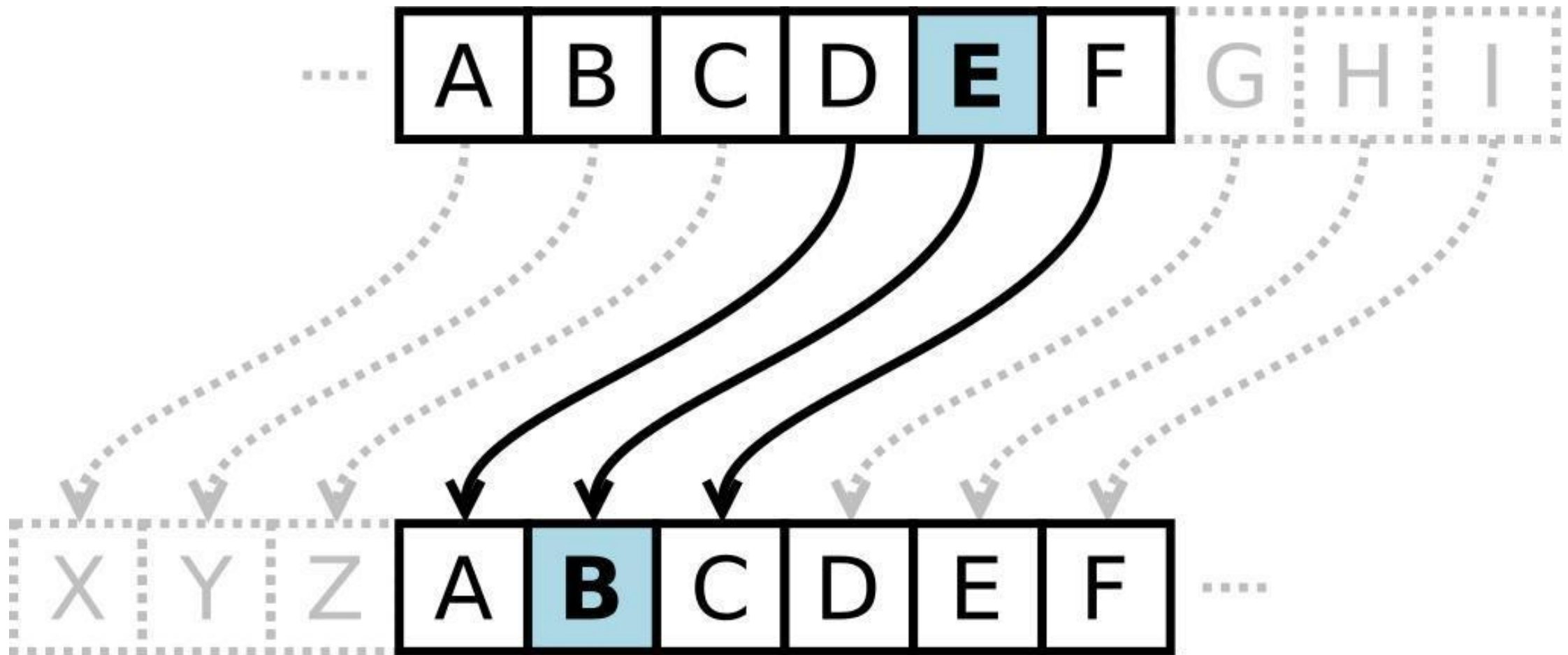


Encryption

LECTURE 5

Encryption

- **Encryption**, another way of protecting people's data, is the process of encoding data to prevent unwanted access. (**Decryption** is the process of decoding data.) Traditionally, encryption was used to send and receive secret messages between spies or military generals. Coding mechanisms like the Caesar Cipher and the French Great Cipher became famous.
- Both of these encryption methods use a **key**, or a secret piece of information, to keep their messages secret. Only the person the message is intended for should know the key.
- For example, the Caesar Cipher works by shifting all the letters in a message down or up a given alphabet. In this case, the key is the number of letters that the message is shifted by. In the image below, all the letters are shifted up by 3: E becomes B, D becomes A, and so on. Therefore, the key is 3.



Encryption Approaches

Two common approaches to encryption are:

- **Symmetric key encryption**, which uses one key for both encrypting and decrypting code.
- **Public key encryption**, which uses a public key to encrypt but a private key to decrypt the message.

 Check out [this encryption overview](#), courtesy of [Code.org](#)!

Digital Certificates

- The public key encryption system relies on **digital certificates**. These are issued by **Certificate Authorities** (CAs) to trusted sites. They allow other computers to verify that a website is who they say they are. These certificates are essential to the public key encryption system because they foster trust between websites. Think of the certificates to be a little like the signature on a check—once we see that signature, we know that the check is trustworthy.
- A **trust model** is used in order to determine if a digital certificate itself is legitimate. (You won't have to understand how these models work for the AP test.)



Additional Measures

LECTURE 6

Other Ways to Foster Safe Computing

- Regular software updates help to patch up any errors or vulnerabilities that were previously undetected in the code.
- Computer virus and malware scanning software can help protect your computer. Some famous brands are Norton and McAfee.
- Firewalls, which monitor internet traffic and block websites deemed unsafe, can also help you protect your devices.
- Making backups of important data can help mitigate the effects of your hardware failing or a virus attacking.

Other Ways to Foster Safe Computing

- Knowing and controlling the permissions companies have to collect your data can empower you to decide what you're comfortable with.
- Keeping your devices out of unsafe locations helps prevent them from being physically stolen or hacked into.
- Being aware of internet connection security is also important. Free WiFi connections are often vulnerable to hackers.
- Finally, stay informed! Technology is ever changing, and staying aware of these changes will help you protect yourself.



Simple Encryption

LECTURE 7

Objectives

- Encryption is not just for the military and spies anymore.
- We use encryption everyday on the Internet, primarily to conduct commercial transactions, and without it our economy might grind to a halt.
- We will see what kind of thinking goes into this.

Vocabulary

- **Caesar Cipher** - a technique for encryption that shifts the alphabet by some number of characters
- **Cipher** - the generic term for a technique (or algorithm) that performs encryption
- **Cracking encryption** - When you attempt to decode a secret message without knowing all the specifics of the cipher, you are trying to "crack" the encryption.

Vocabulary

- **Decryption** - a process that reverses encryption, taking a secret message and reproducing the original plain text
- **Encryption** - a process of encoding messages to keep them secret, so only "authorized" parties can read it.
- **Random Substitution Cipher** - an encryption technique that maps each letter of the alphabet to a randomly chosen other letters of the alphabet.

Caesar Cipher Widget (Code Studio)

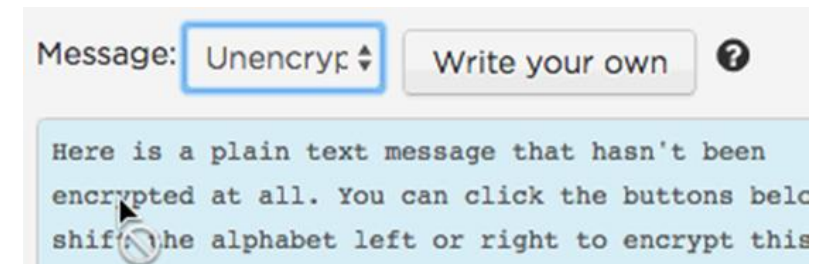
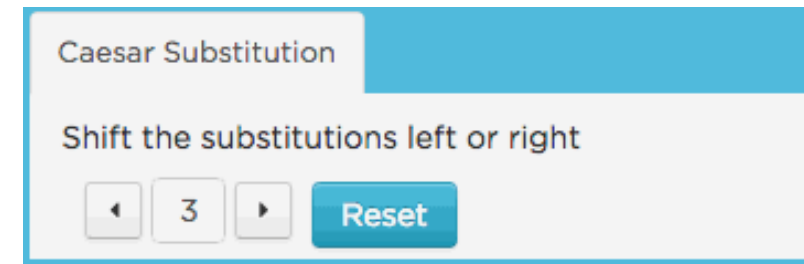
Crack a Caesar cipher!

This tool lets you play with text and do Caesar ciphers. You can use this to either encrypt a message or decrypt it.

Do this

- Load a Sample message from the message dropdown. This will load a message that has been encrypted with a Caesar cipher.
- Using the buttons in the Caesar substitution tab, you can shift the alphabet forwards or backwards to try to unscramble the message.

See how long it takes you to crack the cipher! Is this a good method of encrypting secret data?



Why Encryption?

- Recall some of the facts we learned in Unit 1 while using the Internet Simulator.
- The Internet is not inherently secure. Packets traveling across the Internet move through many routers, each of which could be owned by different people or organizations.
- So we should **assume all information** traveling across the Internet to be **public**, as if written on a postcard and sent through the mail.

Your Secret

- In your daily life what things do you or other people rely on keeping a secret? Who are these secrets being kept from? How are these things kept secret?

Your Secret

- Some areas that need to be kept secret:
 - Social interactions (e.g., a surprise birthday party)
 - A play in a sports game, your hand in a card game
 - Personal identification information, PIN numbers, etc.
 - Business and government negotiations
 - Military activity

Secrecy

- Secrecy is a critical part of our lives, in ways big and small. As our lives increasingly are conducted on the Internet, we want to be sure we can maintain the privacy of our information and control who has access to privileged information.

Classic Encryption - The Caesar Cipher

Many of the ideas we use to keep secrets in the digital age are far older than the Internet. The process of encoding a plain text message in some secret way is called Encryption

Caesar Cipher

- For example in Roman times Julius Caesar is reported to have encrypted messages to his soldiers and generals by using a simple alphabetic shift - every character was encrypted by substituting it with a character that was some fixed number of letters away in the alphabet.
- As a result an alphabetic shift is often referred to as the Caesar Cipher.

Caesar Cipher

- This message was encrypted using a Caesar Cipher (an "alphabetic shift").
Let's see how long it takes you to decode this message (remember it's just a shifting of the alphabet):

serr cvmmn va gur pnsrgrevn

Caesar Cipher

- Answer:

free pizza in the cafeteria

the alphabet was shifted 13 characters

Code Studio

Get into code studio

Part 1 - Crack a Caesar Cipher

review vocabulary

Part 2 - Crack a Random Substitution Cipher

frequency analysis

Encryption

- Encryption is essential for every day life and activity
- The "strength" of encryption is related to how easy it is to crack a message, assuming adversary knows the technique but not the exact "key"
A random substitution cipher is very crackable by hand though it might take some time, trial and error.
- However, when aided with computational tools, a random substitution cipher can be cracked by a novice in a matter of minutes.

Substitution Ciphers

- Simple substitution ciphers give insight into encryption algorithms, but as we've seen fall way short when a potential adversary is aided with computational tools...our understanding must become more sophisticated.
If we are to create a secure Internet, we will need to develop tools and protocols which can resist the enormous computational power of modern computers.

Substitution Ciphers

- How much easier is it to crack a CAESar cipher than a random substitution cipher? Can you put a number on it?
- For Caesar's Cipher there are only 25 possible ways to shift the alphabet. Worst case, you only need to try 25 different possibilities. A random substitution cipher has MANY more possibilities ($26 \text{ factorial} = 4 \times 10^{26}$ possibilities). However, as we learned, with frequency analysis we can avoid having to try all of them blindly.

Substitution Ciphers

- Was it difficult to crack a Random Substitution cipher? Did it take longer than you thought? shorter? Why?
- Computational tools aid humans in the implementation of encryption, decryption, and cracking algorithms. In other words, using a computer changes the speed and complexity of the types of encryption we can do, but it also increases our ability to break or circumvent encryption.

Substitution Ciphers

- Any encryption cipher is an algorithm for transforming plaintext into cipher text. What about the other way around? Can you write out an algorithm for cracking a Caesar cipher? What about a random substitution cipher?
- An algorithm for cracking a Caesar cipher is pretty easy - for each possible alphabetic shift, try it, see if the words come out as English.
- An algorithm for cracking random substitution is trickier and more nuanced. There might not be a single great answer but through thinking about it you realize how tricky it is to codify human intelligence and intuition for doing something like frequency analysis into a process that a machine can follow. It probably requires some human intervention which is an interesting point to make.



Encryption with Keys and Passwords

LECTURE 8

Objectives

- Explain the relationship between cryptographic keys and passwords.
- Explain in broad terms what makes a key difficult to “crack.”
- Reason about strong vs. weak passwords using a tool that shows password strength.
- Understand that exponential growth is related to an encryption algorithm’s strength.
- Explain how and why the Vigenère cipher is a stronger form of encryption than plain substitution.
- Explain properties that make for a good key when using the Vigenère Cipher.

Vocabulary

- **Computationally Hard** - a "hard" problem for a computer is one in which it cannot arrive at a solution in a reasonable amount of time.
- **Venere cipher (Vee-zha-nair)** - a method of encrypting text by applying a series of Caesar ciphers based on the letters of a keyword.
- **Encryption algorithm** - it is some method of doing encryption.
- **Encryption key** - a specific input that dictates how to apply the method and can also be used to decrypt the message. Some people might say "What is the key to unlocking this message?"

Hacking Ciphers

Justification for the practice of cracking ciphers.

Here are some points:

- People in the field of counterterrorism make a living by trying to crack the codes of other nations. Many attribute the success of the Allies in WWII to our ability to crack the Enigma code and uncover the plans of the Germans.
- Others may try to crack more abstract codes that are not written by humans, searching for patterns within DNA models in order to understand their nature and be able to describe the nature of humanity.
- It's useful to try to crack your own codes to see how strong they really are. There are many other reasons related to mathematical exploration, pattern recognition, etc.

Hacking Caesar Cipher

- The Caesar Cipher is an encryption algorithm that involves shifting the alphabet
- The amount of alphabetic shift used to encode the message is the key
- When you are cracking the Caesar Cipher you are trying to figure out how much the alphabet was shifted - you are trying to discover the key.

Hacking Random Substitution Cipher

- If random substitution is an algorithm for encryption, what is the key to a random substitution cipher?
- The key is the actual letter-to-letter mapping that was used to encode the message - it can also be used to decrypt.

Importance of the Strength of Encryption

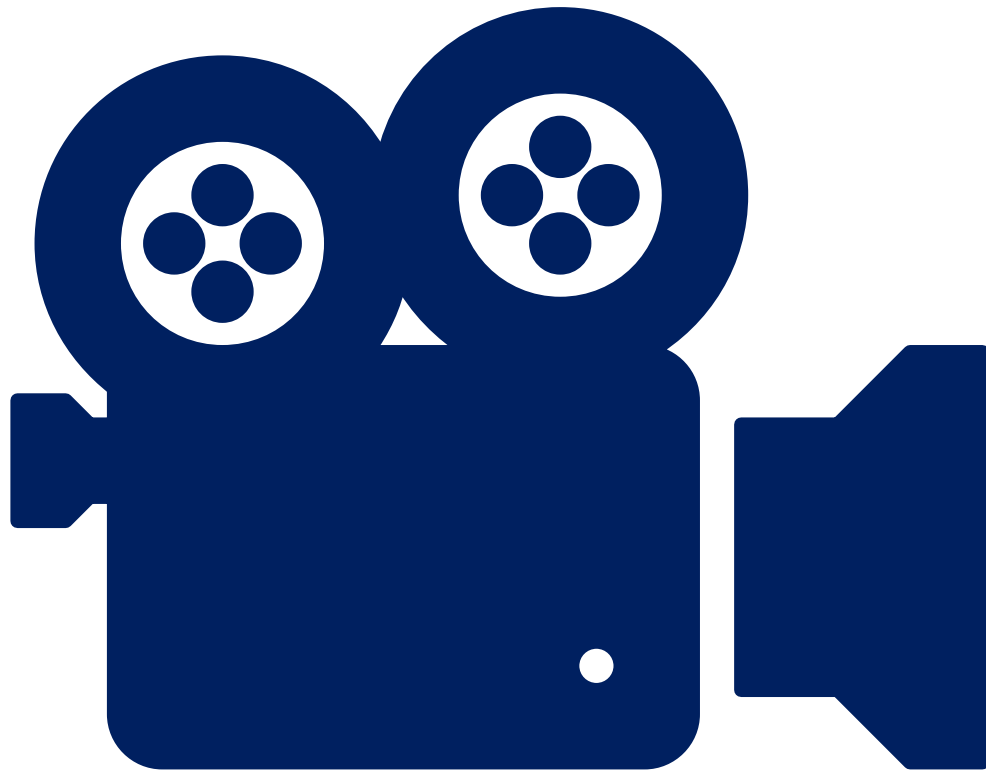
- There is a difference between the algorithm (how to execute the encryption and decryption) and key (the secret piece of information).
- In encryption you should always assume that your 'enemy' knows the encryption algorithm and has access to the same tools that you do.
- What makes **encryption REALLY strong** is making it hard to guess or crack the “key,” even if the “enemy” knows the encryption technique you're using.
- Today we'll learn a little more about it and about keys and their relationship to passwords you use every day.

Vigenère Cipher

Distribute: [Exploring the Vigenere Cipher Widget - Worksheet](#)

Students should click on the [The Vigenere Cipher - Widget](#)

Use the worksheet as a guide for exploring the widget.



Vigenère Cipher

VIDEO -

[HTTPS://YOUTU.BE/SKJCMCAHQSO](https://youtu.be/skjcmcahqso)

Vigenère Cipher

Part 1: Explore the Widget

Students are asked to:

- Jump into the tool and poke around

- Figure out what it's doing

- The worksheet gives a few directed tasks:

 - Encrypt a few different messages using different secret keys

 - Decrypt a message

 - Find a “bad” secret key

 - Find a “good” secret key

 - Try to decrypt without knowing the key

Properties of strong encryption

- Vigenere is strong because looking at the cipher text there are no discernable patterns assuming a good key was chosen.
- Because the cipher text is resistant to analysis, it leaves us simply having to guess what the key is.
- Even if we know the length of the key we might still have to try every possible letter combination which is a prohibitively large number of possibilities.

Vigenère Cipher

For a long time, the Vigenère cipher was considered to be an unbreakable cipher and was used by governments to send important messages.

But in the 1800s Vigenere was discovered to be susceptible to a modified form of frequency analysis. After that point it was considered insecure.

Still the properties of Vigenere that we've found are desirable.

Vigenère Cipher

Computationally Hard Problems -- How good is your password?

We know that a good encryption algorithm reduces the problem of cracking it to simply guessing the key.

We want the key to be Computationally Hard to guess - in other words, hard for a computer to guess.

Computationally Hard typically means that arriving at the solution would take a computer a prohibitively long time - as in: centuries or eons.

In terms of cracking encryption that means that the number of possible keys must be so large, that even a computer trying billions of possible keys per second is unlikely to arrive at the correct key in a reasonable amount of time.

Nowadays when you use a password for a website or device, your password is used as a cryptographic key.

So, choosing a good password is meaningful because we want the key to be hard for a computer to guess. How good is your password?..



How not to get hacked?

ACTIVITY

How not to get hacked?

Look at:

How Not to Get Hacked by Code.org (not in Code.org?)

How Not To Get Hacked



Tip #1: Look for the Lock

When browsing the web, always look at the address bar of the site you're on to see if it's protected.

If the URL address bar says HTTPS and shows a lock, that means any information you send is going on a secure line to the website you're visiting.

This means it's very likely OK to send private information or passwords. (Of course, you never know; somebody could've hacked the computers on the other end, in which case all bets are off.)



Tip #2: Check the URL

- Next, always make sure you're on the legitimate version of a website by checking the URL. Sometimes a web site might look like what you want, but it's a fake. How did you end up here?
- The main way people end up at fake web sites is by clicking on fake emails. This is called a phishing scam.
- A phishing scam is when you get an email from what seems like a trustworthy source, asking you to log in or download something, but the link goes to a fake site. If you log in, you've been tricked into giving away your password and now they have access to your real account.
- The one way to avoid these scams is to make sure the address on your browser matches the web site you think you're at - look for the first DOT COM followed by the slash. Also, look for the lock!



A LEGITIMATE BANK

ON A REAL WEBSITE

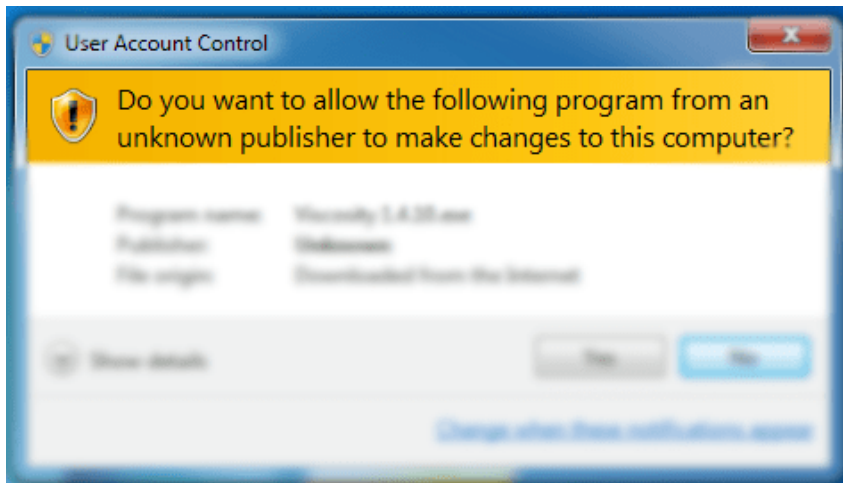
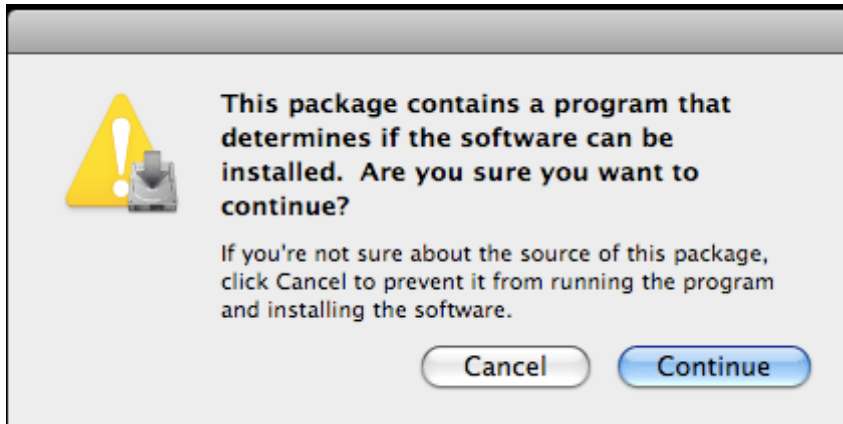
SIGN IN TO
CONTINUE

AWESOME_J

.....

**STEAL
INFORMATION**

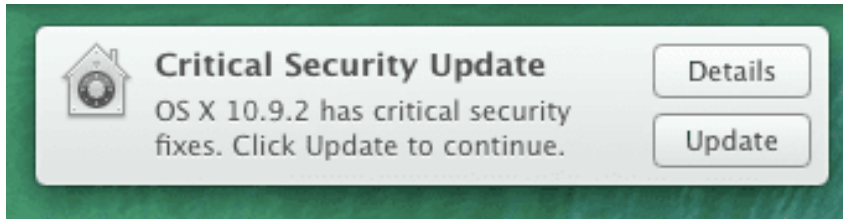
**STEAL
YOUR MONEY**



Tip #3: Only Download From Trustworthy Sources

- Whether you click on links in emails or you're just browsing the web or looking for games, you should take extra care when a web site asks you to download anything. This may lead you to install unwanted apps called viruses, or to add 3rd party browser extensions that snoop on your browsing habits.
- If you accidentally download something like this from the Internet, don't install it. Instead, only download software from verified, trustworthy sources.

Tip #4: Install Security Updates



- Sometimes your computer can get attacked even if you don't do anything, because of vulnerabilities in the system you're using.
- Whether it's Windows or Mac, Android or iPhone, or really whatever it is, ALL computer systems are prone to vulnerabilities. These openings allow attackers to install unwanted apps or access data in a way you didn't intend.
- Of course, the company who makes your computer or device doesn't want this to happen, so when a vulnerability is discovered, a patch to fix it is typically released as quickly as possible.

From:	To:	Secure?
gmail.com	gmail.com	SECURE
yourcompany.com	yourcompany.com	SECURE
gmail.com	anotherdomain.com	OPEN TO ALL EYES



Tip #5: Do NOT Email Private Data

- Even if there's a lock on your browser, not all the information you send and receive is private.
- Whenever you send email on the internet, unless you're sending it to somebody on the same email domain as you, your email is out in the open, available for anybody in the world to access. In fact, almost ALL the emails you send can be seen by third party hackers.

Tip #6: Use Strong Passwords



- Nothing you do online is safe unless you use strong passwords that actually protect your information.
- Most people use the same password everywhere, and their password is easy to guess. You'd be amazed how many people use the password "ABC123" or "12345". Using a password like this is basically like asking to be hacked.
- You may be advised to include special characters like exclamation marks or hyphens in passwords to make them stronger. This is helpful, but it's not enough.
- Passwords like "Rover2015" and "R0v3r2015" are actually the same strength. This is because their length is the same.



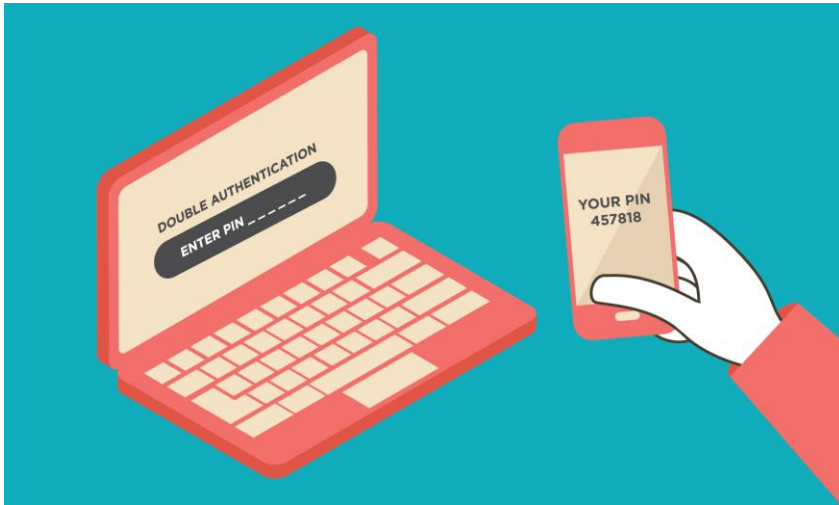
SOCIAL MEDIA

Tip #7: Use Multiple Passwords

In addition to creating strong passwords, you unfortunately must use a different password for each web site you use. If a hacker does get access to one of your passwords, you don't want them to get into ALL your accounts.

A few years back, hackers got access to EVERY password at a popular social networking site and they published all these logins online for anybody to see. If your login was published, anybody in the world can now access your account on any website where you use that same password.

Tip #8: Enable Two-Factor Authentication



This next one makes a big difference! Enable two-factor authentication wherever possible, especially for your most sensitive data -- like email, social media, or cloud storage accounts.

Two-factor authentication adds extra security to your password, so even if somebody knows your password, they need something else to log in as you. Usually this is a security code that's sent to your phone, which means to login somebody needs your password AND your phone. Most email or social networking sites offer this security feature. When they do, you should use it.



Tip #9: Do NOT Plug In Devices/Accessories From Strangers

One last piece of advice: don't plug in a device or accessory from a stranger. If somebody gives you a memory card for your computer or even a USB power cable for your phone, it could infect your device with a virus the moment you plug it in. The person giving it to you may not even know that their plug is infected.

Of course, sometimes you don't have a choice, and most of the time it's probably not a big deal. But you should be aware that anytime you plug something into your computer or device, you take a small risk.



Public Key Cryptography

LESSON 8

Objectives

- Explain what the modulo operation does and how it operates as a "**one-way**" function
- Follow an **asymmetric encryption algorithm** to encrypt a numerical message using the Public Key Crypto widget.
- Explain the difference between symmetric and asymmetric encryption.
- Describe the basic process of encrypting data using public key encryption
- Explain the benefits of public key cryptography

Vocabulary

- **asymmetric encryption** - used in public key encryption, it is a scheme in which the key to encrypt data is different from the key to decrypt.
- **modulo** - a mathematical operation that returns the remainder after integer division. Example: $7 \text{ MOD } 4 = 3$
- **Private Key** - In an asymmetric encryption scheme the decryption key is kept private and never shared, so only the intended recipient has the ability to decrypt a message that has been encrypted with a public key.

Vocabulary

- **Public Key Encryption** - Used prevalently on the web, it allows for secure messages to be sent between parties without having to agree on, or share, a secret key. It uses an asymmetric encryption scheme in which the encryption key is made public, but the decryption key is kept private.
- **symmetric encryption** - an encryption scheme in which the key used to encrypt data is also used to decrypt (contrast with: asymmetric encryption)
symmetric encryption - an encryption scheme in which the key used to encrypt data is also used to decrypt (contrast with: asymmetric encryption)
- **RSA encryption algorithm** - A user of RSA (Relatively Slow Algorithm) creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret.

How can we encrypt the message so that it is hard to hack?

How can two people send encrypted messages back and forth over insecure channels (the Internet) without meeting ahead of time to agree on a secret key? How can two people send encrypted messages back and forth over insecure channels (the Internet) without meeting ahead of time to agree on a secret key?



Modulo Arithmetic

ACTIVITY

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modulo 7

$$3^1 = 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod{7}$$

$$3^2 = 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod{7}$$

$$3^3 = 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod{7}$$

$$3^4 = 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod{7}$$

$$3^5 = 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod{7}$$

$$3^6 = 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod{7}$$

$$3^7 = 2187 = 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod{7}$$

Modulo 7

Observation

Message ^{Key} mod **Prime Number** = **Encrypted Message**

1. **Message** ^{Key} can spread out the message to a unknown encrypted message field.
2. The larger the **Prime Number**, the wider the encryption field.
3. Key can be any non-zero number

Encryption

- $c \equiv m^e \pmod{n}$

Decryption

- $m \equiv c^d \pmod{n}$

c=Cipher Text

m=Message Text

e=Public Key

d=Private Key

n=P * Q (already Calculated)

Principles of Encryption using Prime Modulo

There are two main principles we want to understand:

1. The **mechanics** of communication with public key cryptography
2. The basic **mathematical principles** that make it possible



Public-Key Encryption

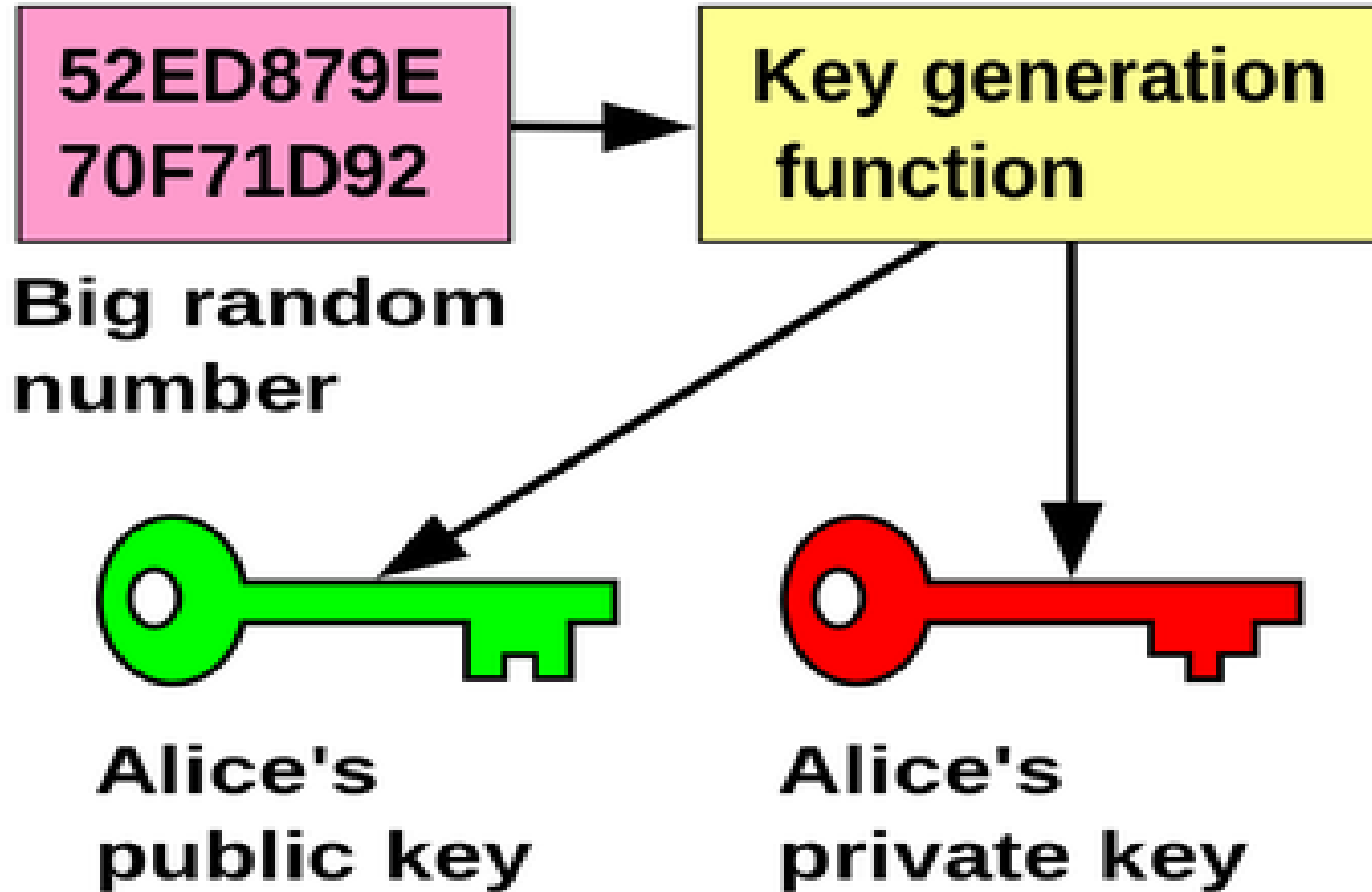


Introduction to Number Theory

- **A prime number** is an integer that can only be divided without remainder by positive and negative values of itself and 1. Prime numbers play a critical role both in number theory and in cryptography.
- **Two theorems** that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem.
- **An important requirement** in a number of cryptographic algorithms is the ability to choose a large prime number. An area of ongoing research is the development of efficient algorithms for determining if a randomly chosen large integer is a prime number.



Alice



RSA public key encryption

p: prime number

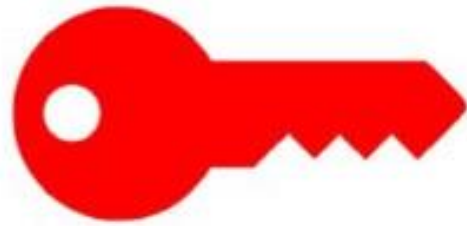
q: prime number

n = pq

$$\phi(n) = (p-1)(q-1)$$

d: $0 < d < n$ and $\gcd(d, \phi(n)) = 1$

e: $de \bmod \phi(n) = 1$



private key

(d, n)



public key

(e, n)

Large Enough $n = p \cdot q$

	12,313	Prime Number 1
X	45,613	Prime Number 2
	<u>561,632,869</u>	Product

Activity Guide - Multiplication + Modulo

Step 1: Experiment with the Mod Clock

Step 2: Toward encryption - Use multiplication to produce inputs

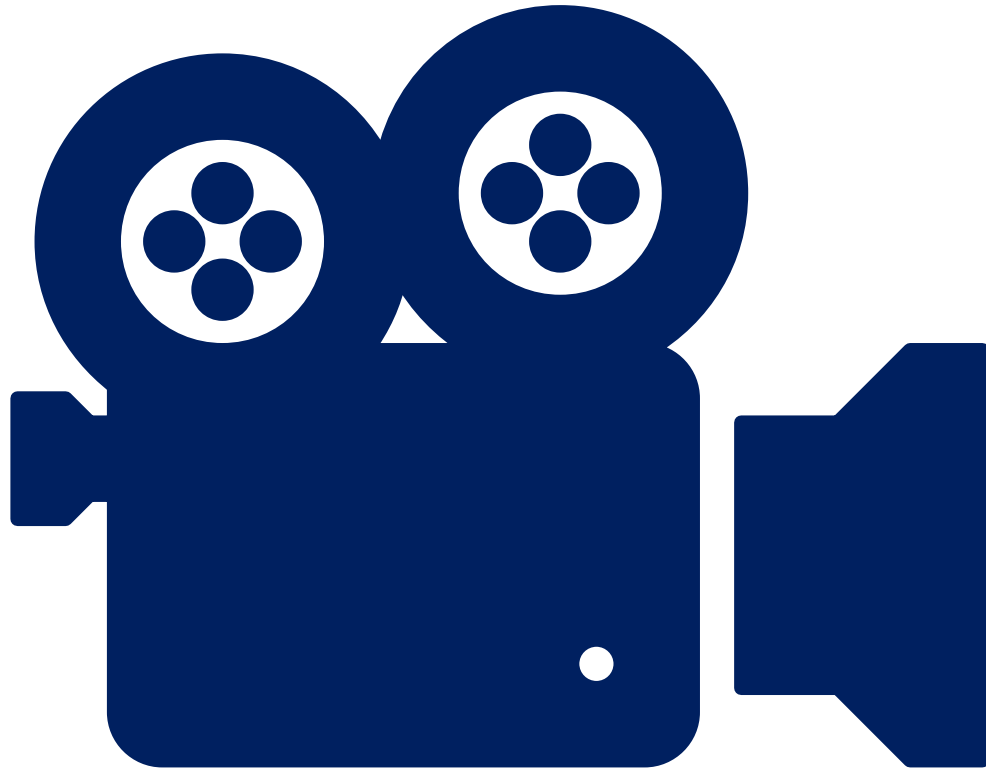
Activity Guide

https://docs.google.com/document/d/1JRWUKPI_3Pd6UUDub6aQ3hhUbb5HPioqJl2K4ipbRe0/edit



Public Key Cryptography

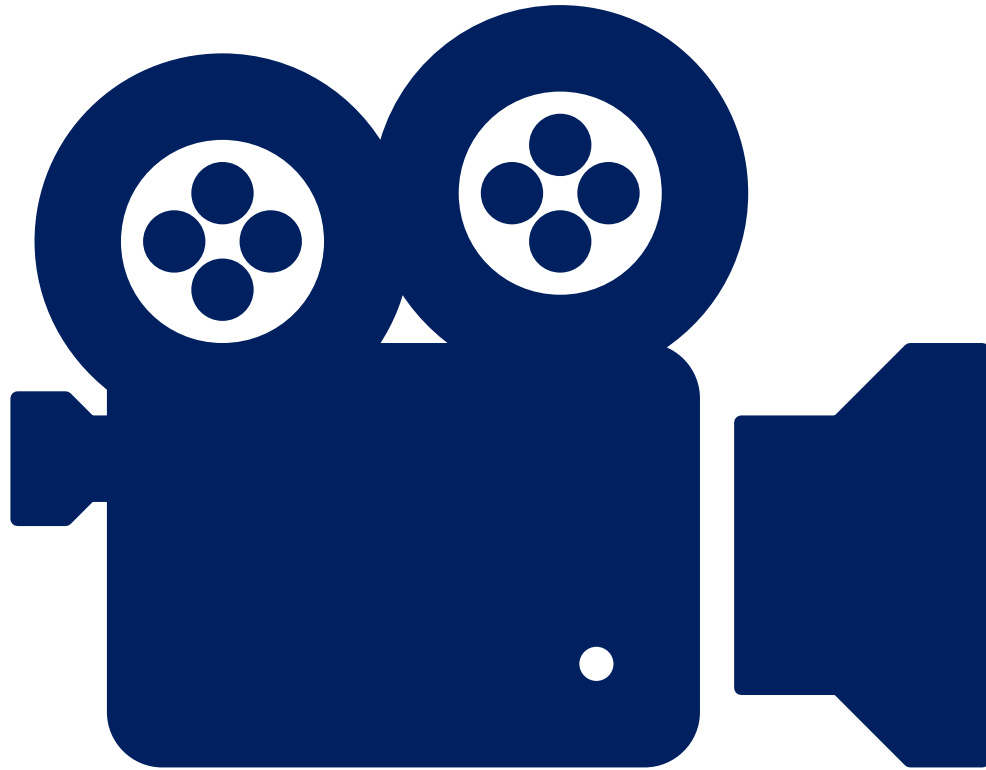
ACTIVITY



Public Key Infra-structure

VIDEO -

[HTTPS://YOUTU.BE/T0F7FE5ALWG](https://youtu.be/T0F7FE5ALWG)

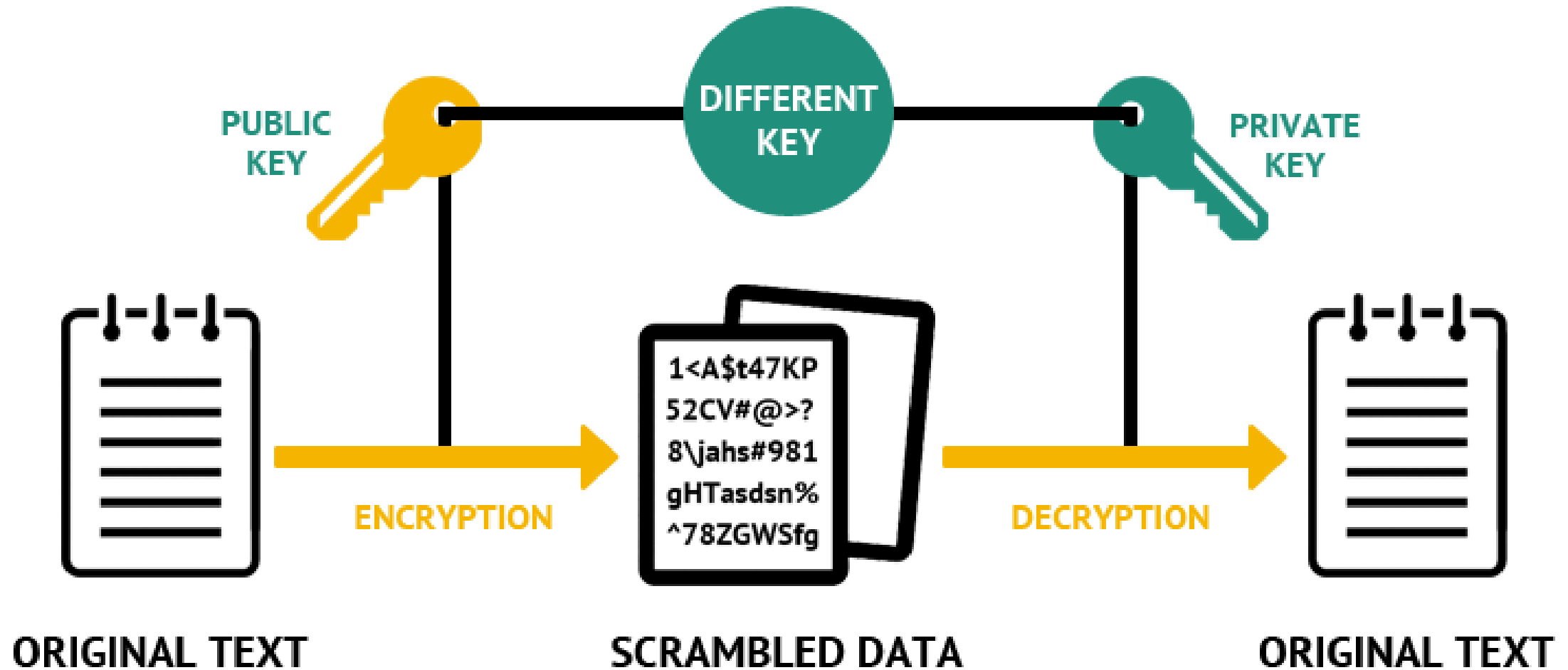


The Internet: Encryption & Public Keys

VIDEO -

[HTTPS://YOUTU.BE/ZGHMPWGXEXS](https://youtu.be/ZGHMPWGXEXS)

Asymmetric Encryption



Encryption

$$c \equiv m^e \pmod{n}$$

Decryption

$$m \equiv c^d \pmod{n}$$

c=Cipher Text

m=Message Text

e=Public Key

d=Private Key

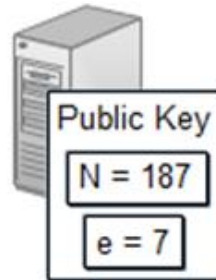
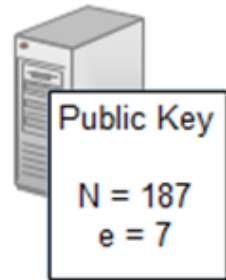
n=P * Q (already Calculated)

• PUBLIC KEY

- 2 giant primes, p and q
 - $p = 17, q = 11$
- $p * q = N$
 - $N = 187$
- Pick another prime, e
 - $e = 7$

• PRIVATE KEY

- Private key = d
- $e * d = 1(\text{mod}(p-1)*(q-1))$
- $7 * d = 1(\text{mod } 16 * 10)$
- $7 * d = 1(\text{mod } 160)$
- $d = 23$



Private Key
 $d = 23$

Step 1

Alice chooses a number, A
Keeps it secret. $A=3$

Bob chooses a number, B
Keeps it secret. $B=6$

Step 2

Alice puts 3 through
 $7^A(\text{mod } 11)$
 $7^3(\text{mod } 11) = 343(\text{mod } 11) = 2$

Bob puts 6 through
 $7^B(\text{mod } 11)$
 $7^6(\text{mod } 11) = 117649(\text{mod } 11) = 4$

Step 3

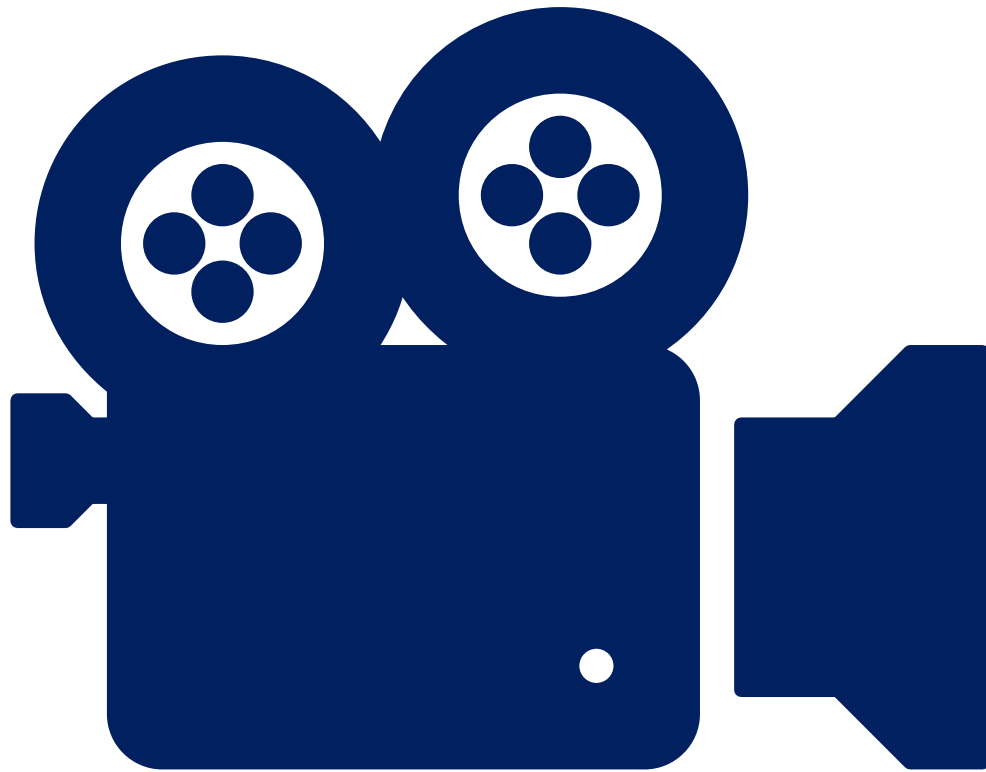
Alice calls result α
Sends 2 to Bob

Bob calls result β
Sends 4 to Alice

Step 4

Alice puts β through
 $\beta^A(\text{mod } 11)$
 $4^3 \text{mod } (11) = 64(\text{mod } 11) = 9$

Bob puts α through
 $\alpha^B(\text{mod } 11)$
 $2^6 \text{mod } (11) = 64(\text{mod } 11) = 9$



RSA Algorithm

VIDEO =

[HTTPS://YOUTU.BE/WXB-V_KEIU8](https://youtu.be/WXB-V_KEIU8)

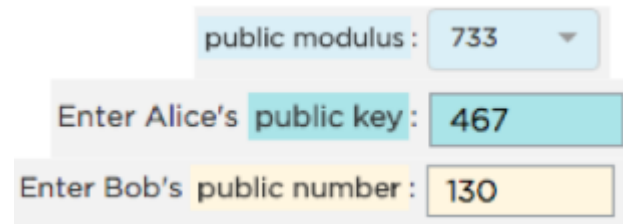
Crack the Message

What does Eve have to do to crack the message?

It turns out that figuring out what numbers to plug in to crack Alice or Bob's secret numbers so that the equations work out is essentially random guessing. If you want to read more about why check out the "How and why does it work?" document which gives a deeper explanation of the math behind the widget.

What does Eve know?

Eve knows only public information announced by Alice or Bob



A screenshot of a web-based cryptographic widget interface. It displays three input fields for public information. The first field is labeled 'public modulus :' and contains the value '733'. The second field is labeled 'Enter Alice's public key :' and contains the value '467'. The third field is labeled 'Enter Bob's public number :' and contains the value '130'.

public modulus :	733
Enter Alice's public key :	467
Enter Bob's public number :	130

Crack the Message

To crack the message she must use this info to guess Alice's Private Key or Bob's Private number.

To Crack Alice's Private Key...

Crack Alice's private key :

$(467 \times ??) \text{ MOD } 733 = 1 = ??$

To crack Alice's private key Eve must figure out what number to multiply by 467 then MOD by 733 to come out = 1 (why 1? It's explained in the *How and Why does it work?* document)

...or to Crack Bob's Private Number

Crack Bob's secret number :

$(467 \times ??) \text{ MOD } 733 = 130 = ??$

To crack Bob's secret number Eve must figure out what number to multiply by 467 then MOD by 733 to come out = 130.

Recap - Properties of Public Key Encryption:

- Alice and Bob did not have to agree on anything, or communicate ahead of time.
- Alice and Bob only exchanged information in public, right in front of Eve. Eve could even choose the public modulus if you wanted to!
- Eve would have to guess either Alice's private key or the secret number Bob is trying to send.
- *Note:* The encrypted messages only go one way. If Alice wanted to send a message to Bob, Bob would have to generate his own public/private key pair.
- However, because the message can only go one way, the sender can feel safe that **ONLY** the intended recipient can decrypt the message.
- The *real* public key crypto does not quite work this way. What we have setup here emulates many important properties, but it is in reality not hard for a computer to crack - just hard for you.
- The *real* version is called RSA encryption and rather than simple multiplication it uses exponentiation in combination with properties of modulo to create even larger numbers that are even harder to guess.

What do you actually need to know?

- **Cryptography has a mathematical foundation.**
- It relies on **asymmetric** keys, which you can make using numbers and math.
- The **modulo** operation acts as a one-way function.
- When you multiply big numbers and mod them by other big numbers, it's really hard to figure out what the original numbers were; the technique is essentially reduced to random guessing.

What do you actually need to know?

- The security of publicly known encryption protocols is based on the fact that cracking a message by brute force would take an unreasonable amount of time.
- With a sufficiently large modulus (say, 256 bits, which would be roughly a 77-digit number), random guessing would take an unreasonable amount of time. Even if you had millions of computers working on it constantly, it would take trillions of years.
- Because the method of encryption is public, it actually *increases* the security, because good guys and bad guys know how hard it is to crack.

Recap:

- What made the encryption harder/easier for Eve to crack?
- Perhaps obvious, but the bigger the clock size the harder it is for Eve to crack.
- There are also certain values that Bob could send, like 0 or 1, that would give away the secret.
There is no way to crack the encryption other than brute force
- If you could imagine that value being not a 4-digit number but, say a 75-digit number the computation for Eve becomes mind bogglingly hard.

Need to Know:

- Alice's public key is no accident. It was computed to make the math in the end work out.

Recap:

Public Key Encryption was (and is) considered a major breakthrough in computer science.

Public key cryptography is what makes secure transactions on the Internet possible.

- In the history of the Internet, the creation of public key cryptography is one of the most significant innovations; without it we could not do much of what we take for granted today --we couldn't buy things, communicate without being spied on, use banks, or keep our own conduct on the Internet secret or private.
- Until asymmetric encryption was invented, the only way to ensure secure transactions on the Internet was to establish a shared private key, or to use a third party to guarantee security. The implications of this are huge. It means any person can send any other person a secret message transmitting information over insecure channels!