Introduction to Cryptography

Cybersecurity

Cryptography Day 1

Class Objectives

By the end of today's class, you will be able to:

- Use basic transcription and substitution ciphers and keys to encrypt simple messages.
- Understand how encryption supports secure communication through the PAIN framework.
- Differentiate between encoding and encrypting.
- Calculate the strength and efficiency of various encryption levels.
- Use symmetric encryption tool OpenSSL to confidentially transmit secure messages.

Introduction to Cryptography

Always remember the CIA!

Confidentiality is focused on keeping information and communication secure from unauthorized parties.

The Importance of Confidentiality

It is critical for organizations to keep private information secure.

- A doctor loses a laptop containing patients' private medical records.
- An unauthorized person finds the laptop, opens it and is able to access the private data.
- This can impact the reputation of the doctor *and* the hospital responsible for the data.
- This can also have a financial impact, as a leak can result in significant legal fines for disclosure of sensitive data.

A primary method for keeping information secure is cryptography.

Cryptography is the art and science of keeping information secure through the use of mathematical concepts and techniques.

This Week's Scenario

In today's activities, we will be playing the role of security analysts at the Hill Valley Police Department.

- You will be investigating the **Alphabet Bandit**, who is responsible for a number of burglaries in Hill Valley.
- The Alphabet Bandit likes to leave hidden messages after each burglary, and we must use cryptographic techniques to investigate the incidents.

Questions?

The History of Cryptography

The Origins

While cryptography seems like a modern concept, cryptographic techniques were actually in use in early human civilizations.

These early civilizations engaged in battles, politics, and fights for supremacy.

Individuals needed to find methods to communicate securely and keep these communications hidden from enemies.

One of the earliest methods of applied cryptography is the Caesar cipher.

A **cipher** is a method of designing secret or hidden messages.

The Caesar Cipher

In an effort to communicate with his military, the Roman general developed a **cipher** to hide his communication.

Caesar's plaintext:	Encrypted ciphertext:
"Launch an attack at sunrise."	*"Odxqfk dq dwwdfn dw vxqulvh"*

The Caesar cipher is a method of **encryption,** a process of modifying a message or information in such a way that prevents unauthorized parties from accessing it.

Encryption takes a **plaintext message** and converts it to an unreadable **ciphertext** message.

The Caesar Cipher

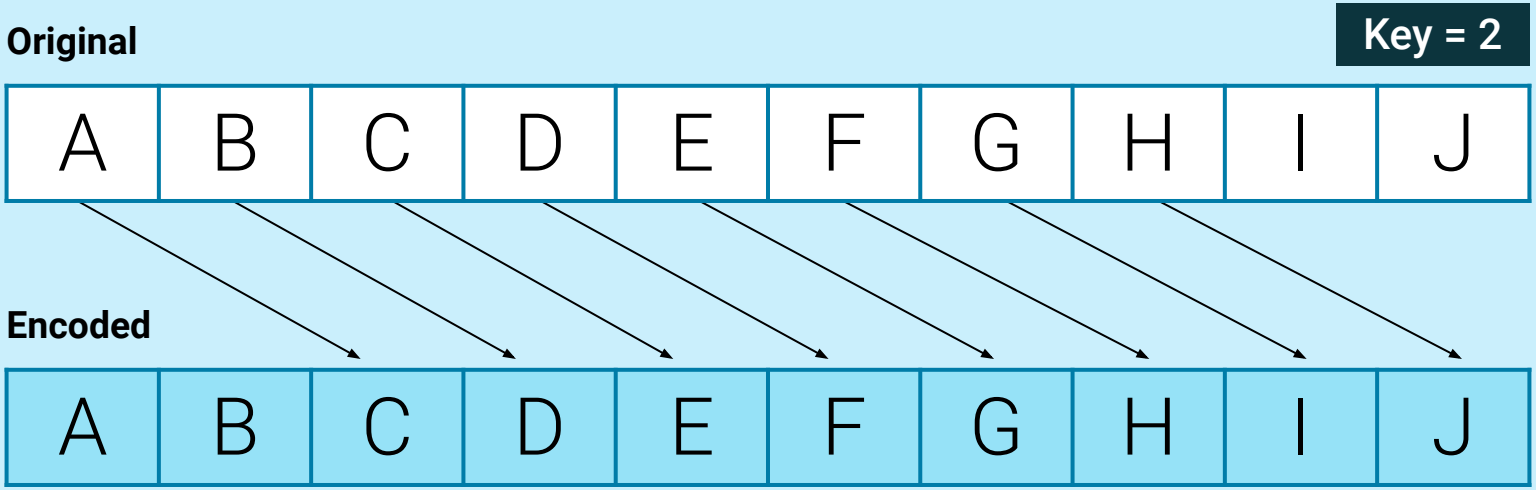
The goal of the Caesar cipher is not only to prevent unauthorized parties from reading the communication, but to also allow authorized parties, such as Caesar's military, to receive and understand the hidden message.

Encrypted ciphertext:	Decrypted plaintext:
"Odxqfk dq dwwdfn dw vxqulvh"	*"Launch an attack at sunrise."*

This is accomplished through **decryption**, the process of converting ciphertext back into readable plaintext.

How the Caesar Cipher Works

The Caesar cipher works by shifting letters a set number of positions (the **key**) from the original letter.



Examples

"I HID A CAB" → "K JKF C ECD"

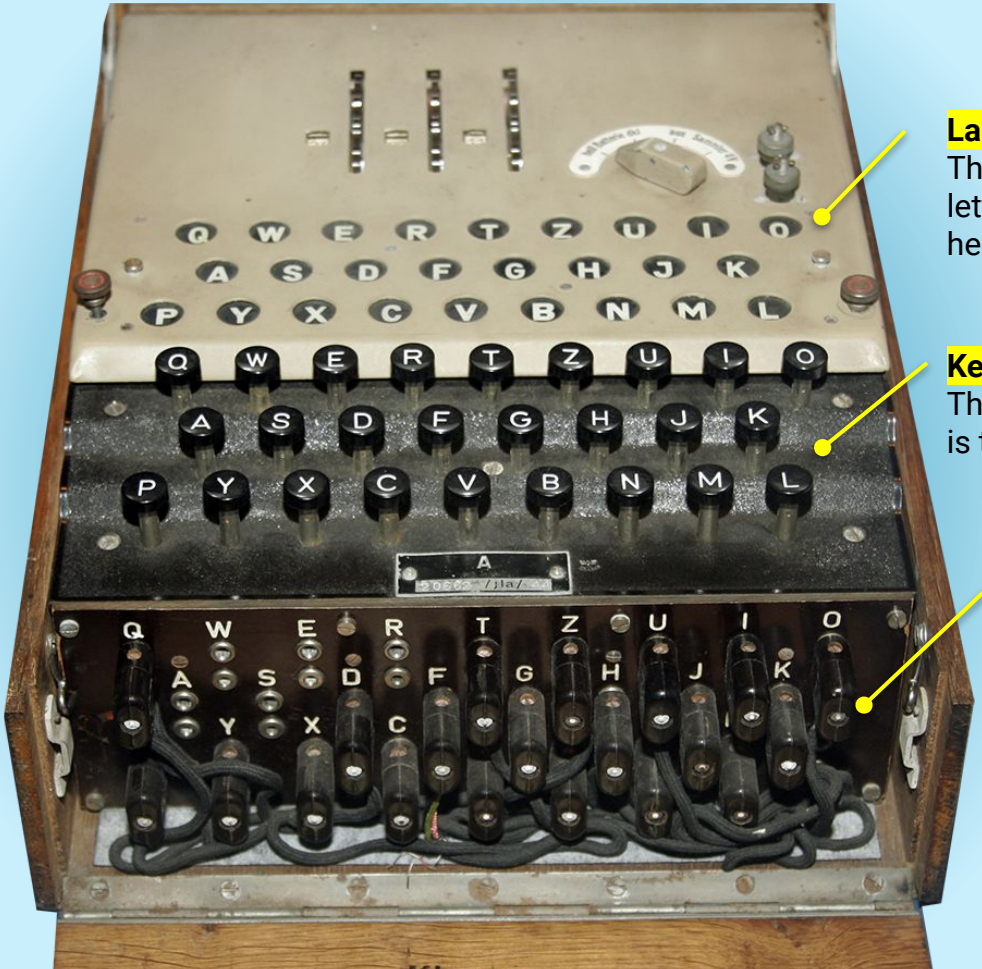
"A BAD DAD" → "C DCF FCF"

The Enigma Machine

As technology advanced, applied cryptography became more complex and harder to crack.

After the end of World War I, a German engineer named Arthur Scherbius developed an advanced encryption tool known as the **Enigma machine.**

The machine scrambles the 26 letters of alphabet, allowing for billions of ways to encrypt a message.



Lampboard
The encrypted letter shows up here.

Keyboard
The message is typed here.

Slots
Wires are plugged into specific slots.

Enigma: Key Creation

Settings were configured by the user.

- The key was created when the sender plugged wires into specific slots and arranged the roto settings.
- The exact settings were then used by the recipient for decryption.

Enigma: Encryption

To **encrypt**, the sender entered the plaintext message on the machine's keyboard one letter at a time.

- After each letter was pressed on the keyboard, another letter lit up on the machine's lampboard.
- The illuminated letters were documented, creating the ciphertext.
- The ciphertext was transmitted to the recipient.

Enigma: Decryption

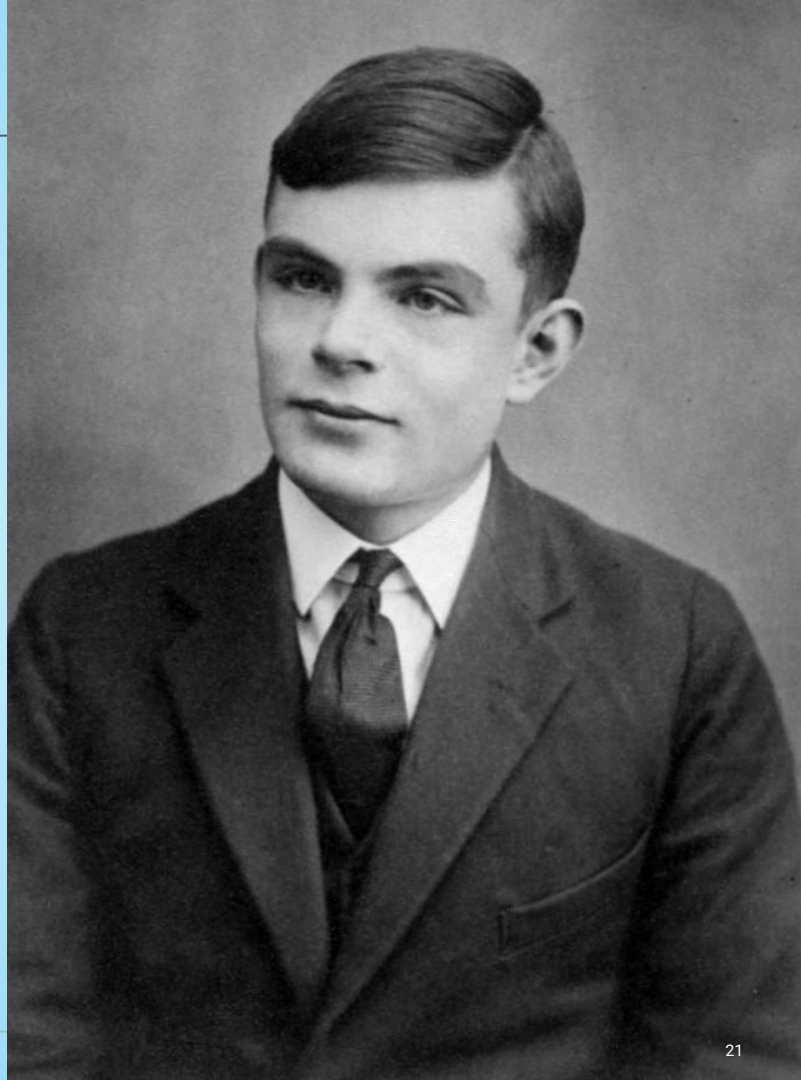
The **secret key** combination was provided to the recipient in advance.

- The recipient used the key to configure their machine with the exact settings used for encryption.
- Ciphertext letters were entered one at a time on the keyboard, showing the original plaintext in the lampboard.
- The illuminated letters were documented one at a time, converting the ciphertext back to plaintext.

Cracking the Enigma Machine

During the height of World War II, English mathematician and computer scientist **Alan Turing** developed a method to exploit the weaknesses of the Enigma machine's design.

- Known as the **Bombe**, Turing's machine helped decrypt the most complex versions of the Enigma cipher.
- Considered one of the most important victories of the Allied forces during the war, Turing's machine was able to prevent many attacks by decrypting secret messages sent by the Germans.



Summary: Key Cryptographic Terms

Plaintext	Information in human-readable form.
Ciphertext	Plaintext message that has been encrypted into an unreadable form.
Encryption	The process of converting plaintext to ciphertext.
Decryption	The process of converting ciphertext to plaintext.
Cipher	A method of performing encryption or decryption.
Key	A parameter specifying how plaintext is converted to ciphertext and vice versa.
Caesar cipher	A type of cipher that shifts the letters in the alphabet by a fixed number.
Enigma cipher	A type of cipher used by Germany in World War II to encrypt messages.

Activity: Caesar Cipher Code Names

In this activity, you will play the role of security analysts working for the Hill Valley Police Department.

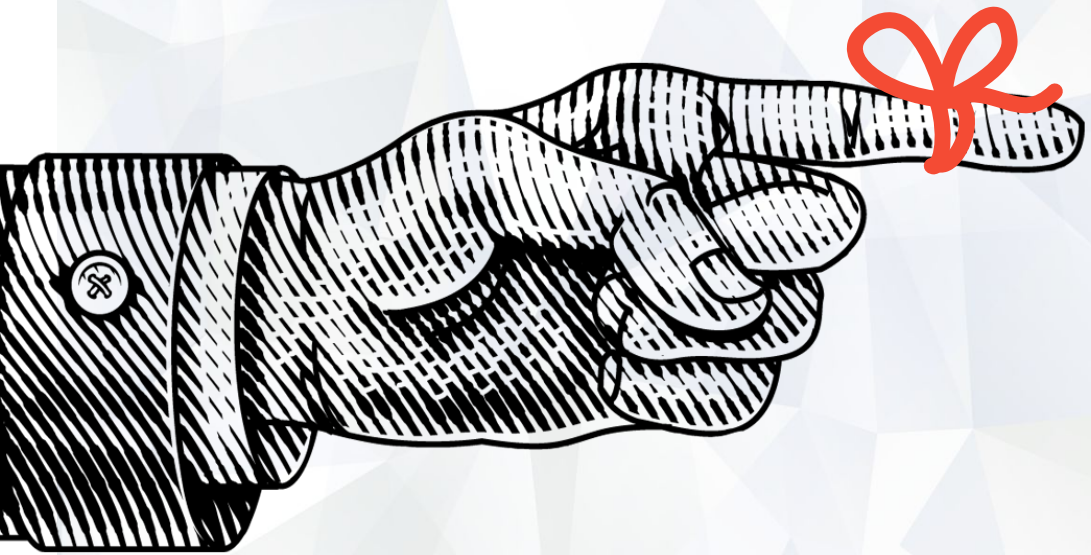
You have been assigned to a top secret task force to find the Alphabet Bandit. You must create a code name, encrypt it, and send it to your partner.

Suggested Time:

10 Minutes

Questions?

Introduction to Character Encoding



Remember,

Computers transmit digital data with **binary**.

Therefore, encrypting data on computers first requires a method of alphanumeric representation, known as **character encoding**.

Character Encoding

While encoding may seem similar to encryption, they have very different goals:

Encoding

- Used to transform data so it can be properly used by different types of system.
- Not used to keep information secret.
- Data is encoded with publicly available schemes that can be decoded by anyone.

***Does not** use a key.*

Encryption

- Used to keep information from being accessed by unauthorized parties.

Uses a key to encrypt and decrypt.

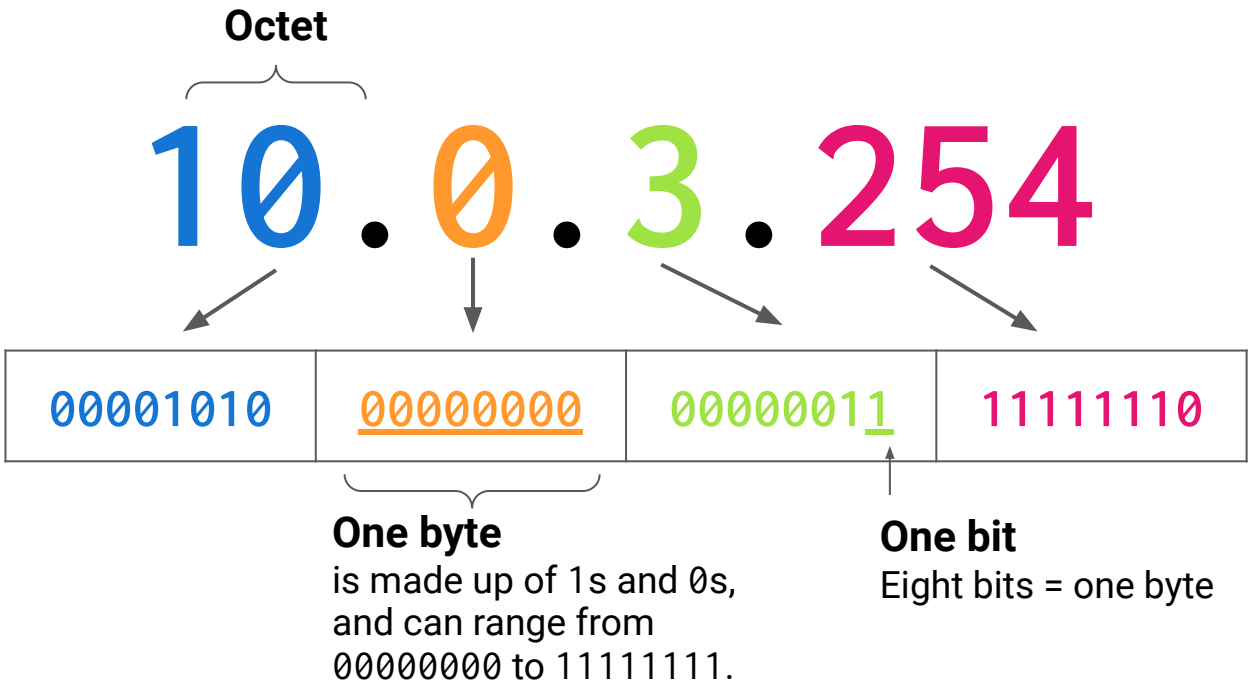
Character Encoding

There are many encoding schemes available. We'll review a few common ones:

- Binary
- ASCII
- Hex
- Octal

Binary Encoding

Most encryption of digital communication takes place at the level of binary data. Readable text is first converted to binary before applying encryption.



Binary Encoding

This conversion is called a **binary to decimal encoding**.

The byte `00000000` represents the decimal **0**.

The byte `11100000` represents the decimal **224**.

The byte `11111111` represents the decimal **255**.

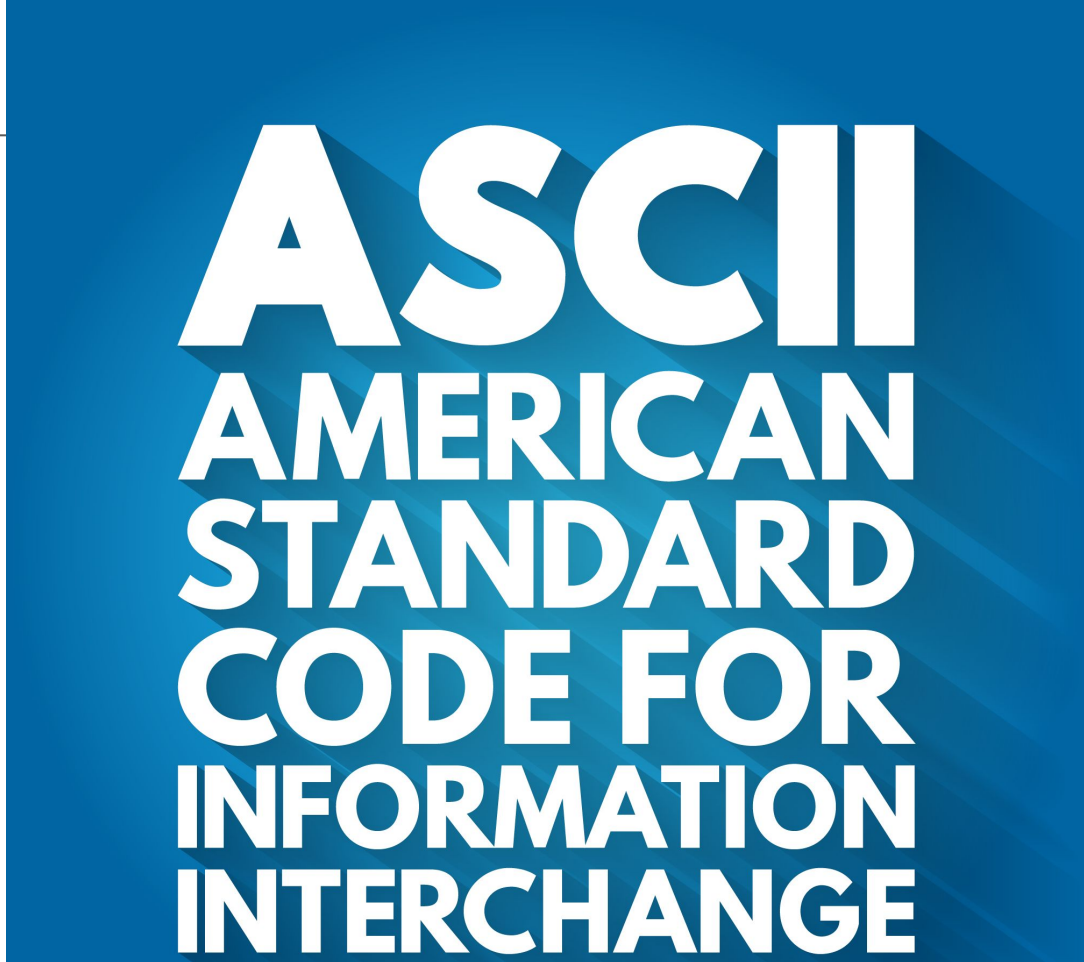
Since each byte can only represent a number from **zero** to **255**, and since we read text with letters, we use ASCII encoding to convert these numbers to letters.

ASCII Encoding Is...

The representation of every upper- and lowercase letter of the English alphabet, as well as common punctuation marks and graphic and mathematical symbols, as a number between zero and 255.

NOTE

Zero to 127 is considered the standard ASCII, and 127 to 255 is considered extended ASCII.



ASCII and The Decimal System

ASCII is used to represent computer-stored characters in a human-readable format.

Look down at your keyboards.

Every character is part of ASCII. Upper and lowercase letters, special characters (!@#$...), and numbers (1,2,3,4...).

The **decimal system** is a little more limited.

It consists of the characters 1, 2, 3, 4, 5, 6, 7, 8, 9, and `0`.

ASCII and the Decimal System

The limited number of characters still allow us to convey complex information. In fact, anything we enter in ASCII can be converted to decimal format.

ASCII Example

A, B, C. It’s easy as 1, 2, 3!

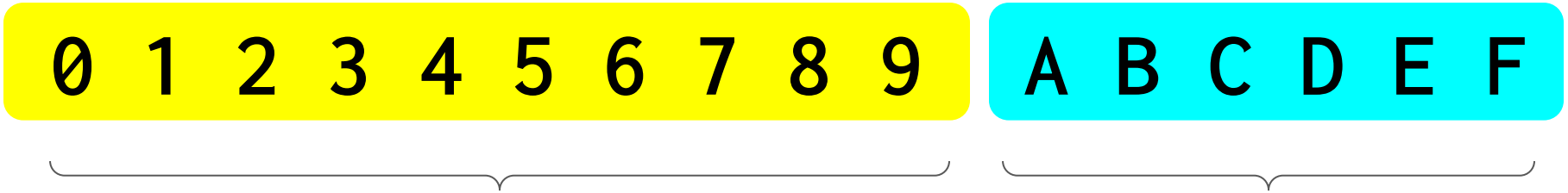
Decimal Example

65 44 32 66 44 32 67 46
32 73 116 39 115 32 101
97 115 121 32 97 115 32
49 44 32 50 44 32 51 33

Binary data can be more efficiently stored and represented by encoding with the hexadecimal number system.

Hex Encoding

The hex system uses **16 symbols** to represent the base values.



The **base numbers** range from 0–9.

The **letters A–F** represent 10–15.

hello = 68 65 6c 6c 6f

This conversion is called **hex-to-ASCII encoding** or **hex-to-text encoding**.

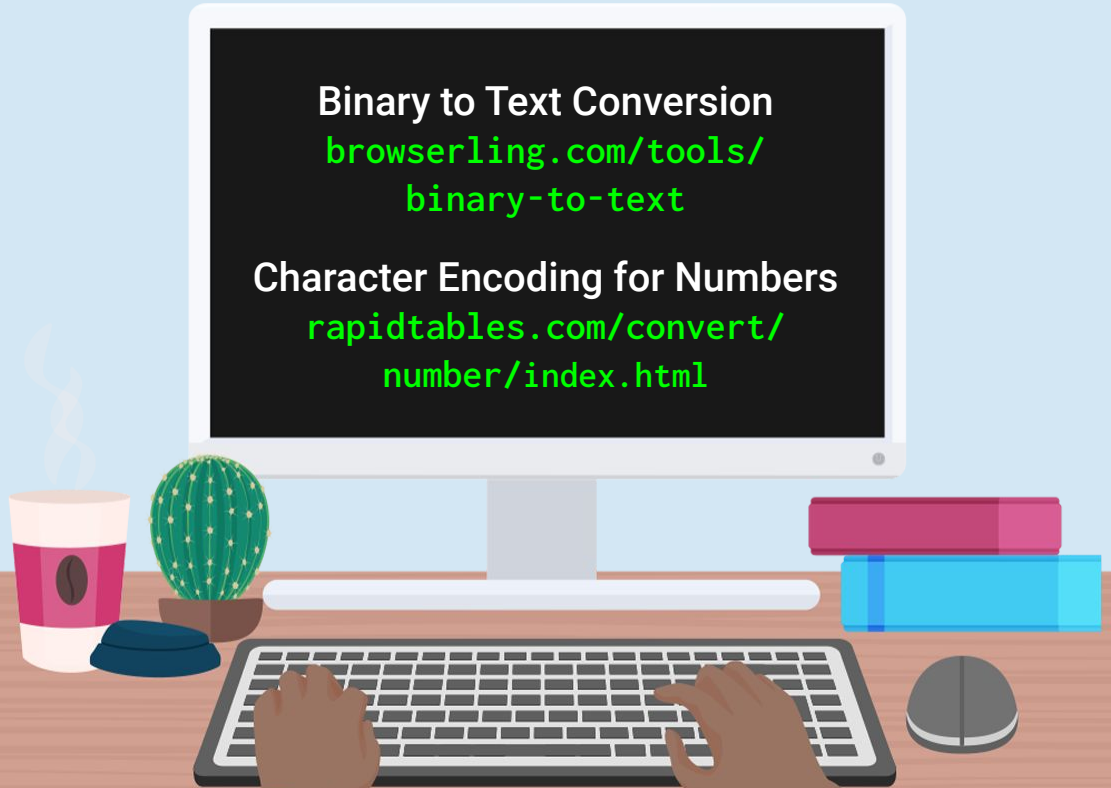
Octal

The **octal system** applies a principle similar to hex, but uses digits 0 through 7.

Octal		Decimal
`042`	=	34

Encoding and Decoding Tools

There are various online tools to help with the encoding and decoding process.



Let’s practice decoding a binary message using browserling.com.

Summary

We’re learning a lot of new concepts this week. Let’s review:

- The goal of encoding isn't to keep a message secret, but to transform data to be used by another system.
- Encoding, unlike encryption, does not use a key.
- Encoding is often used to transform digital text data into binary data, where encryption commonly takes place.
- There are many types of encoding schemes available and each is relevant for different circumstances.
- There are many free online resources for encoding and decoding messages, such as Browserling and Rapid Tables.

Activity: Decoding

In this activity, you'll continue to play the role of security analysts working for the Hill Valley Police Department.

There was another burglary last night. The bandit left behind an encoded message. You are tasked with decoding the message to determine the bandit's next target.

Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?

Goals of Cryptography

Goals of Cryptography

Introducing the P.A.I.N model.

Privacy
(Confidentiality)

Authentication

Integrity

Non-repudiation

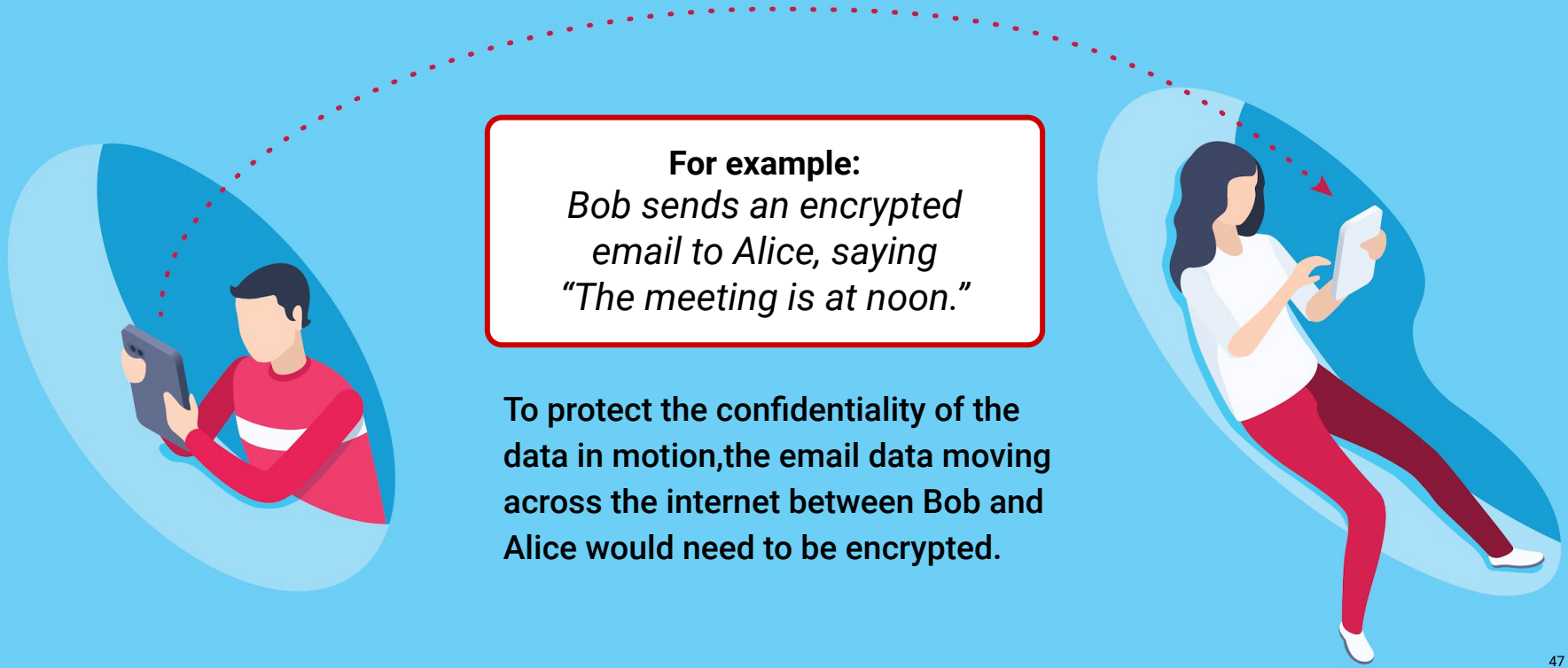
Goals of Cryptography

Introducing the P.A.I.N model.

Privacy keeps data secure from unauthorized parties.

Privacy / Confidentiality

Data in motion: data moving between devices.



For example:
Bob sends an encrypted email to Alice, saying "The meeting is at noon."

To protect the confidentiality of the data in motion,the email data moving across the internet between Bob and Alice would need to be encrypted.

Privacy / Confidentiality

P A I N

Data at rest: static data, such as that stored on a hard drive or in a database.

For example:
Data stored on your laptop.

To protect the confidentiality of this data at rest, the laptop's hard drive would be encrypted.

Goals of Cryptography

Introducing the P.A.I.N model.

Authentication is used to confirm the identities of the sender and receiver of data.

Authentication

P A I N

Even when a message is encrypted, an attacker can still send encrypted data and claim they are someone they are not.

01

Bob sends a message to Alice: **“The meeting is at noon.”**

02

Scammer Tim sends an email impersonating Bob: **“The meeting is cancelled.”**

03

Alice receives the email.

Without authentication, Alice could be tricked into thinking the meeting is cancelled.

Goals of Cryptography

Introducing the P.A.I.N model.

Integrity ensures a message isn't altered between when it's sent and when it's received.

Integrity

P A I N

Even if a message is encrypted and the sender is authenticated, an attacker can still alter the contents of a message.

01 Bob sends a message to Alice: **“The meeting is at noon.”**

02 Scammer Tim intercepts the message and sends an email impersonating Bob: **“The meeting is at 5 a.m.”**

03 Alice receives the email.

Goals of Cryptography

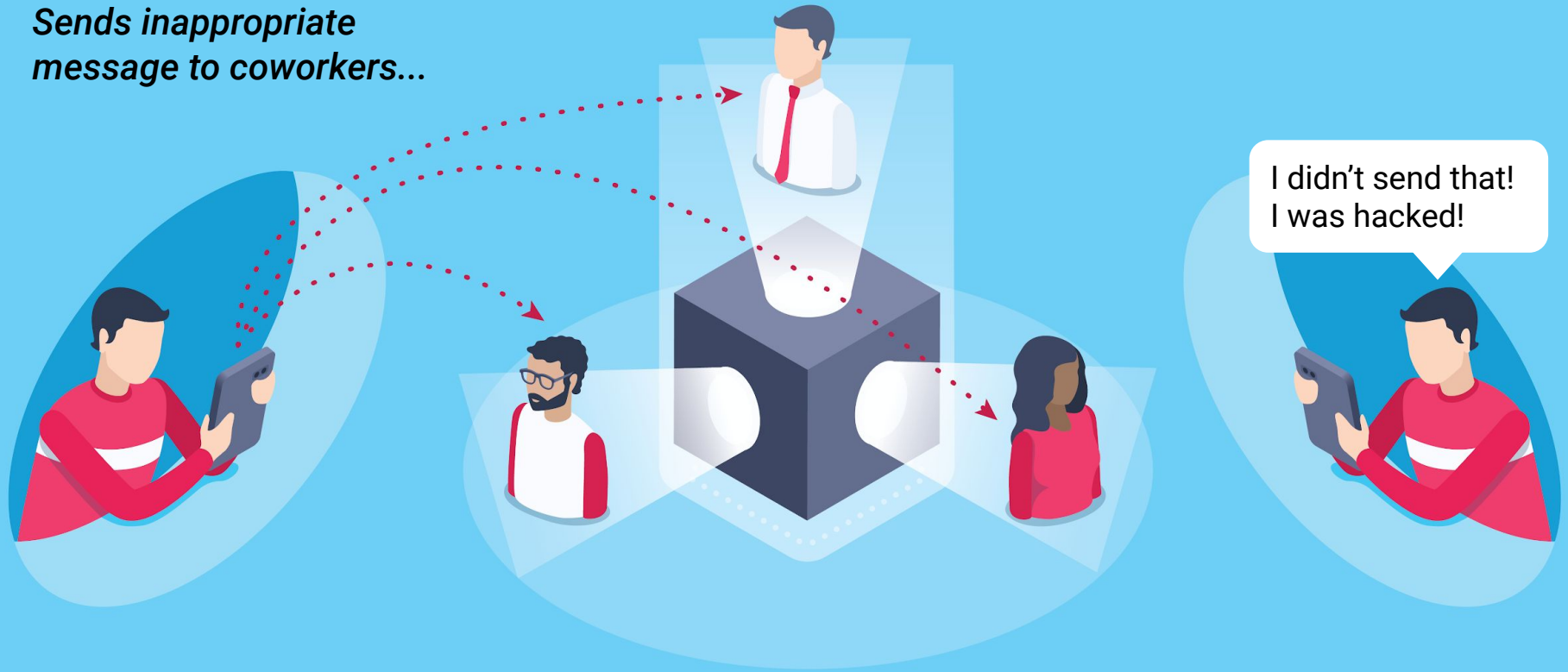
Introducing the P.A.I.N model.

Non-repudiation prevents the original sender from denying they were the sender.

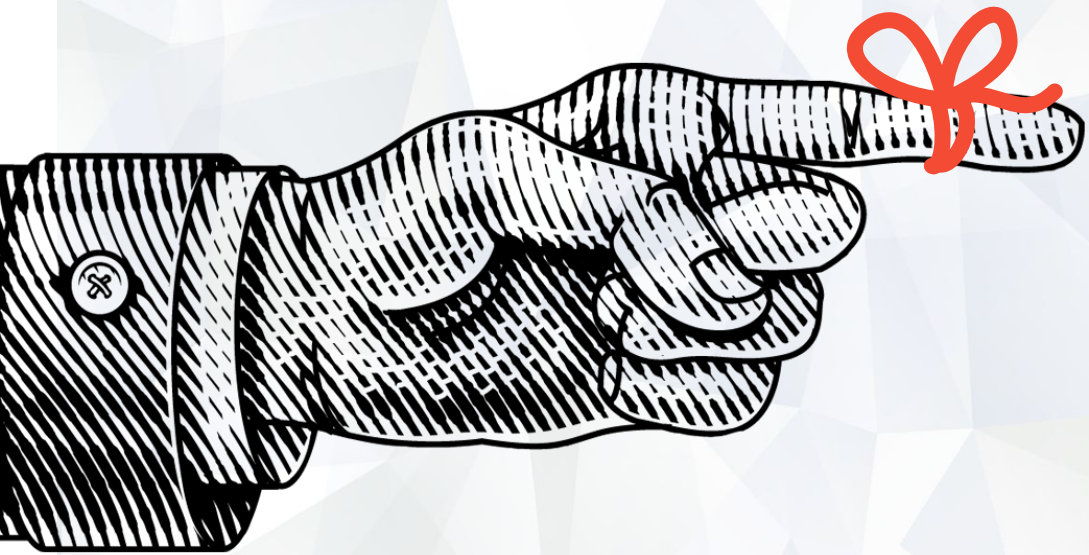
Non-Repudiation

P A I N

Sends inappropriate message to coworkers...



Introduction to Cryptography Ciphers



Remember,

- We covered how ciphers are used to provide confidentiality by encrypting the data.
- Encryption is accomplished by using a key.

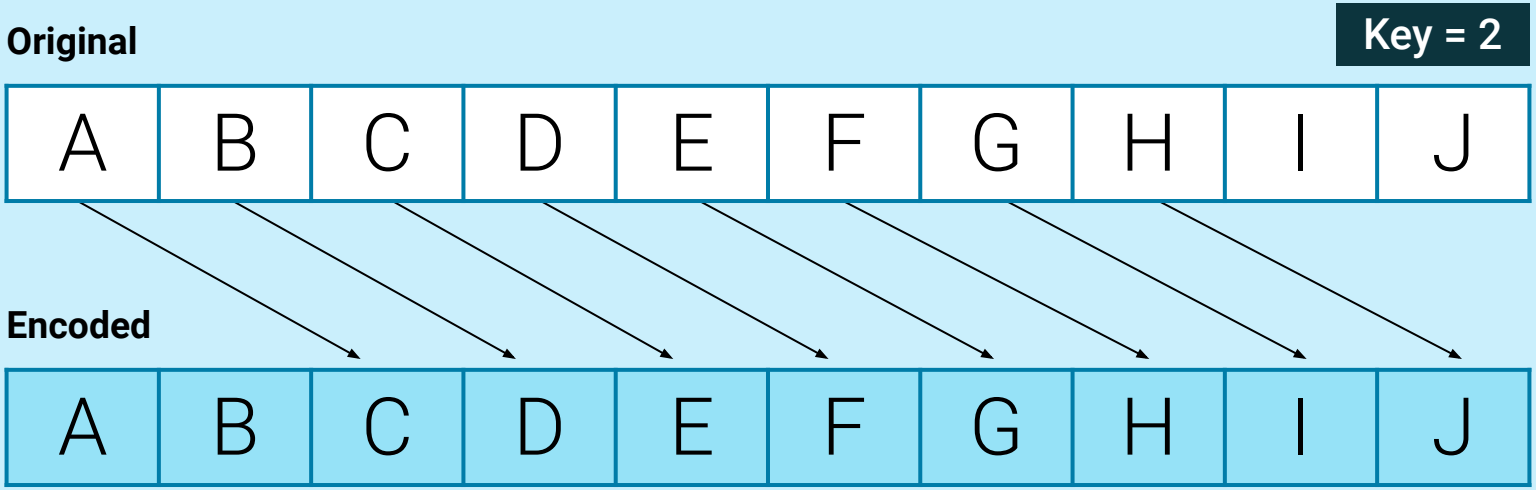
Algorithms are mathematical instructions that ciphers use for encryption.

Stream ciphers apply their algorithm one bit (character) at a time.

Stream and Substitution Ciphers

One prominent stream cipher is the **substitution cipher**, which substitutes out old values for new values of input message.

- The Caesar and Enigma cipher are examples.
- While substitution alone doesn't provide strong encryption, when combined with other techniques it can provide strong, fast encryption.



Block ciphers apply their algorithm to chunks of characters.

Block and Transposition Ciphers

One prominent block cipher is the **transposition cipher**, which breaks an input message into equal-sized blocks and rearranges the letters of each block.

1. Break the message into blocks of three characters.
2. Replace the first, second, and third character of each block with the third, first, and second character.
3. Combine rearranged text.

Key =

1	2	3
3	1	2

Message	H	E	L	L	O	!
Encrypted message	L	H	E	!	L	O

Summary

We're learning a lot of new concepts this week. Let's review!

- The goals of cryptography are illustrated with the **P.A.I.N. model**.
- P.A.I.N. is an acronym standing for Privacy, Authentication, Integrity, and Non-Repudiation.
- Ciphers use mathematical formulas, known as **algorithms**, to encrypt and decrypt data.
- The main cipher categories are **block** and **stream ciphers**.
- Stream ciphers apply their algorithms one character at a time, and block ciphers apply the algorithms to blocks of characters.
- One type of stream cipher is the substitution cipher. One type of block cipher is the transposition cipher.
- Substitution ciphers replace each character with a different character.
- Transposition ciphers rearrange the letters within a defined block size.

Activity: Cryptography Concepts and Cipher

In this activity, you'll continue to play the role of security analysts working for the Hill Valley Police Department.

Your task is to use a found key to decrypt the most recent message left by the Alphabet Bandit.

Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?

Countdown timer

15:00

(with alarm)

Modern Cryptography

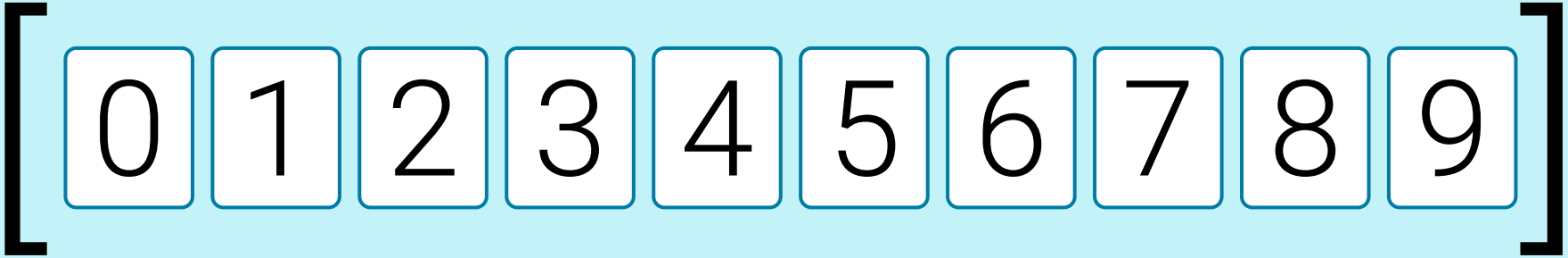
As technology improved, so did methods for cracking ciphers.

Modern cryptography needed more complex algorithms and longer cryptographic keys.

Keys

Each algorithm has a possible range of numbers that can be used as a key, known as a **key space.**

For example:
If a password could only be one numerical digits, the possible values are:



The key space is **10**.

For modern cryptography, key space is defined by the number of binary bits used in the key, known as **bit size**.

You may hear the question:

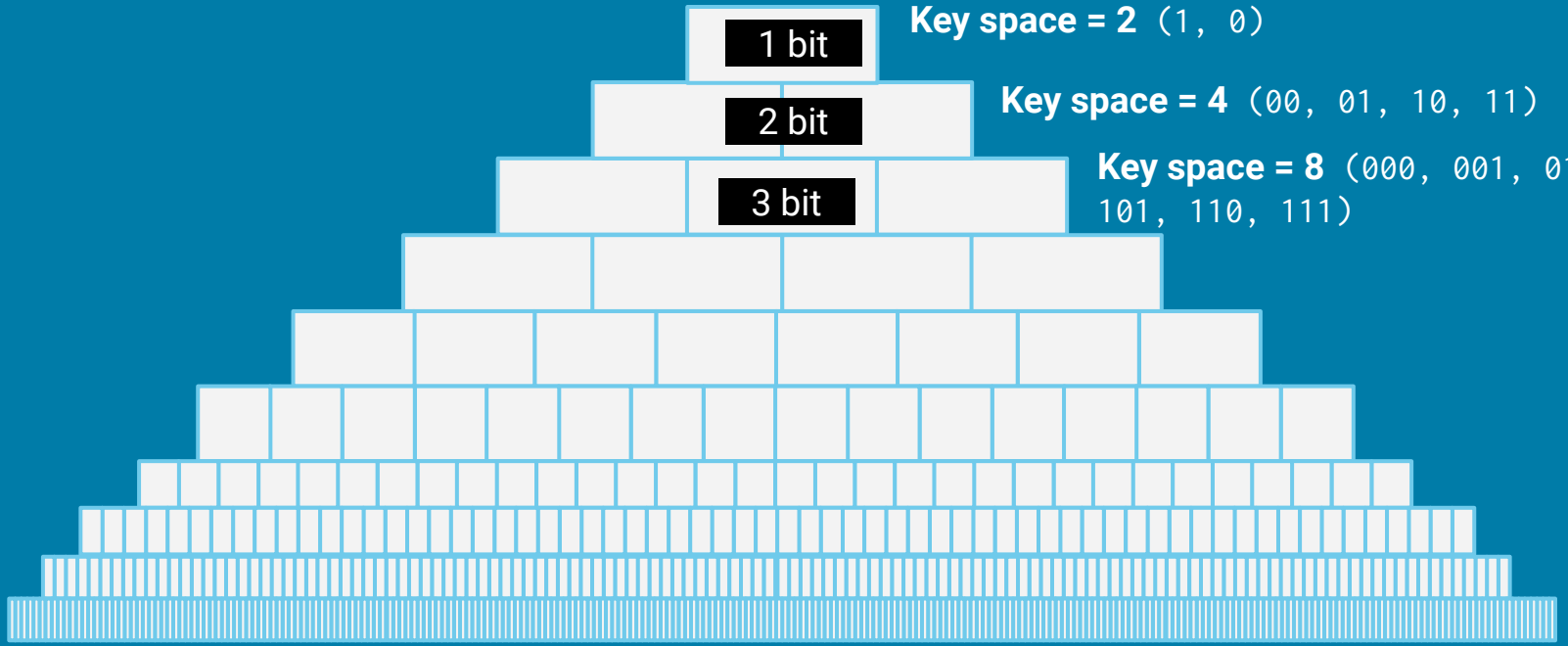
How much more secure is *x* more bits of encryption?

Keys and bit size

We'll need to understand how bit size affects key space and the level of encryption.

For each bit added, the key space doubles in size.

Key space = $2^{\text{bit size}}$



Instructor Demonstration

Encryption Strength (10-Bit and 30-Bit)

Activity: Encryption Strength

In this activity, you'll continue to play the role of security analysts working for the Hill Valley Police Department.

In this activity, you will compare several email security vendors and choose the most cost-effective one for protecting future emails.

Suggested Time:

10 Minutes

Time’s Up! Let’s Review.

Questions?

Symmetric Key Algorithms

If larger bit size means stronger encryption, why don’t we just use a million-bit key?

Security Tradeoffs

It takes time and computational resources to encrypt and decrypt larger keys.

Is the encryption strength worth the time to use the key?

Security Tradeoffs

Do we want an incredibly strong cipher that's hard to compute and difficult to decrypt?

or

Do we prefer average security that's faster?

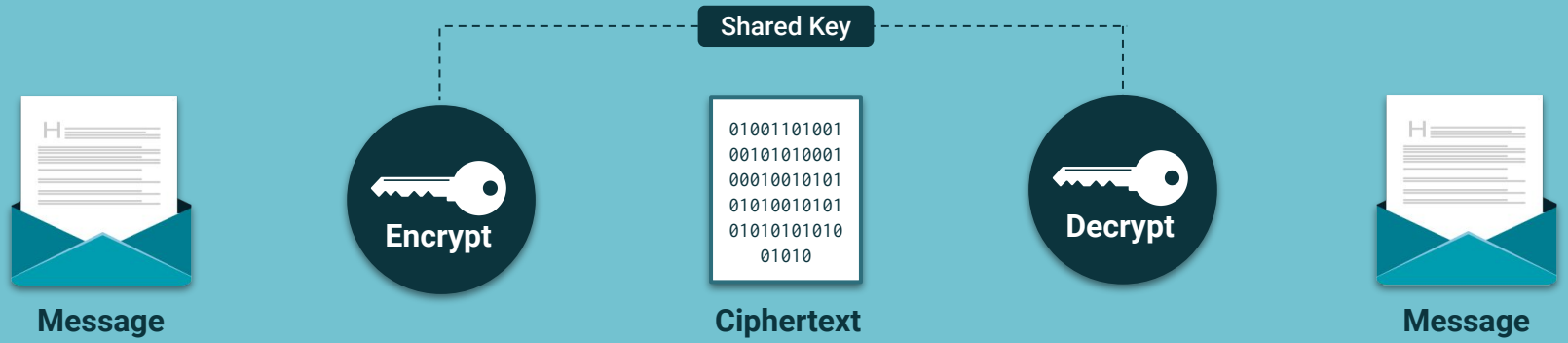
Modern symmetric key algorithms use algorithms that are secure *and* fast.

Finding the Balance

Symmetric key algorithms use a single, shared key to encrypt and decrypt a message. This shared key needs to remain **private**. If exposed, the message can be decrypted by anyone.

Some widely known symmetric key algorithms include:

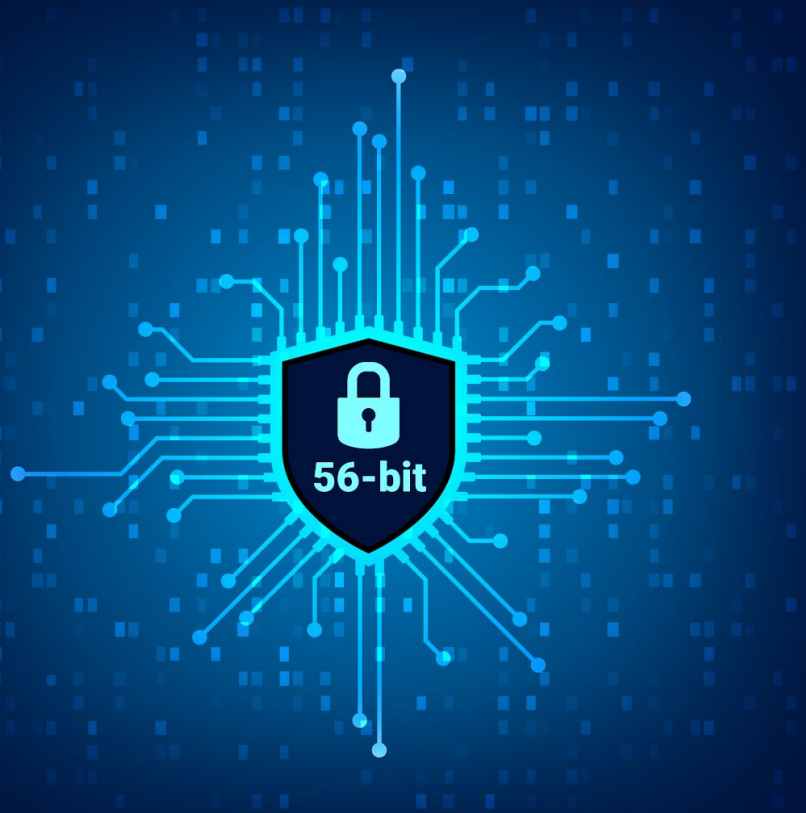
- Data Encryption Standard (DES)
- Triple DES (3DES)
- Advanced Encryption Standard (AES)



Data Encryption Standard (DES)

DES is a 56-bit algorithm published by the United States government in 1977.

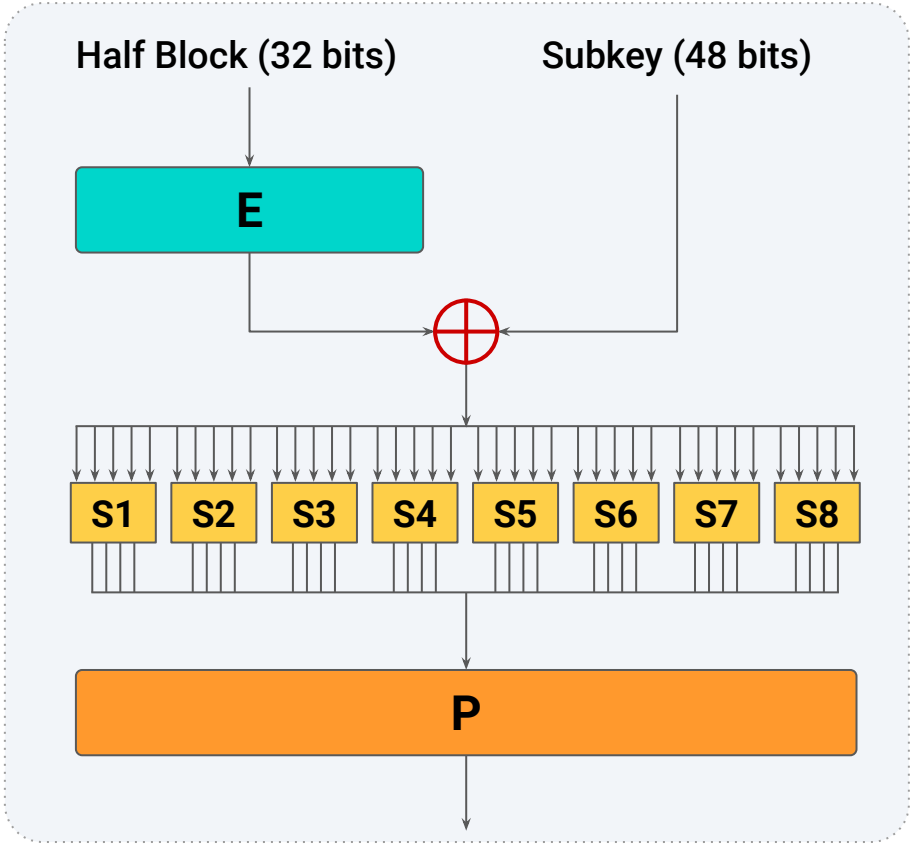
- Flaws were found in DES and additional security was added to create Triple 3DES.
- However, the security community banded together to develop a newer, more secure symmetric encryption algorithm.



Data Encryption Standard (DES)

DES is a 56-bit algorithm published by the United States government in 1977.

- Flaws were found in DES and additional security was added to create Triple 3DES.
- However, the security community banded together to develop a newer, more secure symmetric encryption algorithm.



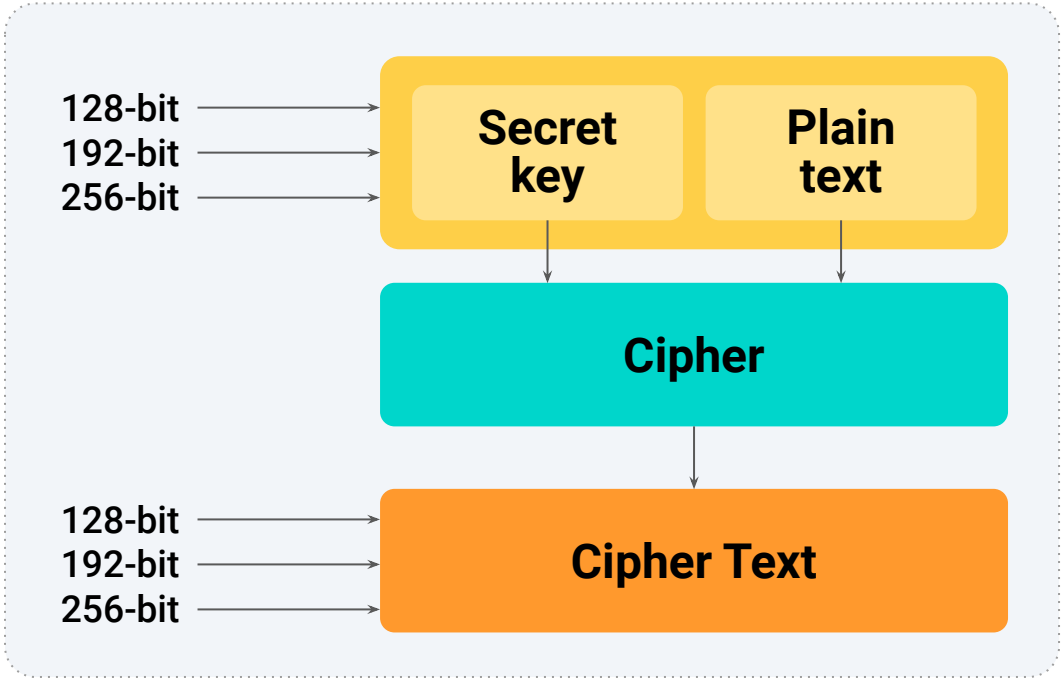
Advanced Encryption Standard

In 1997, the National Institute of Standards and Technology (NIST) announced they were seeking a replacement for DES.

- NIST opened a contest for cryptographers to submit algorithms.
- In the first round, 15 submissions were collected.
- The community attempted to break them all.
- In the second round, the five most promising algorithms were subjected to extensive cryptanalysis by the community.

Advanced Encryption Standard

Eventually the **Rijndael** cipher was determined to be the strongest. After it was refined and standardized, it became the **Advanced Encryption Standard (AES)**.



Now we'll use the command-line tool OpenSSL to encrypt and decrypt data.

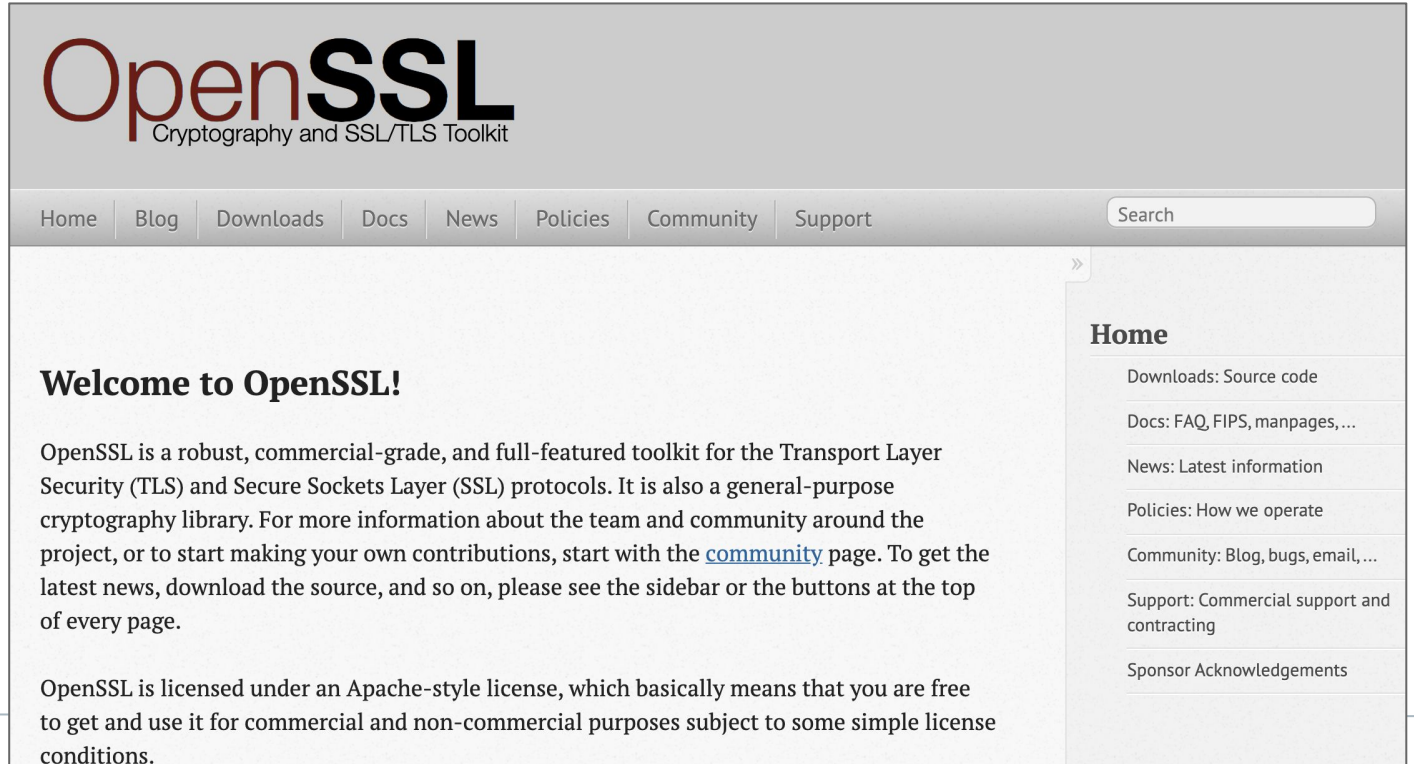
Instructor Demonstration

OpenSSL

OpenSSL is a free command-line tool used for symmetric encryption and decryption.

Demo Summary

OpenSSL can generate a random key and initialization vector (IV). With the key and IV, OpenSSL can encrypt and decrypt a message with simple terminal commands.



Demo Summary

Creating the key and IV:

```
openssl enc -pbkdf2 -nosalt -aes-256-cbc -k mypassword -P > key_and_IV
```

Encrypting:

```
openssl enc -pbkdf2 -nosalt -aes-256-cbc -in plainmessage.txt -out plainmessage.txt.enc -base64 -K
89E01536AC207279409D4DE1E5253E01F4A1769E696DB0D6062CA9B8F56767C8 -iv EE99333010B23C01E6364E035E97275C
```

Decrypting:

```
openssl enc -pbkdf2 -nosalt -aes-256-cbc -in plainmessage.txt.enc -d -base64 -K
89E01536AC207279409D4DE1E5253E01F4A1769E696DB0D6062CA9B8F56767C8 -iv EE99333010B23C01E6364E035E97275C
```

Demo Summary

`openssl`	Initializes the OpenSSL program.
`enc`	Stands for “encryption.”
`-pbkdf2`	Specifies the encryption key type.
`-nosalt`	Specifies that salting will not be applied. (Salting, which we’ll cover in more depth later, adds a random value.)
`-aes-256-cbc`	Is the name of the cipher used.
`-k PASSWORD`	Creates a key, with the password `mypassword`.
`-P > key_and_IV`	Prints out the key and IV to a file called `key_and_IV`.

Activity: OpenSSL

In this activity, you'll continue to play the role of security analysts working for the Hill Valley Police Department.

You must use OpenSSL to decrypt a message from the police captain.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Questions?


The End