Edversity.

CYBERSECURITY SPECIALIZATION PROGRAM WEEK 3 - DAY 1

Instructor: Muddassir Shafique

TA: Suleiman Taj

Agenda

Week 1: Introduction to Cyber Security and Kali Linux (Completed)
Week 2: Networking and Security Fundamentals
Week 3: Cryptography
Week 4: OS Security
Week 5: Web Security
Week 6: Incident Response and Management
Week 7: Security Policies and Risk Management
Week 8: Emerging Technologies and Future trends
Week 9: CAPSTONE Project and Review
Week 10: CAPSTONE Project Presentations

What We'll Learn Today

- What is cryptography? Why do we need it?
- Key terms: plaintext, ciphertext, encryption, decryption, key, algorithm
- Types: Symmetric vs Asymmetric
- Classical ciphers: Caesar, Vigenère, Substitution
- Challenge - Code Decoder

What is Cryptography

Cryptography is the science and practice of securing communication and data by transforming it into a form that only authorized parties can understand. It involves techniques for encrypting (scrambling) information so that unauthorized users cannot access it and decrypting it back to its original form by those who have the right key or permission.

Purpose of Cryptography

Confidentiality: Ensures that information is only accessible to intended recipients and kept secret from unauthorized parties.

Integrity: Guarantees that data has not been altered or tampered with during transmission or storage.

Authentication: Confirms the identities of the parties involved in communication or transaction.

Non-repudiation: Prevents parties from denying that they sent or received a message.

Data security: Protects sensitive data like passwords, credit card information, and personal communication from cyber threats.

Why do we need it?

Cryptography helps protect confidentiality, ensure data integrity, authenticate users, and build trust in digital interactions. It's fundamental for safe online banking, shopping, private communication, secure government operations, and basically any digital service where security matters. Without it, the digital world would be vulnerable to cyberattacks, fraud, and privacy invasions.

Without cryptography, this information would be exposed to many risks, such as:

Privacy breaches: Unauthorized people could easily read private messages, emails, or data.

Data theft: Hackers could steal passwords, credit card details, or intellectual property.

Data tampering: Attackers could alter data in transit, leading to misinformation or fraud.

Identity theft: Without secure authentication, it's easier for someone to impersonate others.

Loss of trust: Users and businesses need assurance that their communications and transactions are safe and trustworthy.

Key Terms of Cryptography

Plaintext

- The original, readable data or message that you want to protect or send securely.
- Example: "Hello, how are you?"

Encryption

- The process of converting plaintext into ciphertext using a specific algorithm and key, to keep the information secret.
- Think of it as locking your message in a safe.

Ciphertext

- The scrambled, unreadable version of the plaintext after it has been encrypted. Only someone with the right key can convert it back to plaintext.
- Example: "X7!&$2#bQ" (nonsense without the key)

Key Terms of Cryptography

Decription

- The reverse process of encryption, where ciphertext is converted back into readable plaintext using the correct key.
- Unlocking the safe to read the original message.

Key

- A secret value used by the encryption and decryption algorithms to lock and unlock the data.
- Without the key, it's extremely difficult or impossible to decrypt the ciphertext.

Algorithm

- A set of mathematical rules or procedures used for encryption and decryption.
- It defines how the plaintext is transformed into ciphertext and back.

Key Terms of Cryptography

Plaintext —[Encryption + Key + Algorithm]→

Ciphertext —[Decryption + Key + Algorithm]→ **Plaintext**

Types of Cryptography

Symmetric Cryptography — The Shared Key Door

Imagine you and your friend have one special key that opens a locked box. You put a secret note inside the box and lock it with this key. Then you send the locked box to your friend. Since your friend has the same key, they can unlock the box and read the note.

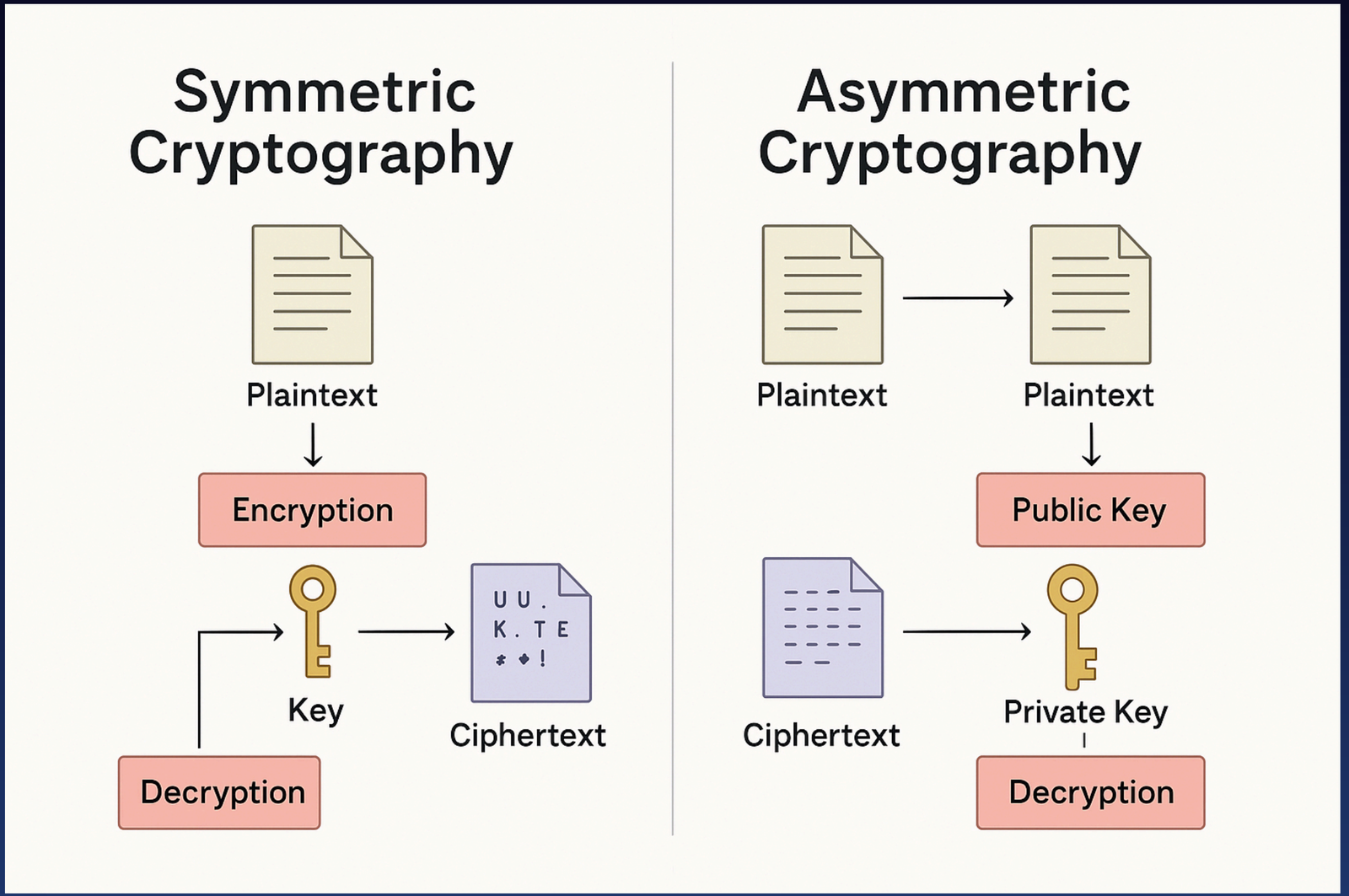
- **Problem**: You both need to meet beforehand to share that key safely. If someone else gets the key, they can open your box too.

Asymmetric Cryptography — The Locked Mailbox

Now imagine you have a mailbox with a slot that anyone can drop letters into, but only you have the key to open it and read the letters inside.

- You share the mailbox's slot (public key) openly with everyone. Anyone can use the slot to send you a message.
- But only you have the private key to open the mailbox and read the messages.
- **Advantage:** You don't need to share your private key with anyone. Others can send messages securely without needing a shared secret.

Types of Cryptography



Classical Ciphers

- Caesar Cipher (Shift letters by a fixed amount)
- Vigenère Cipher (Keyword-based shifting)
- Monoalphabetic Substitution (Replace each letter with another)

Classical Ciphers

Caesar Cipher

Definition:

A substitution cipher where each letter in the plaintext is shifted a fixed number of positions in the alphabet.

Purpose:

To hide the meaning of a message using a simple, consistent shift.

Method:

Choose a shift value (e.g., 3).

Replace each letter with the one that comes 3 places after it in the alphabet.

A → D, B → E, C → F, etc.

Wrap around from Z to A if needed.

Classical Ciphers

Caesar Cipher

Pros	Cons
Very simple and easy to understand	Very easy to break by brute force (only 25 possible shifts)
Quick to implement manually	Offers minimal security

Classical Ciphers

Substitution Cipher (Monoalphabetic)

Definition:

A cipher where each letter of the alphabet is replaced by a different, fixed letter or symbol.

Purpose:

To replace each letter with another according to a fixed system, more complex than Caesar.

Method:

- Create a substitution table (e.g., A → Q, B → L, C → G, etc.).
- Replace each letter in the plaintext using the table.
- One letter maps to one other letter.

Classical Ciphers

Substitution Cipher (Monoalphabetic)

Pros	Cons
More secure than Caesar (many more combinations — 26! possible keys).	Still vulnerable to frequency analysis.
Harder to break by brute force.	Creating and securely sharing the substitution table is challenging.

Classical Ciphers

Vigenère Cipher

Definition:

A polyalphabetic substitution cipher that uses a keyword to shift letters multiple times in different ways.

Purpose:

To improve security over Caesar by using multiple Caesar ciphers based on letters of a keyword.

Method:

- Choose a keyword (e.g., KEY).
- Repeat the keyword to match the length of the message.
- Each letter of the keyword determines a shift (K = shift 10, E = shift 4, Y = shift 24).
- Apply each shift to the corresponding letter of the plaintext.

Classical Ciphers

Vigenère Cipher

Pros	Cons
More secure than Caesar because it uses multiple shifts.	Still vulnerable to more advanced attacks (like Kasiski or frequency analysis if the keyword is short or reused).
Resistant to simple frequency analysis	Requires both sender and receiver to know the keyword.

Classical Ciphers

How these 3 Differ

Feature / Cipher	Caesar Cipher	Vigenère Cipher	Substitution Cipher
Cipher Type	Monoalphabetic	Polyalphabetic	Monoalphabetic
Key Type	Numeric shift (e.g., shift by 3)	Keyword-based shifting	Random fixed letter mapping
Key Example	Shift = 3	Keyword = "KEY"	A → Q, B → W, etc. (random)
Encryption Logic	Same shift for all letters	Shift amount varies per letter (based on keyword)	Each letter replaced by a different fixed letter
Alphabet Use	One shifted alphabet	Multiple shifted alphabets (based on keyword)	One jumbled alphabet
Pattern Detection	Easy to spot (frequency analysis works)	Harder to detect patterns	Patterns exist but harder to crack than Caesar

"Codebreaker Challenge"

Objective:

To decrypt a series of encrypted messages using the Caesar cipher. Each correct decrypted message unlocks a clue for the next challenge. The fastest ones wins!

Round 1: Easy (2 Min)

- Ciphertext: WKH FDW LV FXWH
- Clue: “Shift back by the number of legs on a tripod.”
- Shift: ?
- Plaintext:
- Next Clue: “Shift = sides of a square”

"Codebreaker Challenge"

Objective:

To decrypt a series of encrypted messages using the Caesar cipher. Each correct decrypted message unlocks a clue for the next challenge. The fastest ones wins!

Round 2 (Moderate) – 3 Min

- Ciphertext: XLMW MW E GLMPHS
- Clue: “Think of how many sides a square has.”
- Shift: ?
- Plaintext: ?
- Next Clue: “Shift = number of letters in the word ‘KEYWORD’”

"Codebreaker Challenge"

Objective:

To decrypt a series of encrypted messages using the Caesar cipher. Each correct decrypted message unlocks a clue for the next challenge. The fastest ones wins!

Round 3: Intermediate (4 min)

- Ciphertext: ULCLY ZOHYL WHZZDVYKLZ
- Clue: “Count the number of letters in the word ‘KEYWORD’.”
- Shift: ?
- Plaintext: ?
- Next Clue: “Multiply the number of continents (7) by 2”

"Codebreaker Challenge"

Objective:

To decrypt a series of encrypted messages using the Caesar cipher. Each correct decrypted message unlocks a clue for the next challenge. The fastest ones wins!

Round 4: Challenging - 4 min

- Ciphertext: QIH HVS UFSOH BSH
- Clue: “Double the number of continents = ?”
- Shift: ?
- Plaintext: ?
- Next Clue: “Oxygen’s atomic number” → 8

"Codebreaker Challenge"

Objective:

To decrypt a series of encrypted messages using the Caesar cipher. Each correct decrypted message unlocks a clue for the next challenge. The fastest ones wins!

Final Round: Boss Level (3 min)

- Ciphertext: UQAAQWV IKKWUXTQAPML
- Clue: “Oxygen’s atomic number = ?”
- Shift: ?
- Plaintext: ?

"Codebreaker Challenge"

Congratulations
You are “Master Decoder”

What We Learned Today

- What is cryptography? Why do we need it?
- Key terms: plaintext, ciphertext, encryption, decryption, key, algorithm
- Types: Symmetric vs Asymmetric
- Classical ciphers: Caesar, Vigenère, Substitution
- Gamified Activity

What We Learned Tomorrow

- Modern Cryptography & Real-World Applications
- Symmetric (AES) and Asymmetric (RSA, Public/Private keys)
- Hashing (SHA-256), digital signatures
- Where cryptography is used (banking, passwords, messaging apps)
- Gamified Challenge