

Welcome to this session:

Introduction to Cryptography and Cryptographic Algorithms

The session will start shortly...

Questions? Drop them in the chat.
We'll have dedicated moderators
answering questions.





What is Safeguarding?

Safeguarding refers to actions and measures aimed at protecting the human rights of adults, particularly vulnerable individuals, from abuse, neglect, and harm.



To report a safeguarding concern reach out to us via email:
safeguarding@hyperiondev.com

Live Lecture Housekeeping:

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- No question is daft or silly - ask them!
- For all non-academic questions, please submit a query:
www.hyperiondev.com/support
- To report a safeguarding concern reach out to us via email:
safeguarding@hyperiondev.com
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.



Lecture Overview

- Introduction to cryptography
- Cryptographic Algorithms



Learning Outcomes

- ❖ Define Cryptography
- ❖ Identify the Purposes of Cryptography
- ❖ Understand Key Cryptographic Concepts such as encryption, decryption, and hashing
- ❖ Recognise Real-World Applications of Cryptography

Cryptography

What are some reasons to want to hide information or data?



What is Cryptography?

Cryptography is the process of hiding or coding information so only the person who the message was intended for can read it.



Why do we use Cryptography?

- Privacy and Confidentiality
- Authentication
- Non-repudiation



Encryption

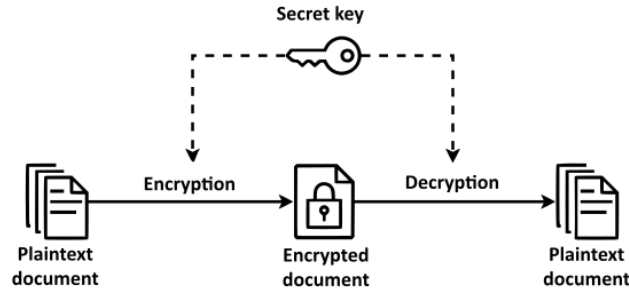
- Process of changing data, through mathematical processes, making it unreadable. The data can only be changed back by someone who has the correct key.

Encryption can be divided in 2 categories:

- Symmetrical
 - Uses the same key for both encryption and decryption
- Asymmetrical
 - Uses a private/public key pair for encryption and decryption.

Symmetrical Encryption

- Symmetrical encryption uses the same key for both encryption and decryption.
- **User A** encrypts a message using a key.
- **User A** can now send the encrypted message to **User B**
- **User B** can then use the key to decrypt the message and read it.



Advanced Encryption standard

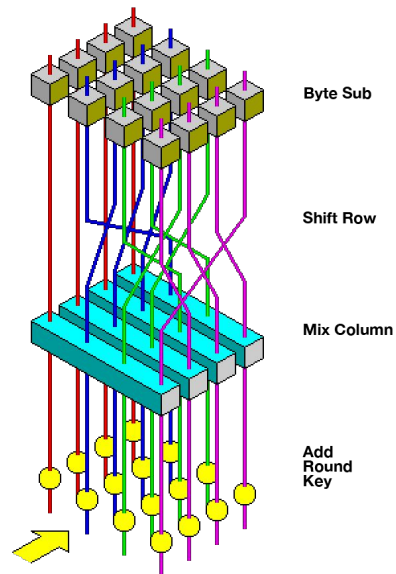
- Block cipher used by the US government to protect classified information.
- Split the message into smaller blocks of 128 bits each.
- Uses same key to encrypt and decrypt.



Advanced Encryption standard

Transformation Stages

- 1: Involves data substitution with a predefined cipher and a substitution table.
- 2: Data rows get shifted except for the first row.
- 3: Uses the Hill cipher to mix columns.
- 4: Block of data uses a small portion of the encryption key.



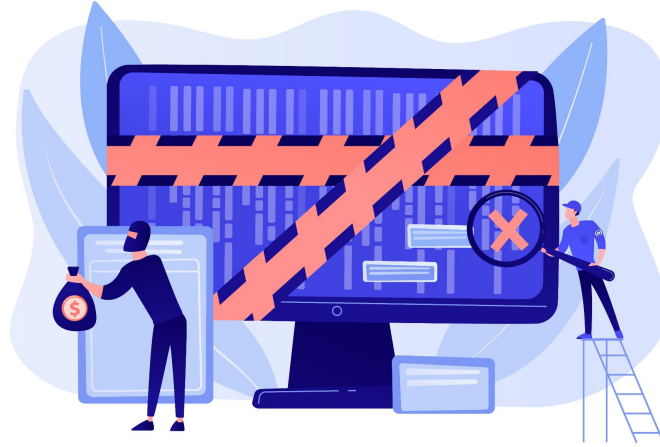
Advantages of AES

- Security
- Cost
- Implementation



AES Vulnerabilities

- Incorrect configuration.
- Not enough encryption rounds.
- Side channel attacks.

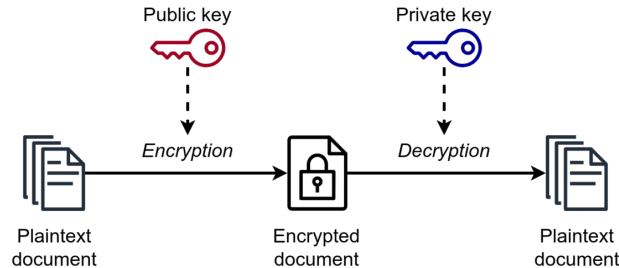


Asymmetrical Encryption

- Uses a private/public key pair for encryption and decryption.

User A wants to send a message to User B

- **User A** encrypts a message using **User B's** public key.
- **User A** can now send the encrypted message to **User B**
- **User B** can then use their private key to decrypt the message and read it.





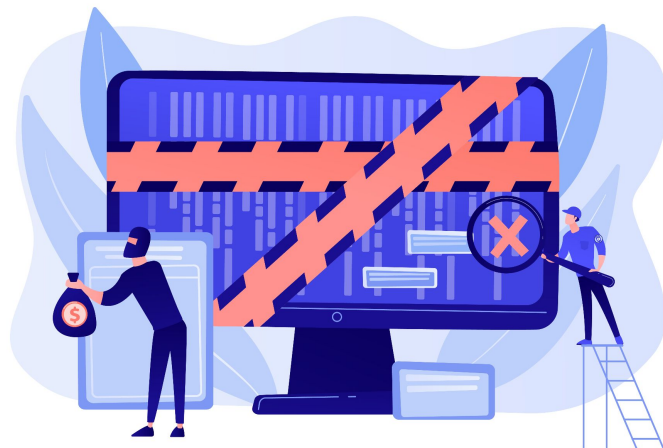
Let's take a break

Rivest Shamir Adleman (RSA)

- Protects data through encryption and decryption with private and public keys.
- Most widely used encryption mechanism in the world.
- Uses 2 very large prime numbers and performs a sequence of steps to produce a private and public key set that can be used.

Vulnerabilities

- Key sizes
- Future technology
- Side channel attacks
- Weak Random Number Generators



Use Cases

- Digital Signatures
- Digital Certificates
- Secure Communication Protocols



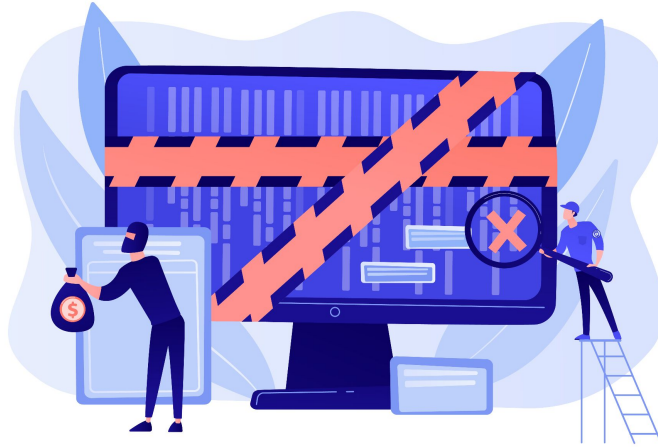
Keys and Key Management

Keys are at the centre point of our cryptography and protecting them should be off highest priority.



Vulnerabilities

- Weak keys
- Overused keys
- Using keys for multiple purposes
- Keys stored alongside Data
- Insider threats



Mitigating Risks

- We can mitigate risks using a key management system.



Consequences of Key Leaks

- Investigation costs
- Loss of sensitive data
- Financial losses
- Fines
- Reputational damage
- Some cases the business closes.



Hashing

- Hashing is the process of changing data into a fixed size string value called a hash.



Benefits

- Data retrieval
- Digital Certificates
- Password storing



Disadvantages

- Risk of collisions.
- Very difficult to reverse.
- Not very friendly with data that requires sorting.



Cryptography

How would life change if cryptography didn't exist?



Polls

Please have a look at the poll notification and select an option.

What is the primary purpose of cryptography?

- A. Data compression
- B. Data protection
- C. Data deletion
- D. Data sorting

Polls

Please have a look at the poll notification and select an option.

What type of key pair is used in asymmetric cryptography?

- A. Two public keys
- B. Two private keys
- C. A public key and a private key
- D. No key is required

Q & A SECTION

**Please use this time to ask
any questions relating to the
topic, should you have any.**

Thank you
for attending



HyperionDev