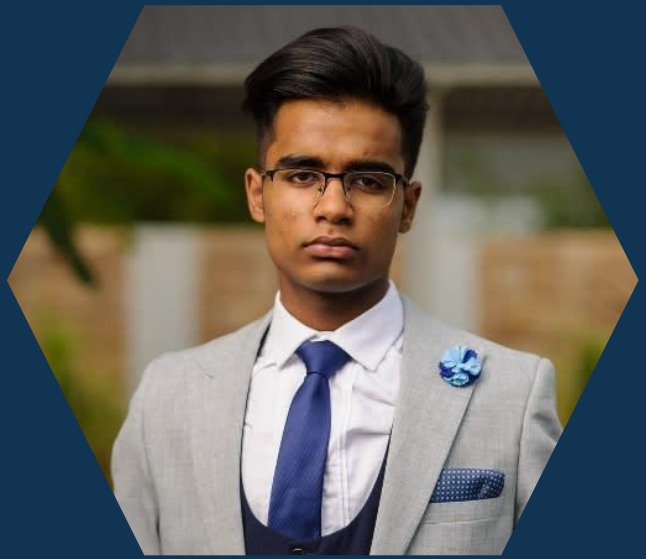
Ciphers

HyperionDev

Welcome



Lecturer: Liano Naidoo

Moderator: Zahir Junjeo

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Define Web Development
- Explore Front-End Developments and common Cyber-Risks
- Explore Back-End Developments and associated risks
- Differences

Objectives

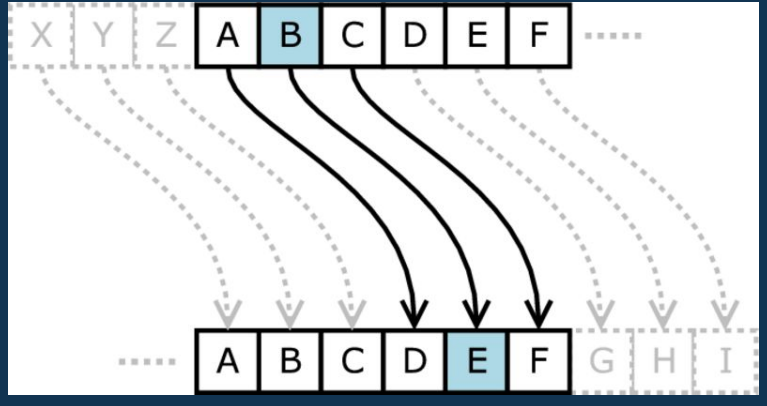
- Define Cryptographic Ciphers
- Symmetrical Ciphers + Examples
- Asymmetrical Ciphers + Examples
- Note some differences between the above :)
- Importance in CyberSecurity

What is a Cipher?

- A cryptographic cipher is an encryption and decryption algorithm. The purpose of a cipher is to make it challenging for unauthorized parties to access or read a message's content.

- In essence, it's a technique for encrypting a message so that only the intended audience can decipher it. This is accomplished by encrypting the message with a mathematical algorithm and decrypting it with a key. The message is just a jumbled mess of letters and numbers without the key.

What is a Cipher?



Symmetric Ciphers

- Where The same key is used by symmetric ciphers to encrypt and decrypt messages. This indicates that the key, which needs to be kept a secret, is shared by the sender and the recipient. Julius Caesar used the Caesar Cipher (Substitution Cipher)to encrypt messages and is one of the earliest instances of symmetric encryption. Which shifts each letter a specific number of positions in the alphabet. So "HELLO" becomes "KHOOR" if we move each letter three spaces. Simple, right?

- The Advanced Encryption Standard (AES), created by two Belgian cryptographers in 1998, is one of the most popular symmetric ciphers. AES is used to encrypt everything, including government secrets, military data and financial information. It is extremely challenging to crack because it uses keys that are either 192 or 256 bits long.

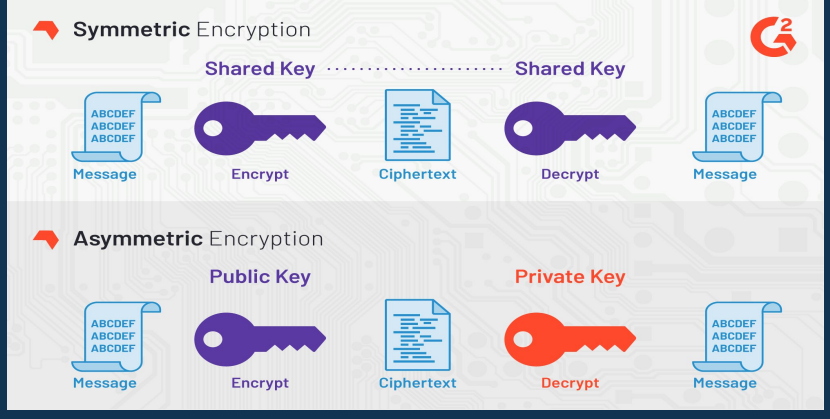
- The IBM-developed Data Encryption Standard (DES), which was created in the 1970s, is another widely used symmetric cipher. DES is frequently used in electronic banking and other financial transactions and has a key length of 56 bits.

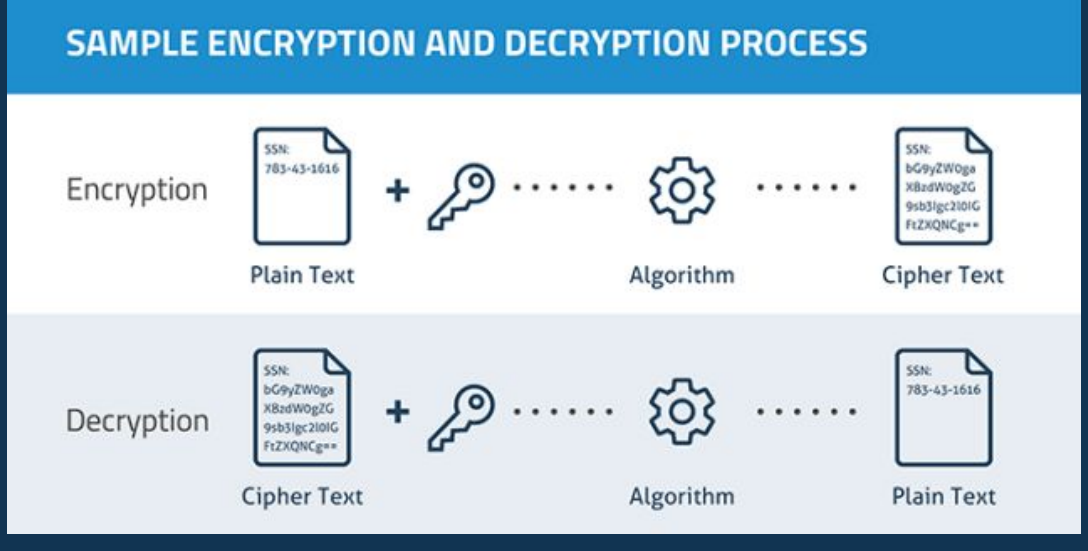
Asymmetric Ciphers

- Public-key cryptography(AKA Asymmetric), employs a pair of keys for both encryption and decryption. The private key is kept secret, while the public key is released. Only the owner of the private key is able to decrypt messages that are encrypted using the public key. This makes it possible to communicate securely without requiring a secret key to be shared between the sender and the recipient.

- The most popular asymmetric cipher is the RSA algorithm, which was created by Ron Rivest, Adi Shamir, and Leonard Adleman. For secure communications, including email, messaging services, and online transactions, RSA is frequently used.

- The Elliptic Curve Cryptography (ECC) algorithm, which generates the key pair using elliptic curves, is another illustration of an asymmetric cipher. For use in mobile devices, ECC is preferred over RSA because it is known to be more effective and swifter.


Symmetric Encryption
Shared Key
Shared Key
ABCDEF
ABCDEF
ABCDEF
Message
Encrypt
Ciphertext
Decrypt
ABCDEF
ABCDEF
ABCDEF
Message
Asymmetric Encryption
Public Key
Private Key
ABCDEF
ABCDEF
ABCDEF
Message
Encrypt
Ciphertext
Decrypt
ABCDEF
ABCDEF
ABCDEF
Message


SAMPLE ENCRYPTION AND DECRYPTION PROCESS
Encryption
SSN:
783-43-1616
Plain Text
Algorithm
SSN:
bG9yZWOga
XBzdWOgZG
9sb3lgc2l0IG
FtZXQNCg==
Cipher Text
Decryption
SSN:
bG9yZWOga
XBzdWOgZG
9sb3lgc2l0IG
FtZXQNCg==
Cipher Text
Algorithm
SSN:
783-43-1616
Plain Text

Question:

Which modern cipher do you think is the most secure and why?

Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

Math in Cryptography

- The area of mathematics known as number theory is concerned with the characteristics of numbers, particularly integers. Numerous cryptographic ciphers, including those based on prime numbers, modular arithmetic, and the Chinese Remainder Theorem, are important because of this.

- The area of mathematics known as linear algebra is concerned with the properties of systems of linear equations. It is crucial to cryptography because many contemporary ciphers are built on ideas from linear algebra, like vector spaces and matrix multiplication.

- The area of mathematics known as probability theory is concerned with the investigation of random events and their characteristics. It is crucial in cryptography because many ciphers, like those that use one-time pads and random key generation, rely on the unpredictable nature of random events and numbers.

Math in Cryptography

- The area of mathematics known as combinatorics is concerned with the investigation of discrete structures and their characteristics. It is crucial to cryptography because many ciphers, like substitution ciphers and permutations, rely on the combinatorial properties of permutations and combinations.

- Graph theory is the area of mathematics that examines graphs and their characteristics. Since many contemporary ciphers are based on graph theory ideas, such as the use of graphs to model encryption and decryption procedures, it is crucial to cryptography.

Cryptography in Cyber Security

- Sensitive data is protected from theft and unauthorized access thanks to the use of encryption. Encryption has become a crucial tool for protecting digital communications, transactions, and sensitive information in the current digital era, where data breaches and cyber attacks are frequent occurrences.

- Therefore, it is crucial for cybersecurity professionals to have a basic understanding of the mathematical concepts used in cryptography, such as modular arithmetic, prime numbers, and finite fields. It enables them to evaluate the security of a cryptographic system, spot any potential flaws, and suggest the necessary security precautions. They can then select the best cipher for a given use case.

Wrapping up

- Some into account when it comes to cryptography, such as the value of privacy and freedom of expression. Individuals' privacy and security are greatly protected by cryptography, which also enables them to communicate and share information without worrying about being monitored or intercepted.

- Nevertheless, it's also critical to understand that cryptography can be employed for immoral activities like terrorism and organized crime. As a result, it's critical to balance security and privacy while preventing the improper use of cryptography for illegal activities.

- Finally, it should be noted that symmetric and asymmetric ciphers are two distinct categories of encryption techniques that are crucial for protecting digital communication. While asymmetric ciphers use a public-private key pair to encrypt data, they are more secure than symmetric ciphers, which are easier to understand and use. When it comes to cryptography, it's crucial to strike a balance between the need for security and privacy and the need to stop crime while upholding British values like freedom of speech and privacy.

Next up

Cross Site Scripting (XSS)

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise