Cryptography

HyperionDev

VeraCrypt:

https://www.veracrypt.fr/en/Downloads.html

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:

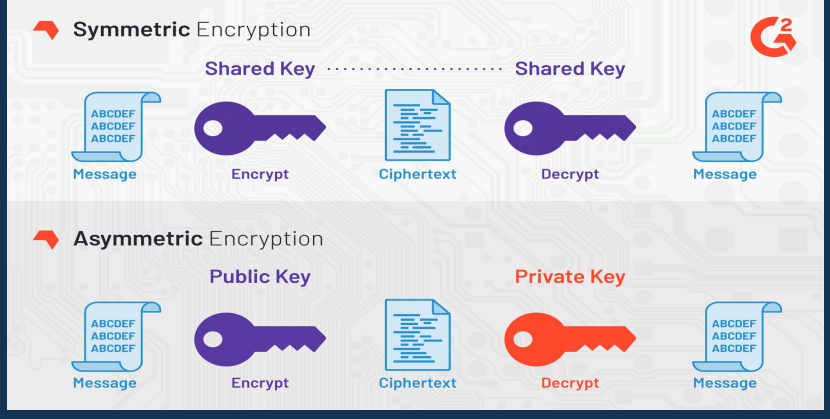
- Explored basic server configuration in Python (HTTP.server) and Apache :)

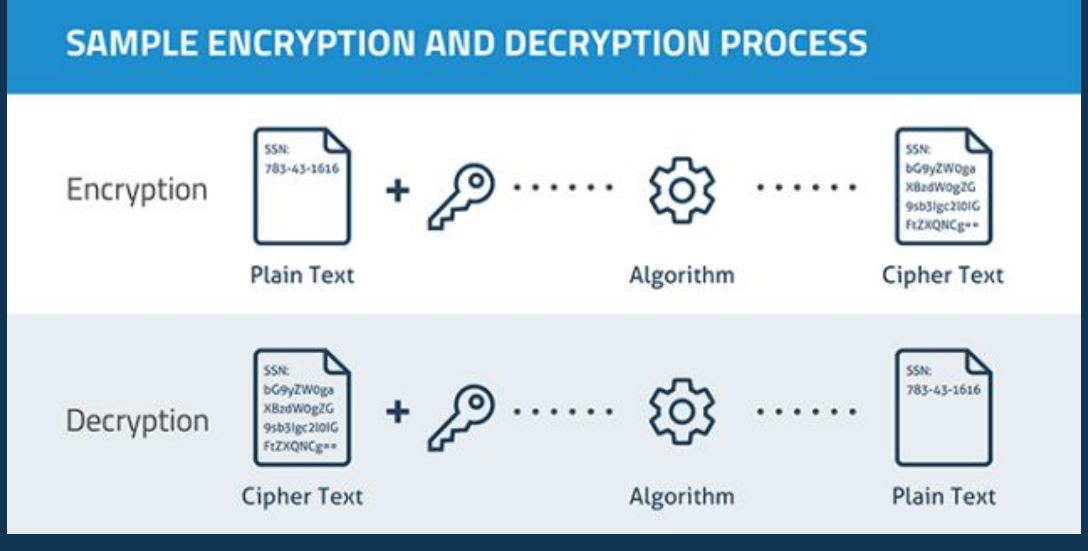
Objectives

Explore how we can practically implement:

- Hashing (using Python)
- Asymmetric Encryption (Using PuTTY)
- Symmetrical Encryption (Using VeraCrypt)

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


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 for the day:

Do you know how to create a virtual encrypted volume?

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.

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

Burp Suite Walkthrough

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

"With great power, comes great responsibility."