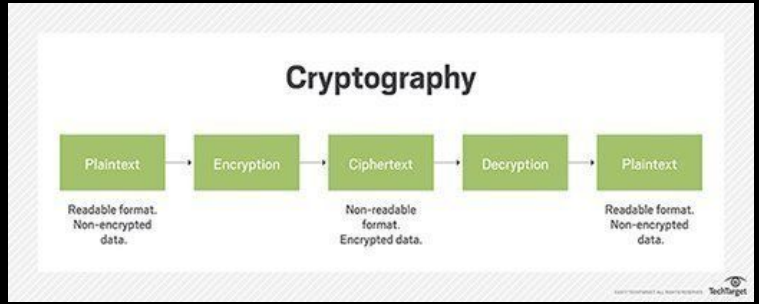
Cryptography

Parneet Singh

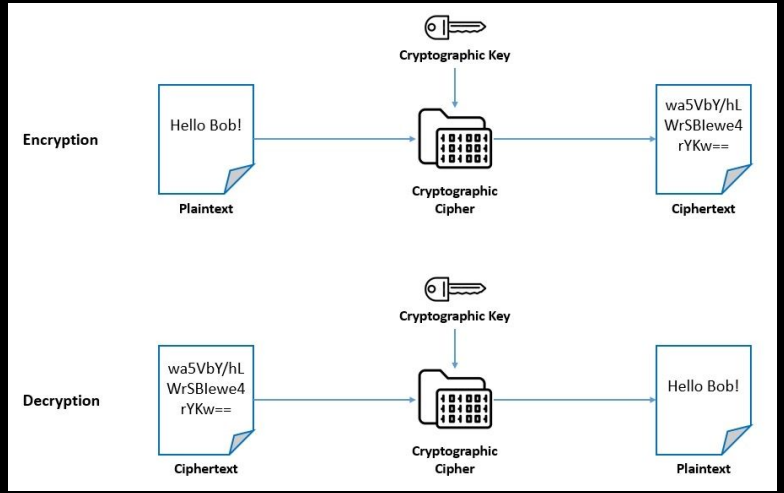
CS 131

Professor. Yuen Yuen



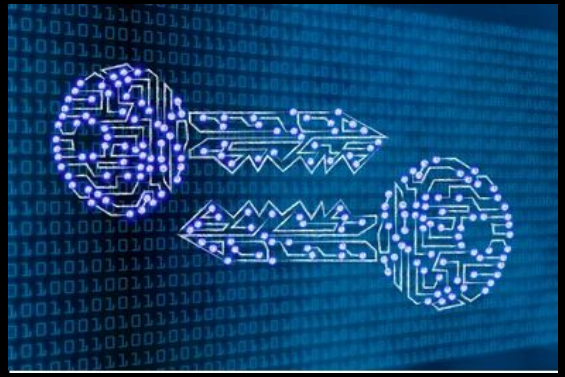
Introduction

- Cryptography is the science and practice of encoding and decoding information to protect its confidentiality and integrity. It is vital in securing information and communication by preventing unauthorized access, interception, and tampering, ensuring privacy and trust in our digital world.



Historical Background

- Cryptography has a long history dating back to ancient times. One of the earliest known methods is the Caesar cipher, used by Julius Caesar to encrypt his military messages. This technique involved shifting each letter of the alphabet by a fixed number of positions.
- Substitution techniques, such as the Atbash cipher and Polybius square, were also prevalent. These methods involved replacing letters with other symbols or using grids to map letters to coordinates. Throughout history, cryptography has played a crucial role in securing sensitive information and communication.

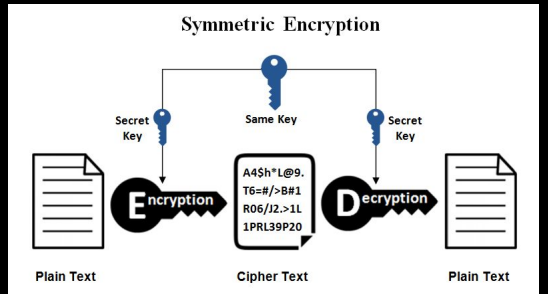


Cryptographic Terminology

- Ciphertext: It is the result of encrypting the plaintext using a cryptographic algorithm. Ciphertext is unintelligible and cannot be understood without proper decryption.
- Encryption: Encryption is the process of converting plaintext into ciphertext using a specific algorithm and a key. It ensures that the information is transformed into a form that is not readily understandable to unauthorized individuals.
- Decryption: Decryption is the reverse process of encryption. It involves converting the ciphertext back into plaintext using the corresponding algorithm and key. Decryption allows authorized individuals to recover the original message.
- Keys: Keys are essential components in cryptographic algorithms. They are unique and secret values used to control the encryption and decryption process. The same key is typically required for both encryption and decryption. The choice and management of keys are critical for ensuring the security of encrypted data.
- The secrecy and complexity of the key play a vital role in maintaining the confidentiality and integrity of the encrypted information.

Symmetric Key Cryptography

- Symmetric key cryptography is a type of encryption where the same key is used for both the encryption and decryption processes. The sender and receiver share a secret key that they keep confidential.
- To encrypt a message, the sender applies the shared key to the plaintext, producing the ciphertext. The receiver, in turn, applies the same key to the ciphertext, decrypting it back into the original plaintext.
- Symmetric key algorithms include DES (Data Encryption Standard), AES (Advanced Encryption Standard), and 3DES (Triple Data Encryption Standard). These algorithms employ mathematical operations on blocks of data using the shared key to provide secure encryption and decryption capabilities.



Asymmetric Key Cryptography

- Asymmetric key cryptography, also known as public-key cryptography, is a cryptographic method that uses a pair of mathematically related keys for encryption and decryption.
- In this system, each user has a pair of keys: a public key and a private key. The public key is freely shared with others, while the private key is kept secret.
- To encrypt a message, the sender uses the recipient's public key. Only the corresponding private key can decrypt the ciphertext back into plaintext. This ensures that only the intended recipient, who possesses the private key, can decrypt and access the message.
- Asymmetric key algorithms include RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). RSA is based on the mathematical properties of large prime numbers, while ECC relies on the algebraic structure of elliptic curves. These algorithms provide secure encryption and digital signature capabilities, supporting the integrity and authenticity of digital communication.

Hash Functions

- Hash functions are cryptographic algorithms that take an input (data) and produce a fixed-size output called a hash value or digest. The key characteristics of hash functions are determinism and preimage resistance.
- Hash functions play a crucial role in ensuring data integrity and digital signatures. In terms of data integrity, a hash function generates a unique hash value for each unique input. Any change in the input data, no matter how small, will result in a completely different hash value. This property allows for easy verification of data integrity by comparing the computed hash value with the original hash value.
- Commonly used hash functions include MD5 (Message Digest Algorithm 5) and SHA-256 (Secure Hash Algorithm 256-bit). However, it's important to note that MD5 is now considered weak and vulnerable to collision attacks, while SHA-256 is widely used and considered more secure for various applications.

Digital Signatures

- Digital signatures are cryptographic mechanisms that provide authenticity and integrity to digital documents or messages. They ensure that the sender of the document is verified, and the document has not been altered during transit.
- To generate a digital signature, the sender uses a hash function to create a unique hash value or digest of the document. The sender then encrypts this hash value with their private key, creating the digital signature. This signature is attached to the document and sent to the recipient.
- Digital signatures provide a secure way to verify the origin and integrity of digital documents, ensuring that they have not been modified and that they come from the claimed sender.

Key Exchange Protocols

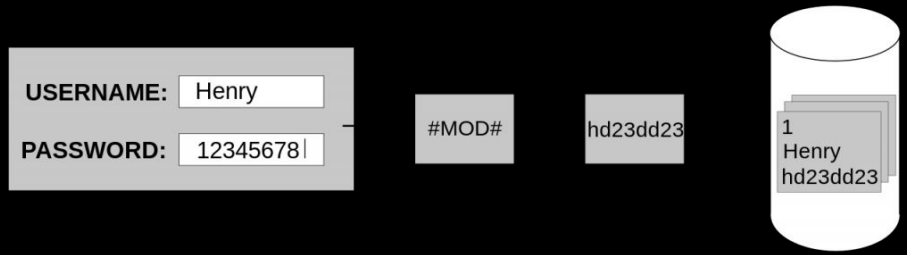
- Securely exchanging keys is a critical challenge in cryptographic systems. The main concern is ensuring that the shared key remains confidential and protected from unauthorized access or interception.
- Secure key exchange is crucial for secure communication because it ensures that only authorized parties possess the shared key needed for encryption and decryption. Without a secure key exchange mechanism, communication can be vulnerable to eavesdropping, man-in-the-middle attacks, and unauthorized access to sensitive information. Therefore, establishing a secure and confidential key exchange is essential to maintain the confidentiality and integrity of the communication.

Cryptographic Attacks

- Common cryptographic attacks include: Brute force attack, Known-plaintext attack, Chosen-plaintext attack.
- Side-channel attacks are another class of attacks that exploit information leaked through indirect channels, such as timing or power consumption. Examples include: Timing attacks, Power analysis,
- Choosing strong cryptographic algorithms is crucial to withstand these attacks. Strong algorithms have undergone rigorous analysis and are designed to resist known attack methods. They provide increased resistance to brute force attacks, have robustness against known-plaintext and chosen-plaintext attacks, and are resistant to side-channel attacks.
- By using strong cryptographic algorithms, organizations can enhance the security of their systems and protect sensitive information from being compromised by attackers.

Applications of Cryptography

- Cryptography has numerous real-world applications that play a crucial role in ensuring security and privacy. Here are a few examples: Secure Communication, E-commerce, Data Protection, Email Encryption, Virtual Private Networks (VPNs),
- These applications demonstrate the importance of cryptography in securing communications, protecting data, and facilitating trust in various domains of our digital world.



Future Trends in Cryptography

- Emerging trends in cryptography include:
- Post-Quantum Cryptography: With the advent of quantum computers, post-quantum cryptography focuses on developing algorithms that can resist attacks from quantum computers.
- Homomorphic Encryption: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it.
- Zero-Knowledge Proofs: Zero-knowledge proofs allow one party (the prover) to prove the validity of a statement to another party (the verifier) without revealing any other information.
- Multi-Party Computation: Multi-party computation enables secure computations on data held by multiple parties without revealing individual inputs. It finds applications in scenarios where data privacy is crucial, such as collaborative data analysis and secure auctions.
- These advancements in cryptography address new challenges and opportunities in privacy, security, and data protection, paving the way for enhanced confidentiality, integrity, and trust in various domains.

Conclusion

- The presentation covered the concept of cryptography as the practice of securing information through encryption and decryption techniques. It highlighted the importance of cryptography in securing digital information and communication by ensuring confidentiality, integrity, and authenticity.
- The presentation discussed various cryptographic methods, such as symmetric and asymmetric encryption, hash functions, and key exchange protocols. It also mentioned real-world applications like secure communication, e-commerce, and data protection.
- Lastly, the presentation touched upon emerging trends, including post-quantum cryptography and homomorphic encryption. Overall, cryptography plays a critical role in safeguarding sensitive data and fostering trust in our digital world.

References

- https://research.ibm.com/topics/cryptography
- https://www.cylab.cmu.edu/research/cryptography.html
- https://crypto.cs.washington.edu/