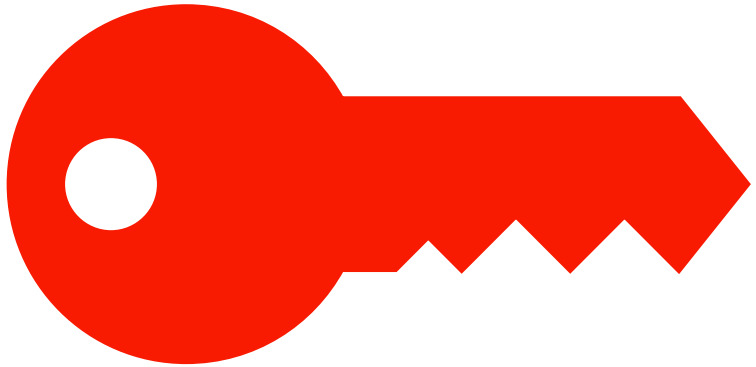


Cryptography

Introduction

Cryptography is the practice and study of secure communication techniques, ensuring that third parties or the public cannot access private information

Importance of Information Security: In the digital age, where data is the new currency, protecting information is crucial to prevent unauthorized access, tampering, or theft.

What is Cryptography?

Encryption involves converting **plaintext** into **ciphertext** using an algorithm and a secret **key**.

Key Terminology (Plaintext, Ciphertext, Key): **Plaintext** is the original readable data, **ciphertext** is the encrypted data, and the **key** is the secret parameter used in encryption and decryption.

Confidentiality, Integrity, Authentication: Cryptography aims to achieve confidentiality by keeping information private, integrity by ensuring data remains unaltered, and authentication by verifying the identities of parties involved in communication.

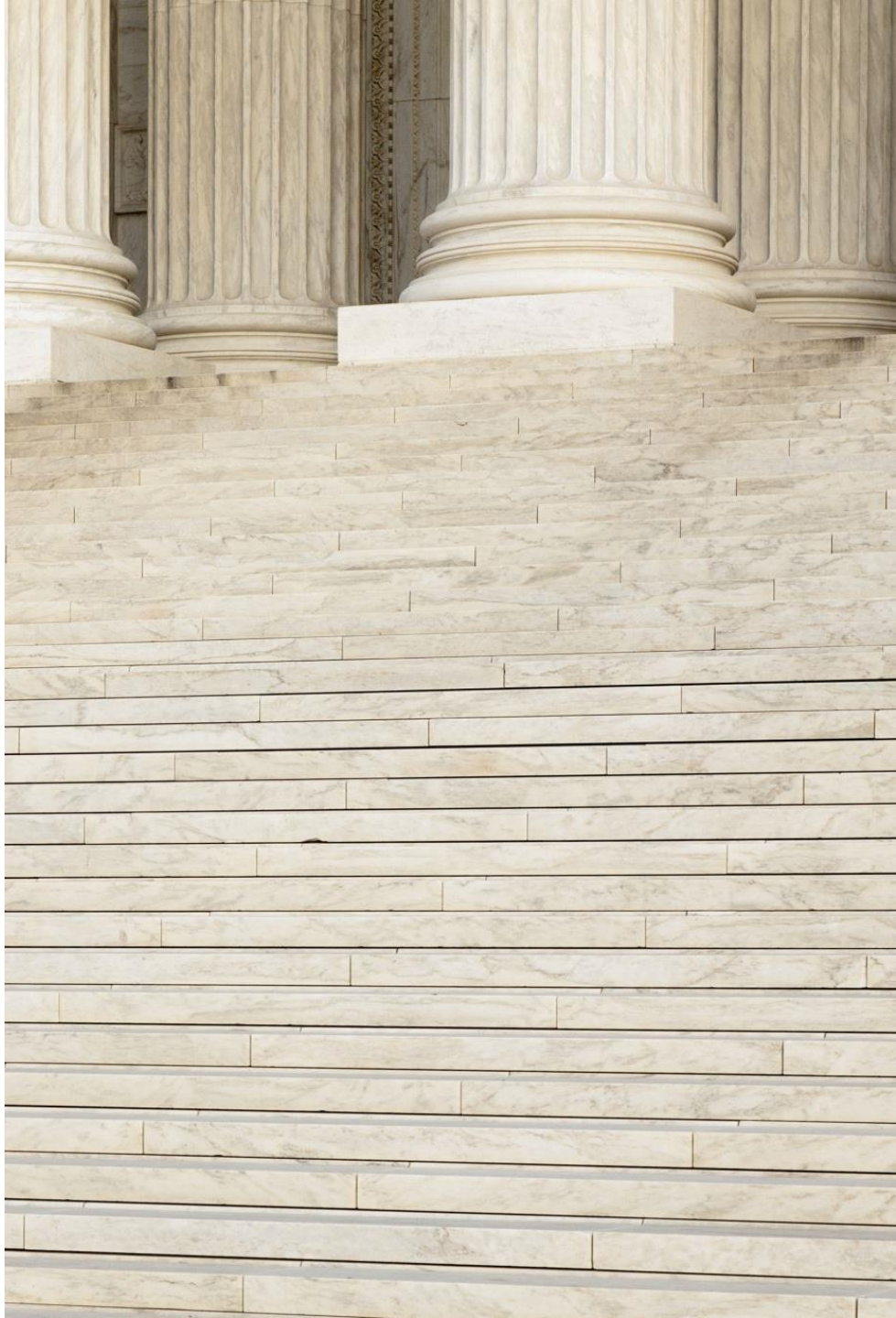
History of Cryptography

Ancient Cryptography: Early methods such as the Caesar cipher, used by Julius Caesar to protect military messages.

Modern Cryptography: Advancements in the 20th century, including the Enigma machine and the development of mathematical principles.

World War Era and Codebreaking: The pivotal role of cryptography in World War II and subsequent codebreaking efforts.

Public-Key Cryptography: A revolutionary concept introduced by Whitfield Diffie and Martin Hellman in 1976.



Types of Cryptography

Symmetric Cryptography: Uses a single key for both encryption and decryption, faster but requires secure key distribution.

Asymmetric Cryptography: Involves a pair of keys (public and private), offering secure key exchange but slower than symmetric.

Hash Functions: Produces a fixed-size output (hash) for any input, commonly used for data integrity verification.

Cryptographic Algorithms

DES, 3DES, and AES: Symmetric key algorithms for data encryption.

RSA, ECC, and DSA: Asymmetric key algorithms for secure communication and digital signatures.

SHA-256, MD5, and HMAC: Hash functions used for data integrity and authentication.

Cryptographic Applications

Secure Communication: Using encryption to protect sensitive information during transmission.

Data Encryption: Safeguarding data at rest to prevent unauthorized access.

Digital Signatures: Verifying the authenticity and integrity of digital messages.

SSL: Securing web communications for online transactions and data transfer.

VPNs: Creating secure, private networks over the internet for remote access.

Security Considerations

Key Management: Ensuring secure generation, distribution, and storage of cryptographic keys.

Cryptanalysis: The study of analyzing and breaking cryptographic systems.

Quantum Computing Threats: Potential risks to current cryptographic algorithms posed by quantum computers.

Social Engineering: Manipulating individuals to disclose confidential information.

zSystems: End to End Encryption

z/OS Data Set Encryption: the IBM z16 provides quantum-safe AES256 encryption for data at rest with no application updates

Application Transparent TLS (AT-TLS): provides network encryption for data in motion with few or no application updates

zSystem TKE

TKE: Trusted Key Entry

TKE was developed to provide compliant-level hardware-based HSM management and streamline management in complex environments.

TKE has a 1-to-Many relationship with IBM Z and LinuxONE servers.

TKE simplifies HSM management tasks and enforces security mechanisms such as dual controls and smart cards.