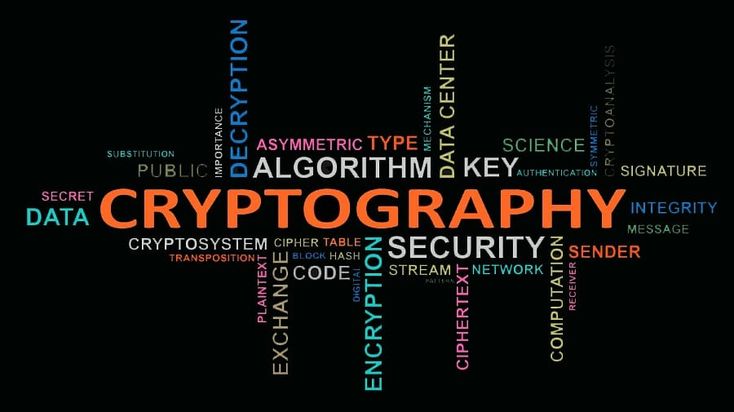
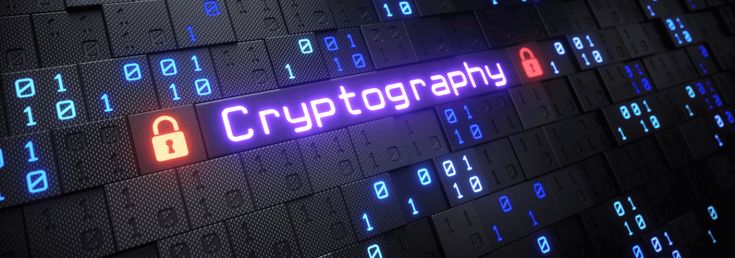
**CTF Challenge: Cryptography**

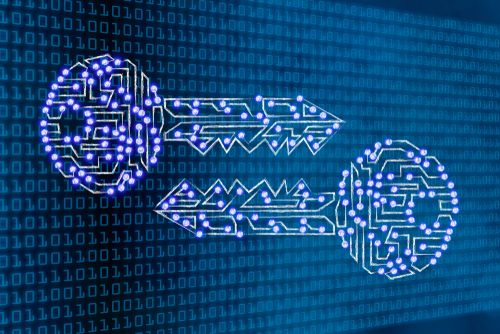
****

**Cryptography?**

****

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. It involves creating written or generated codes that allow information to be kept secret. Here’s an overview of key concepts in cryptography:

### **Key Concepts of Cryptography**



1. **Encryption**:
   * **Symmetric Encryption**: Uses the same key for both encryption and decryption. Example: AES (Advanced Encryption Standard).
   * **Asymmetric Encryption**: Uses a pair of keys, a public key for encryption, and a private key for decryption. Example: RSA (Rivest-Shamir-Adleman).
2. **Hash Functions**:
   * Produce a fixed-size hash value from input data of any size. Used for data integrity and authentication. Example: SHA-256 (Secure Hash Algorithm 256-bit).
3. **Digital Signatures**:
   * Provide authentication, data integrity, and non-repudiation. They use asymmetric encryption where the sender's private key is used to sign the message and the public key is used to verify the signature.
4. **Public Key Infrastructure (PKI)**:
   * A framework for managing digital keys and certificates. Ensures secure exchange of information over networks.
5. **Cryptographic Protocols**:
   * **SSL/TLS**: Secure Sockets Layer / Transport Layer Security, used for secure communication over a computer network.
   * **PGP**: Pretty Good Privacy, used for securing emails.

# **Capture the Flag (CTF) Challenges**

**Flag 1. What encryption standard uses the same key for both encryption and decryption?**

Answer: AES

**Flag 2. Which cryptographic algorithm is commonly used for creating digital signatures?**

Answer: RSA

**Flag 3. What cryptographic hash function produces a 256-bit output?**

Answer: SHA-256

**Flag 4. What is the protocol used to secure communication over a computer network?**

Answer: TLS

**Flag 5. What framework manages digital keys and certificates for secure information exchange?**

Answer: PKI