

**قــســــــــــم الأمــــــــــــــــــــــــــن الــــــــــــــــــــــــــــــــــــسيبرانــــــــــــــــــــــــــــــــــــي**

**Department of Cyber Security**

**Subject:**

**Principles of Cyber Security**

**Class:**

**First**

**Lecturer:**

**Muntather AL-mussawee**

**Lecture: (9)**

**Components of Encryption System**

**Encryption Algorithms**

**Hill Cipher**

**Definition:**

* The Hill cipher is a classical encryption method based on linear algebra, utilizing matrices and matrix multiplication to encrypt and decrypt texts. It was invented by the American mathematician Lester Hill in 1929.

**كيفية عمل طريقة Hill للتشفير؟**

**1. تحديد حجم الكتلة (Block Size):**

**يتم تقسيم النص الأصلي إلى كتل من الأحرف بطول n على سبيل المثال، كتلتين أو ثلاث أو أربع حروف في كل مرة.**

**2. إنشاء مصفوفة المفتاح (Key Matrix):**

**يتم اختيار مصفوفة مربعة ((n × n تحتوي على أعداد صحيحة وتكون قابلة للعكس (Invertible)**

**في الحسابات ضمن حسابيات المودولو ((mod 26**

**3. تحويل الأحرف إلى أرقام:**

**يتم تحويل كل حرف إلى رقم مطابق في الأبجدية (A = 0, B = 1, C = 2, ... , Z = 25).**

**4. القيام بعملية الضرب المصفوفي:**

**يتم ضرب مصفوفة المفتاح في مصفوفة النص الأصلي، ثم أخذ النتيجة مود 26 للحصول على القيم المشفرة.**

**5. تحويل الأرقام إلى حروف:**

**يتم تحويل الأرقام الناتجة إلى أحرف للحصول على النص المشفر.**

**Encryption**













**Modern Encryption Methods and How They Work**

* Modern encryption relies on advanced mathematical algorithms and digital techniques to ensure data security. It is generally categorized into three main types:
1. **Symmetric Encryption**
2. **Asymmetric Encryption**
3. **Hashing Encryption (used for data integrity verification)**

**1-Symmetric Encryption**

Uses a single key for both encryption and decryption.

Fast and efficient but faces the challenge of securely sharing the key.

**Popular Algorithms:**

**A. Advanced Encryption Standard (AES)**

Based on substitution and permutation matrices.

Uses key sizes of 128, 192, or 256 bits.

Commonly used in Wi-Fi security, VPNs, mobile applications, and banking transactions.

**B. Triple DES (3DES)**

An improved version of the old DES algorithm, encrypting data three times for enhanced security.

Used in legacy systems but less secure than AES.

**C. Blowfish & Twofish**

Open-source, fast encryption algorithms.

Twofish is an improvement over Blowfish and is widely used in modern security applications.

**2-Asymmetric Encryption**

Uses two different keys:

A public key for encryption.

A private key for decryption.

More secure but slower than symmetric encryption.

**Popular Algorithms:**

**A. RSA (Rivest-Shamir-Adleman)**

Based on prime factorization of large numbers.

Used in secure communications, HTTPS, and encrypted emails.

Slow but highly secure when using 2048-bit or larger keys.

**B. Diffie-Hellman (DH) Key Exchange**

Establishes a shared secret key between two parties without transmitting the key itself.

Used in VPNs and security protocols.

**C. Digital Signature Algorithm (DSA)**

Used for digital signatures to ensure data integrity.

Common in electronic transactions and digital certificates.

**3-Hashing Encryption**

One-way encryption that cannot be reversed, generating a unique fingerprint for data.

Used in password protection, file integrity verification, and digital signatures.

**Popular Hashing Algorithms:**

**A. MD5 (Message Digest 5)**

Produces a 128-bit hash value, but it is no longer secure against modern attacks.

**B. SHA (Secure Hash Algorithm)**

Available in different versions: SHA-1, SHA-256, SHA-512.

SHA-256 is widely used in Bitcoin, blockchain, and network security.

**C. bcrypt & Argon2**

Used for password hashing, adding a salt to make brute-force attacks harder.