



DATA SECURITY & CRYPTOGRAPHY FOURTH STAGE

***University of Basrah
College of Education for Pure Science
Computer Science Department***

***Prof. Dr. Eng. Hamid AL-Asadi
2016-2017***





DATA SECURITY & CRYPTOGRAPHY

- General Introduction
 - Introduction to Number Theory
 - *Classical Encryption Techniques*
- Block Ciphers and Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Stream Cipher
- Public-Key Cryptography and Rivest-Shamir-Adleman Algorithm (RSA)
 - Key Managements
 - Hash Algorithms
 - Digital Signatures

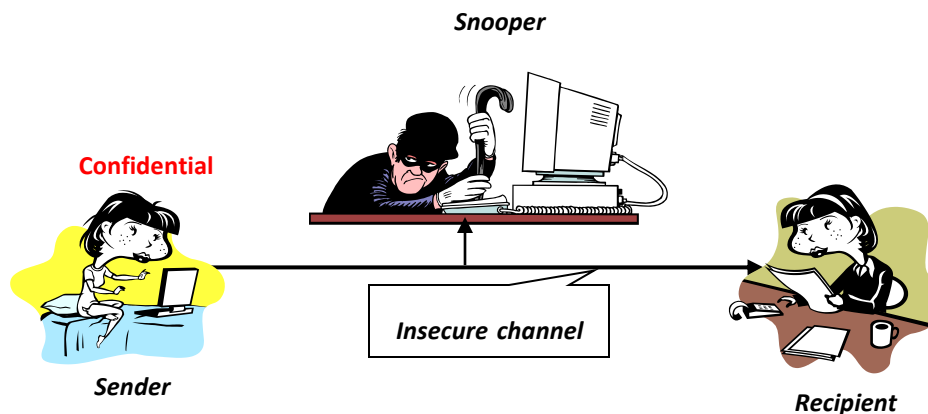
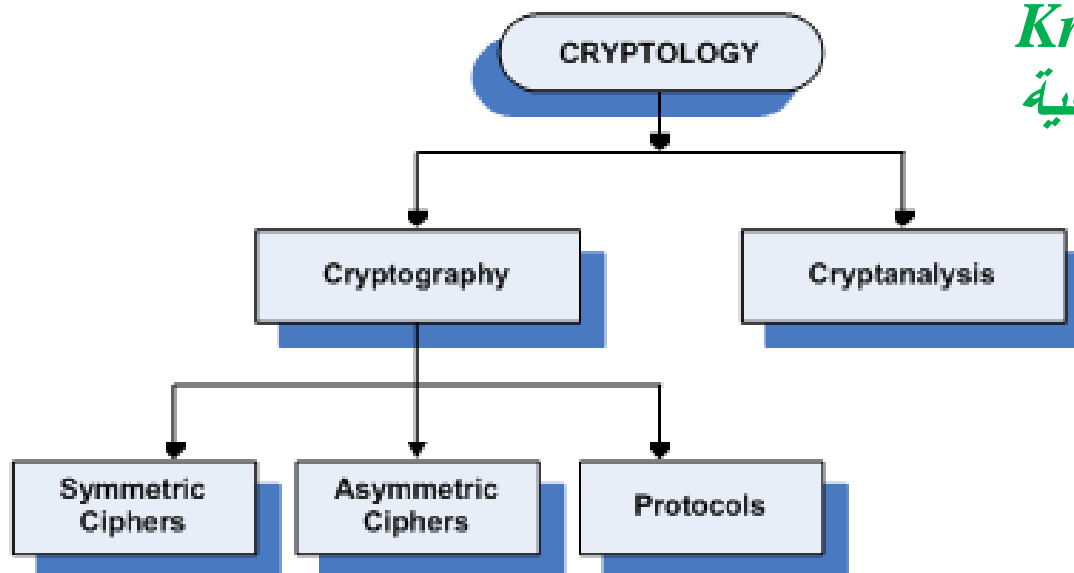
WHAT IS *DATA SECURITY*???

- *General Introduction*
- ❖ *Data security*
- ❖ *Categorizing security*
- ❖ *Overview of Cryptology*



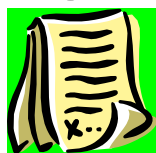
Overview of the field of cryptology

Kryptus logo
الكتابة المخفية



Encryption & decryption

Original Text



+

Secret key



=

Encrypted Text



Encryption

Encrypted Text



+

Secret key



=

Original Text



Decryption





• *Number Theory*

❁ *Numbers in different bases*

❁ *Time estimates for doing arithmetic*

❁ *prime numbers*

❁ *composite numbers*

• ❁ *The greatest common divisor GCD & the least common multiple LCM*

❁ *Modular arithmetic*

❁ *Euler phi-function $\varphi(n)$*

❁ *relatively prime*

❁ *The Euclidean algorithm*

❁ *Euclid's Extended Algorithm*



Classical Encryption Techniques

1. Substitution encryption techniques

the plaintext $x = (x_0, x_1, \dots, x_{n-1})$

are substituted by the letters in a ciphertext alphabet:

$$x = (x_0, x_1, \dots, x_{n-1}) \rightarrow (y_0, y_1, \dots, y_{n-1}).$$

2. Transposition Encryption Techniques

Ciphertext results when the positions of letters in the plaintext

$$x = (x_0, x_1, \dots, x_{n-1})$$

are rearranged $(x_0, x_1, \dots, x_{n-1}) \rightarrow (x_{\pi_0}, x_{\pi_1}, \dots, x_{\pi_{n-1}})$

according to a permutation $\pi = (\pi_0, \pi_1, \dots, \pi_{n-1})$.



Substitution Encryption Techniques

❁ *Monoalphabetic substitution ciphers.*

❁ *Homophonic substitution ciphers.*

❁ *Polygraphic substitution ciphers.*

❁ *Polyalphabetic substitution ciphers.*

❁ Monoalphabetic substitution ciphers.

Shift cipher



• *Caesar Cipher*

General monoalphabetic
substitution/Random letter pairs



random permutation

❁ Polygraphic substitution ciphers.



Playfair Chipper

❁ Polyalphabetic substitution ciphers.



Vigenere technique

❁ *Cryptanalysis of the Substitution Cipher*

The frequency analysis



The Transposition Cipher



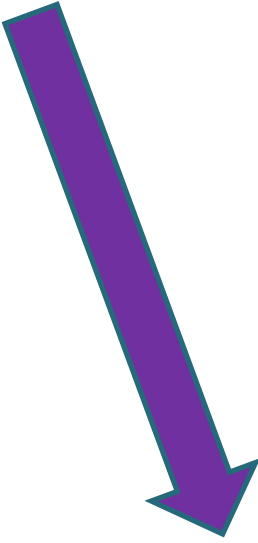
*Permutation
Cipher*



*Columnar
transposition
cipher*



**Double
columnar
transposition**



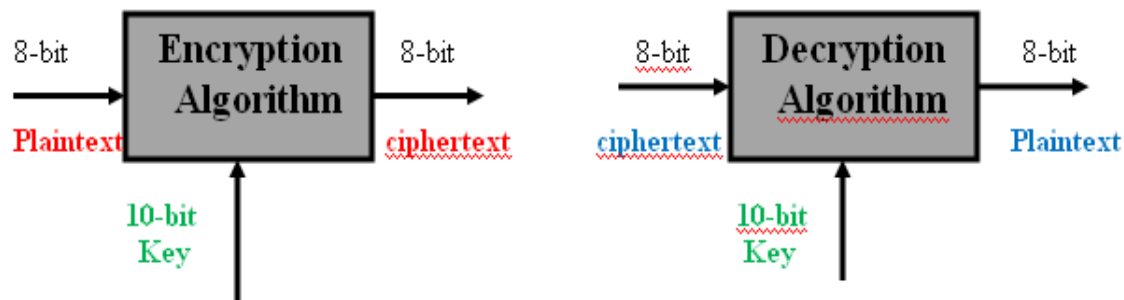
**Digraph
columnar
transposition**

Block cipher and data encryption standard

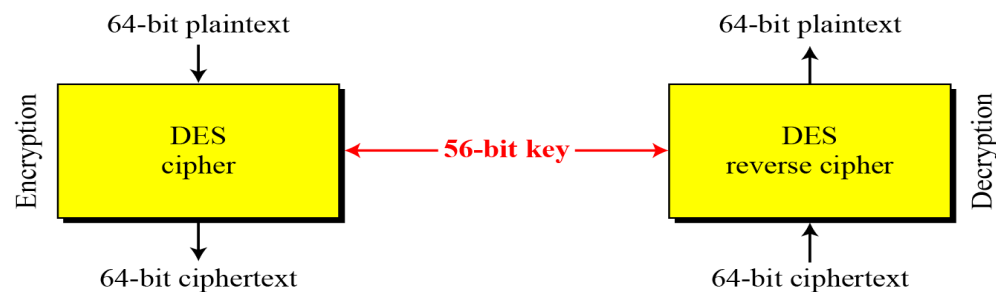
- *Simplified Data Encryption Standard (SDES)*
- *Data Encryption Standard (DES)*
- *The Advanced Encryption Standard (AES)*

SDES

- An initial permutation (IP);
- A complex function
- A simple permutation function that switches (SW) the two halves of the data
- A complex function
- A permutation function that is inverse of the initial permutation.



DES



AES

	Key Length (<i>Nk words</i>)	Block Size (<i>Nb words</i>)	Number of Rounds (<i>Nr</i>)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14



Public-Key Cryptography



Goals

- ❑ To review public-key cryptography.
- ❑ To demonstrate that **confidentiality** and **authentication** can be achieved simultaneously with public-key cryptography.
- ❑ To review the **R**ivest-**S**hamir-**A**dleman (**RSA**) algorithm for public-key cryptography





- **Key Managements**
- *Message Authentication*
- **Hash Algorithms**
- *Digital Signatures*



REFERENES

- **Allen, Julia H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison.**
- **Layton, Timothy P. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications.**
- **McNab, Chris (2004). Network Security Assessment. Sebastopol, CA: O'Reilly. Peltier.**
- **Thomas R. (2001). Information Security Risk Analysis. Boca Raton, FL: Auerbach publications.**
- **F. L. Bauer (2007). Decrypted Secrets: Methods and Maxims of Cryptology. Springer, 4th edition.**
- **N. Biggs (2002). Discrete Mathematics. Oxford University Press, New York, 2nd edition.**
- **C. Cid, S. Murphy, and M. Robshaw (2006). Algebraic Aspects of the Advanced Encryption Standard, Springer.**
- **Bart Preneel. MDC-2 and MDC-4. In Henk C. A. van Tilborg, editor, Encyclopedia of Cryptography and Security. Springer, (2005).**
- **T. Collins, D. Hopkins, S. Langford, and M. Sabin (1997). Public key cryptographic apparatus and method. United States Patent US.**
- **Yehuda Lindell (2003). Composition of Secure Multi-Party Protocols: A Comprehensive Study, Springer.**
- **W. Stallings (2005). Cryptography and Network Security: Principles and Practice. Prentice Hall, 4th edition.**

• 2016 – 2017 *University of Basrah - College of Education for Pure Science -
Computer Science Department*

Prof. Dr. Eng. Hamid Ali AL-Asadi



Thank you for your Attention ●