

CYB650

Introduction to Cryptography An Overview



Prepared by Dr. Esraa Saleh Alomari
Orientation lecture



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

اهلا ومرحباً بكم طلبتنا الاعزاء في
مادة

INTRODUCTION TO CRYPTOGRAPHY



الاستاذ المساعد الدكتورة اسراء صالح حسون
تخصص علوم حاسبات / أمنية شبكات
من جامعة العلوم الماليزية
العراق / واسط

esraaalomari@esu.ac.ae

Welcome To The Course

Dr. Esraa Alomari

Modules

There are five modules during this course are as follows:

- *Module 1: Foundations and principles of Cryptography*
- *Module 2: Cryptography protocols*
- *Module 3: Cryptography techniques*
- *Module 4: Cryptography Algorithms*
- *Module 5: Public key Algorithms*



The Part 1 of the module 1 which is (Lecture 1) covers the basics of Foundations and principles of Cryptography are as follows:

- *Story of Cryptography*
- *Definitions*
- *Encryption & Decryption*
- *Strong Cryptography*
- *How does Cryptography work?*
- *Classical encryption techniques*
- *Symmetric Cipher Model*



The Part 2 of the module 1 which is (Lecture 2) covers the basics of Foundations and principles of Cryptography (Number Theory) are as follows:

- *Divisibility and The Division Algorithm*
- *The Euclidean Algorithm*
- *Modular Arithmetic*
- *Groups, Rings, and Fields*
- *Finite Fields of the Form $GF(p)$*
- *Polynomial Arithmetic*
- *Finite Fields of the Form $GF(2^n)$*



The Part 1 of the module 2 which is (Lecture 3) covers The Transport-Level Security are as follows:

- ❑ **Web Security Considerations**
 - **Web Security Threats**
 - **Web Traffic Security**
- ❑ **Secure Sockets Layer**
 - **SSL Architecture**
 - **SSL Record Protocol**
 - **Change Cipher Spec Protocol**
 - **Alert Protocol**
 - **Handshake Protocol**



The Part 2 of the module 2 which is (Lecture 4) covers The Transport Layer Security are as follows:

❑ Transport Layer Security

- Version Number
- Message Authentication Code
- Pseudorandom Function
- Alert Codes
- Cipher Suites
- Client Certificate Types
- Web Traffic Security
- Certificate-Verify and Finished Messages

❑ HTTPS

- Connection Initiation
- Connection Closure

❑ Secure Shell (SSH)

- Transport Layer Protocol
- User Authentication Orotocol
- Connection Protocol



The Part 1 of the module 3 which is (Lecture 5) covers the Cryptography Techniques are as follows:

- ❑ **Symmetric Techniques**
 - **Stream Cipher**
 - **Block Cipher**

The Part 2 of the module 3 which is (Lecture 6) covers the Cryptography Techniques are as follows:

❑ *Asymmetric Techniques*

- *Diffie–Hellman key exchange protocol.*
- *DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm.*
- *ElGamal.*
- *Elliptic-curve cryptography*



The Part 1 of the module 4 which is (Lecture 7) covers the Cryptography Algorithms are as follows:

- *Public Key Algorithms*
- *Secret Key Algorithms*
- *Block Cipher Modes*

The Part 2 of the module 4 which is (Lecture 8) covers the Cryptography Algorithms are as follows:

- *Cryptographic Hash Functions*
- *Random Number Generators*

The Part 1 of the module 5 which is (Lecture 9) covers the Public Key Algorithms are as follows:

- *Principles of Public-Key Cryptosystems*
- *Rivest-Shamir-Adleman (RSA)*
- *Elliptic Curve Digital Signature Algorithm (ECDSA)*

The Part 2 of the module 5 which is (Lecture 10) covers the Public Key Algorithms are as follows:

- *Digital Signature Algorithm (DSA)*
- *Diffie-Hellman key agreement protocol*

Thank You

ANY
QUESTIONS?



جامعة الزكاة
EVERYONE'S SMART UNIVERSITY