Birzeit University
Computer Science Department
Encryption Theory
First Semester 2024/2025

Instructor Information

Instructor Name: Mohammed Alkhanafseh.

Office Number: Massri 314.

Email: Malkhanafseh@birzeit.edu

Course Description:

Cryptographic primitives and how they are applied within security systems, brief overview of classical cryptographic algorithms, symmetric-key encryption algorithms, Stream ciphers, Block cipher modes of operation, secure hash algorithms, message authentication codes, asymmetric ciphers, digital signatures, public key infrastructure, pseudorandom number generation, and design of cryptographic protocols, such as user authentication protocols.

Course Pre-Requisites

MATH234, COMP311, (COMP242 OR COMP2321).

Required Books/ Reading

- Cryptography and Network Security: Principles and Practice, William Stallings, 7th Edition, 2017.
- Cryptography: Theory and Practice, Third Edition, Douglas R. Stinson, CRC Press, 2006.
- Introduction to Cryptography with Coding Theory, Trappe & Washington, Prentice Hall, 2005.
- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. Van Orschot, Scott A. Vanstone, CRC Press.
- Heys' tutorial on linear and differential cryptanalysis.

Course Learning Outcomes LOCs

Upon successful completion of this course, the learner should be able to:

- Describe the Fundamental concepts of information hiding (Steganography and Watermark).
- Describe the fundamental concepts of encryption theory.
- Describe the standard encryption techniques.
- Understand advanced encryption techniques.
- Understand other block cipher operations such as (3DES, ECB, CBC).
- Demonstrate with public-key cryptography and RSA.
- Understand key management, message authentication and hash functions.
- Demonstrate with hash and MAC algorithms.
- Illustrate with digital signatures and authentication protocols.
- Understand authentication applications.

Birzeit University
Computer Science Department
Encryption Theory
First Semester 2024/2025

Course Content

Basic Mathematical Information for Encryption

Basic and fundamental concepts of numbering theory will be covered, matrix operation square matrix, matrix inverse, determinants, multiplicative inverse, cofactors of matrices, transformation, adjoint of matrices 3*3, Prime Numbers, Chinese Remainder Theorem, Diophantine equations, Solution of polynomial congruences.

The covering of these topic depends on the encryption theory such as the matrix operation that will be covered in the first three chapters since the transposition algorithms depends highly on matrix operation through the encryption and decryption process, such as Hill-Cipher algorithm, the Chinese Remainder Theorem will be covered in modern encryption algorithm section, and so on.

1- Introduction to cryptography and information hiding

1.1 What is Cryptography, Steganography, and Digital watermarking?
1.2 History of Cryptography and Steganography.
1.3 Cryptography and Steganography Terminology.
1.4 Cryptography Services (CIA)
1.5 Passive and Active Attack

2 **Classical Encryption Algorithms**

2.1 Cryptography Classification
2.2 Classical Encryption techniques (Symmetric Cipher Model)
2.2.1 Substitution Techniques:
1- Caesar Cipher.
2- Monoalphabetic Cipher
3- Play fair Cipher.
4- Hill Cipher.
5- Polyalphabetic Cipher.
2.2.2 Transposition Techniques.
1- Rail fence Cipher.
2- Matrix transposition Cipher.
2.2.3 Bit-Manipulation ciphers

3 **Modern Encryption Techniques**

3.1 Simplified Data Encryption Standard (DES)
3.2 S-DES Structure.
3.3 Examinations of the elements of DES
(a) S-DES Key Generation.
(b) S-DES Encryption.
(c) Relationship to DES.
(d) Block Cipher Principle.

4 **Public key Cryptography**

4.1Introduction.

4.2 Principle of Public Key Encryption.
4.3 Symmetric Versus Public Key Encryption.
4.4 Essential Elements of Public-Key Encryption.
4.5 Application of Public-Key Encryption.
4.6 RSA Algorithm.
4.7 Simple RSA Implementation examples.
4.8 Mini RSA.
4.9 Computational Aspects.
4.10 Security of RSA.
5 **Cryptanalysis of Symmetric and Asymmetric Key Ciphers**
5.1 Linear Cryptanalysis.
5.2 Differential Cryptanalysis.
5.3 Other Cryptanalytic Techniques.
6 **Cryptanalysis of Symmetric and Asymmetric Key Ciphers**
6.1 Linear Cryptanalysis.
6.2 Differential Cryptanalysis.
6.3 Other Cryptanalytic Techniques.
7 **Application of Cryptography**
7.1 Certificate Authority (CA)
7.2 Digital Certificate
7.3 Wi-Fi Encryption
7.4 Steganography Implementation
7.5 Suggestion from students.
7.6 Digital Signature.
8 **Design of Cryptographic protocols**

Methods of Teaching

The methods of instruction may include, but not limited

1- Lectures.
2- Discussion and problem solving.
3- Individual Assignments
4- Final Project.

FINAL PROJECT

There will be a set of ideas for the students to work on based on the covered material; groups will be formed by a group of students, or as an individual work will be done; a set of ideas can be provided here as projects ideas to be implemented by the students, such as
Keylogging idea, which depends on the step of authentication, since the project can identify the keystroke made in applied system. If the students are in advance level of programing, they can apply this idea on virtual keyboards.

Network Traffic Analyzer, the idea of this project depends mainly on packet sniffing, and packet analysis based on sniffed ideas.

Breaking CAESAR cipher algorithm, which refers to the earliest encryption technique, the idea of this algorithm refers to do shifting for the letters of original message based on the number which specified by the sender, such as do shifting for two letters and so on. The idea of the project here is to build an application that can decrypt the CAESER Cipher; this project can be classified as essential project on cipher security

Other projects, based on new concepts in the field of cipher security and encryption theories, can be implemented.

Assessment Policy

Assessment Description	Assessment Weight
Quizzes & Assignments	15%
Final Project	15%
Midterm Exam	30%
Final Exam	40%