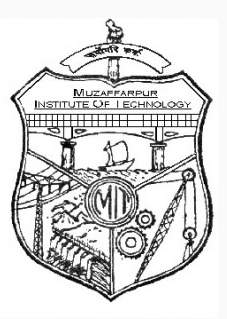
[**MUZAFFARPUR INSTITUTE OF TECHNOLOGY**](https://collegedunia.com/college/9706-muzaffarpur-institute-of-technology-mit-muzaffarpur)**, MUZAFFARPUR**



**COURSE FILE**

**OF**

**CRYPTOGRAPHY**

**(IT 051X18)**

**Faculty Name:**

**RAJEEV KUMAR**

**GUEST ASSISTANT PROFESSOR**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

****

****

****

**Course Description**

* In today’s cyber world, it is important for engineers to understand and appreciate computer/information security as it has become an essential aspect of our day life.
* This course provides students with concepts of computer security, cryptography, digital money, secure protocols, detection and other security techniques.
* Upon the completion of this course, students should be able to understand, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information.

**Course Objectives**

* To understand basics of Cryptography and Network Security.
* To be able to secure a message over insecure channel by various means.
* To learn about how to maintain the Confidentiality, Integrity and Availability of a data
* To understand various protocols for network security to protect against the threats in the networks.

**Course Outcomes**

* After successful completion of the course, the learners would be able to
* Provide security of the data over the network.
* Do research in the emerging areas of cryptography and network security.
* Implement various networking protocols. 4. Protect any network from the threats in the world.

**05 1x18 CRYPTOGRAPHY**

**L–T–P : 3–0–0 Credit : 3**

1. Introduction : The OSI Security Architecture, Security attack, Security Services, Security Mechanism, A model for Network Security. Lecture : 4

2. Symmetric Cipher : Classical Encryption Techniques, Symmetric Cipher Model, Block Cipher Principles, DES, Cryptanalysis, Block Cipher Design Principle, The Euclidean Algorithm, Finite field of Form GP(p), Advance Encryption Standard (AES), AES Cipher, Multiple Encryption and Triple DES, Stream, Placement of Encryption Function, Traffic Confidentiality, Key Distribution, Random number generation.Lecture : 15

3. Public Key Encryption and Hash Function : Fermat’s & Euler’s Theorems, The Chinese Remainder Theorem, RSA Algorithm, Diffe-Hellman Key Exchange, Elliptic Curve Cryptography, Massage authentication code, Security of Hash Functions and MAACs, Secure Hash algorithm, Whirlpool, HMAC, CMAC, Digital Signature. Lecture : 12

4. Network Security Applications : Kerberos, X.509 Authentication Service, S/MIME, IP Security Architecture, Encapsulating Security Payload, Secure Socket Layer (SSL), Transport layer security, Secure Electronic Transaction. Lecture : 6

5. System Security : Intrusion detection, Password Management, Virus countermeasure, Denial of Service Attack, Firewall design principles, Trusted System. Lecture : 6

**Text Book : 1.** Cryptography and Network Security : Principle and Practice, 4e by William Stalling, Pearson Education/PHI.

**Reference Books :** 1. Beginning Cryptography with Java by David Hook, Wiley Dreamtech.

2. Modern Cryptography Theory & Practices by Wenbo Mao, Pearson Education.

3. Cryptography for Database and Internet Application by Nick Galbreath, Wiley Dreamtech.

4. Network Security : Private Communication in a Public World, 2e, by Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson Education.





|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **COURSE PLAN** | | | |  | |  | |  | |  | |
| **Semester** | | 7th | |  | |  | |  | |  | |
| **Course Code** | | 051x18 | |  | |  | |  | |  | |
| **Course Credit** | | 3 | |  | |  | |  | |  | |
| **Course Name** | | Cryptography | |  | |  | |  | |  | |
| **Branches** | | Information Technology | |  | |  | |  | |  | |
| **Course Coordinator** | | ***Rajeev kumar*** | |  | |  | |  | |  | |
| **Date** | | 03-08-2018 | |  | |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
| **Part-A** | | **Lecture Plan** | |  | |  | |  | |  | |
| **Sl. No.** | | **Topic Name** | **Periods** | |  |  | |  | |  | |
| **1** | | **Introduction to Cryptography** |  | |  |  | |  | |  | |
|  | **1.1** | The OSI Security Architecture, Security attack, Security Services | **2** | |  |  | |  | |  | |
|  | **1.2** | Security Mechanism, A model for Network Security. | **2** | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
| **2** |  | **Symmetric Cipher** |  | |  |  | |  | |  | |
|  | **2.1** | Classical Encryption Techniques, Symmetric Cipher Model | **3** | |  |  | |  | |  | |
|  | **2.2** | Block Cipher Principle | **1** | |  |  | |  | |  | |
|  | **2.3** | DES | **2** | |  |  | |  | |  | |
|  | **2.4** | Cryptanalysis, Block Cipher Design Principle | **1** | |  |  | |  | |  | |
|  | **2.5** | The Euclidean Algorithm, Finite field of Form GP(p | **2** | |  |  | |  | |  | |
|  | **2.6** | Advance Encryption Standard (AES), | **2** | |  |  | |  | |  | |
|  | **2.7** | AES Cipher, Multiple Encryption and Triple DES, Stream, Placement of Encryption Functio | **2** | |  |  | |  | |  | |
|  | **2.8** | Traffic Confidentiality, Key Distribution, Random number gener | **1** | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
| **3** |  | **Public Key Encryption and Hash Function** |  | |  |  | |  | |  | |
|  | **3.1** | Fermat’s & Euler’s Theorems, The Chinese Remainder Theorem | **2** | |  |  | |  | |  | |
|  | **3.2** | RSA Algorithm, Diffe-Hellman Key Exchange | **2** | |  |  | |  | |  | |
|  | **3.3** | Elliptic Curve Cryptography, Massage authentication code | **2** | |  |  | |  | |  | |
|  | **3.4** | Security of Hash Functions and MAACs | **2** | |  |  | |  | |  | |
|  | **3.5** | Secure Hash algorithm, Whirlpool | **1** | |  |  | |  | |  | |
|  | **3.6** | HMAC, CMAC, Digital Signature | **2** | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
| **4** |  | **Network Security Applications** |  | |  |  | |  | |  | |
|  | **4.1** | Kerberos, X.509 Authentication Security | **2** | |  |  | |  | |  | |
|  | **4.2** | S/MIME, IP Security Architecture | **2** | |  |  | |  | |  | |
|  | **4.3** | Encapsulating Security Payload, Secure Socket Layer (SSL) | **2** | |  |  | |  | |  | |
|  | **4.4** | ransport layer security, Secure Electronic Transaction | **1** | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
| **5** |  | **System Security** |  | |  |  | |  | |  | |
|  | **5.1** | Intrusion detection | **1** | |  |  | |  | |  | |
|  | **5.2** | Password Management | **1** | |  |  | |  | |  | |
|  | **5.3** | Virus countermeasure, Denial of Service Attack | **2** | |  |  | |  | |  | |
|  | **5.4** | Firewall design principles, Trusted System | **2** | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
|  |  | **TOTAL** | **42** | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
|  | **PART B** | **Assignment Numbers** | **Topics** | |  |  | |  | |  | |
|  | 1 | Assignment # 1 | 1 | |  |  | |  | |  | |
|  | 2 | Assignment # 2 | 2 | |  |  | |  | |  | |
|  | 3 | Assignment # 3 | 3 | |  |  | |  | |  | |
|  | 4 | Assignment # 4 | 4 | |  |  | |  | |  | |
|  |  |  |  | |  |  | |  | |  | |
| **Text Books :** | |  |  | |  |  | |  | |  | |
|  | 1Cryptography and Network Security : Principle and Practice, 4e by William Stalling, Pearson Education/P | | |  | |  | |  | |  | |
| **Reference Books :** | |  |  | |  |  | |  | |  | |
|  | 1. Beginning Cryptography with Java by David Hook, Wiley Dreamtech.  Modern Cryptography Theory & Practices by Wenbo Mao, Pearson Education. | | | | | |  | |  | |  | |
|  |  | | |  | |  | |  | |  | |
|  | 1. Cryptography for Database and Internet Application by Nick Galbreath, Wiley Dreamtech | |  | |  |  | |  | |  | |
|  | 1. Network Security : Private Communication in a Public World, 2e, by Charlie Kaufman, Radia   Perlman and Mike Speciner, Pearson Education. | | | | | | | | | | | |
|  |  |  |  | |  |  | |  | |  | |

**ASSIGNMENT**

1. Define the three security goals. List and describe security attacks that threaten security goals.
2. Distinguish between security services and security mechanisms.
3. What are the components of a Modern Block Cipher? Explain why modern block ciphers need to be designed as substitution ciphers.
4. Draw a block diagram showing a single round structure at the encryption site of DES algorithm and explain the main components and operations of a single round at the encryption site of DES algorithm
5. Discuss the weaknesses in DES algorithm.
6. Consider an RSA Public Key Cryptosystem

A) Alice selects two prime numbers: p=5, q=11. Compute n, and Φ(n) ?

B) Alice selects her public exponent e = 3, Is this choice for “e” valid? Why?

C) Compute d , the private exponent of Alice?

D) Now you want to send message M=4 to Alice. Encrypt your plaintext M using Alice public exponent. What is the resulting cipher text C?

E) Now Alice receives C, verify that Alice can obtain M from C, using her private decryption exponent. (use Fast Exponentiation /Square and Multiply method)

1. A) Briefly explain the idea behind the knapsack cryptosystem

B) Given the super increasing tuple b=[7,11,19,39,79,157,313], r =37, and modulus n=900, encrypt and decrypt the letter "g" using the knapsack crptosystem. Use [4 2 5 3 1 7 6] as the permutation table. ( The 7-bit ASCII representation of "g" is (1100111)2 )

1. Alice needs to send the message "Enemy attacks to night" to Bob. Assume that Alice and Bob used the transposition-cipher encryption key (3,1,4,5,2). What is the decryption key? If the double transposition cipher is used, what is the cipher text?
2. State and explain four kinds of cryptanalysis attacks based on what is known to the attacker.
3. List and describe briefly four modes of operations and explain why modes of operation are needed (possibly use a diagram).

