INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KALYANI
Autonomous institution under MHRD, Govt. Of India
&
Department of Information Technology & Electronics, Govt. of West Bengal
WEBEL IT Park Campus (Near Buddha Park), Kalyani -741235, West Bengal
Tel : 033 2582 2240, website : www.iiitkalyani.ac.in

Weekly contact : **3 – 0 – 0 (L – T – P)**
Course No. : **CS 764**
Course Title : **Cryptography and Network Security**
Instructor-In-Charge : **Dr. SK Hafizul Islam**

---

1) Course Description

Basics of Cryptography, Different types of attack, Classical Encryption, Random Number Generators, Block Cipher, Stream Cipher, DES, AES, Group Theory, Modes of Operations, Cryptographic Hash Functions, MAC, HMAC, Fermat's and Euler's Theorems, Testing for Primality, Public-Key Cryptography, RSA, ElGamal Cryptosystem, Diffie-Hellman Key Exchange, RSAES-OAEP, RSA Digital Signature, ElGamal Digital Signature Scheme, Schnorr Digital Signature, Digital Signature Standard, Remote User Authentication Using Symmetric and Asymmetric Encryption, Kerberos, Key Management, Symmetric Key Distribution, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure, SSL, TLS, PGP, S/MIME, IP Security, IKE, VPN.

2) Objective

To define various security goals. To define security attacks that threatens security goals. To define security services and how they are related to the security goals. To define security mechanisms to provide security services. To introduce cryptography to implement security mechanisms. To provide the theoretical foundations of number theory and applied cryptography. To understand the network/information security protocols/schemes designed for various Internet-based applications.

3) Scope

This course covers basic concepts of number theory and applied cryptography. This course discusses different protocols/schemes usable for many information/network security applications. This course also discusses different arracks on protocols/schemes and their possible countermeasures.

4) Text Book

[T1] W. Stallings: Cryptography and Network Security, 5e, Pearson.
http://www.tnstate.edu/faculty/wchen/plabworkshop.aspx

5) References

[R1] B. A. Forouzan & D. Mukhopadhyay: Cryptography and Network Security, 2e, McGraw-Hill.
[R2] D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), 3e, CRC Press.
[R3] B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, 2e, John Wiley & Sons.
[R4] Bernard Menezes: Network Security & Cryptography, 1st Edition, Cengage Learning, Delhi, 2011.

Note: In this course, I will follow two books [T1] & [R1]. However, the students are suggested to consult with the books [R2] - [R5] for Modern Cryptography and Network Security.

6) Lecture Modules

No.	Module	Learning Objective
I	Introduction	To understand the basic concepts and notation
II	Symmetric Encryption and Hash Function	To understand different classical encryption techniques and attacks on them. To modern symmetric encryption techniques and issues.
III	Number Theory and Public Key Cryptography	To understand number theory for public key cryptography. To understand the need of public key cryptography. To understand different public key encryption techniques. To understand different attacks and possible countermeasures.
IV	Digital Signature	To understand different digital signatures schemes, attacks and possible solutions.
V	User Authentication and Key Management	To understand different user authentication techniques using symmetric and asymmetric key techniques. To understand the need of public key infrastructure. To understand different public key management and distribution techniques.
VI	Security for Transport and Networks Layers	To understand the need of security protocols for Transport and Networks Layers. To understand different Transport and Networks Layers security protocols, issues and possible countermeasures.

7) Lecture Plan

Module	Topic	No. of Hours
I	Introduction to Network Security, Trends, Architecture, Levels, Attacks, Services, Mechanism, Network Security model and Standards.	**2**
II	**Classical Encryption Techniques:** Basics of Cryptography, Simple Symmetric Ciphers, General thought on breaking cryptosystems, Modular Arithmetic, Substitution and, Transposition Ciphers, Stream Cipher, RC4, Random Numbers, Cryptographically Secure Random Number Generators, One Time Pad **Block Ciphers and the Data Encryption Standard:** Block Cipher Principles, Data Encryption Standard (DES), Block Cipher Design Principles**.** **Advanced Encryption Standard** The Extended Euclidean Algorithm, Galois Fields, AES Structure, AES Round Functions, AES Key Expansion, AES Implementation **Block Cipher Operation** Multiple Encryption, 3DES, DESX, Modes of Operations: Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode. **Cryptographic Hash Functions and MAC:** Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm, MAC from hash functions and block ciphers.	**10**
III	**Number Theory:** Relevant Number Theory for public-key algorithms, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality. **Public-Key Cryptography:** Principles of Public-Key Cryptosystems, RSA, ElGamal Cryptosystem, Diffie-	**8**

	Hellman Key Exchange, Attacks in RSA, RSAES-OAEP.	
IV	**Digital Signatures** Digital Signatures, RSA Digital Signature, ElGamal Digital Signature Scheme, Schnorr Digital Signature Scheme, Digital Signature Standard	**6**
V	**User Authentication Protocols** Remote User Authentication Principles, Remote User Authentication Using Symmetric Encryption, Kerberos, Remote User Authentication Using Asymmetric Encryption **Key Management and Distribution** Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public Key Infrastructure	**12**
VI	**Transport Layer Security** Secure Sockets Layer (SSL), Transport Layer Security (TLS) **Electronic Mail Security** Pretty Good Privacy (PGP), S/MIME **IP Security** IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, IKE, Virtual Private Network (VPN)	**14**

8) Evaluation scheme

Component	Weightage	Duration
Short Quiz	5%×6 = 30%	TBD
Assignment/Mega Quiz	10%×2 = 20%	TBD
Mid-Sem. Examination	TBD	TBD
End-Sem. Examination	TBD	TBD

9) Class Schedule:

- Thursday: 10:20 AM --12:00 PM
- Friday: 10:20 AM --11:10 AM

10) Notices: All notices related to the course will be putted up/circulated on the institute notice board/group e-mail.

11) De-Registration Policy: Will be notified.

12) Chamber consultation hour: N/A

13) Make-Up Policy:

- For Mid-Sem./End-Sem., as per institute rules.
- **No Makeup for Assignment/ Quiz**

Instructor-In-Charge
CS 764