CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
ITT402	CRYPTOGRAPHY AND NETWORK SECURITY	PCC	2	1	0	3

Preamble: Cryptography is essentially important for secure communication in digital form and to provide security services in today's internet environment. The syllabus is prepared with a view to provide the Engineering Graduates a better foundation in cryptography and networksecurity.

Prerequisite: MAT203Discrete Mathematical Structures, ITT305 Data Communication and Networking

Course Outcomes: After completion of the course the student will be able to

CO No.	Course Outcome (CO)	Bloom's Category Level
CO 1	Apply the concepts of number theory in designing crypto systems	Level 3: Apply
CO 2	Explain various network security aspects, cryptanalytic attacks and classical cryptosystems	Level 2: Understand
CO 3	Describe various symmetric key cryptosystems, hash and message authentication functions.	Level 2: Understand
CO 4	Apply the principles of asymmetric key cryptosystems and digital signature.	Level 3: Apply
CO 5	Discuss various protocols to ensure Email Security and Network Security.	Level 2: Understand

Mapping of Course Outcomes with Program Outcomes

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO 1	3	-	2	-	-	-	-	-	-	-	-	1
CO 2	1	1	2	-	-	-	-	-	-	-	-	-
CO 3	1	-	-	-	-	-	-	-	-	-	-	1
CO 4	3	-	-	-	1	-	-	-	-	-	-	1
CO 5	1	2	1	-	2	-	-	-	-	-	-	1

3/2/1: High/Medium/Low

Assessment Pattern

Bloom's Category Levels	Continuous Assessment Tests		End Semester Examination
	1	2	
BL 1: Remember	10	10	20
BL 2: Understand	30	30	60
BL 3: Apply	10	10	20
BL 4: Analyse			
BL 5: Evaluate			
BL 6: Create			

Mark distribution

Total Marks	Continuous Internal Evaluation (CIE)	End Semester Examination (ESE)	ESE Duration
150	50	100	3 hours

Continuous Internal Evaluation Pattern:

Attendance : 10 marks
Continuous Assessment Test (2 numbers) : 25 marks
Assignment/Quiz/Course project : 15 marks

End Semester Examination Pattern: There will be *two* parts; **Part A** and **Part B**. Part A contains 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer *all* questions. Part B contains 2 questions from each module of which student should answer *any one*. Each question can have maximum 2 sub-divisions and carry 14 marks.

Sample Course Level Assessment Questions

Course Outcome 1 (CO 1):

1. Using Euclid's algorithm, obtain the greatest common divisor of the(42, 105, 91).
2. Find 33^{100} mod 40 (use Euler's theorem).
3. Compute the value of x for the set of congruence given using Chinese Remainder Theorem. x≡4 mod 5, and x≡ 10 mod 11.
4. Define Fermat's theorem and list out its applications.

Course Outcome 2 (CO 2):

1. Describe the three security goals of Information Security.
2. Explain with examples some of the attacks threatening confidentialityand integrity.
3. Encrypt the message "beware of strangers" using Vigenere cipher with key "dollars". Ignore the space between words. Decrypt the message to get the plain text.
4. Compare stream cipher and block cipher with example.

Course Outcome 3 (CO 3):

1. Summarize the key generation process in DES.
2. With suitable examples, explain the significance of hash function for message authentication.
3. List and briefly describe the design objectives of HMAC.
4. Explain the single round operation of SHA-512.

Course Outcome 4 (CO 4):

1. Perform encryption and decryption using RSA algorithm for the following. P=7; q=11; e=13; M=8.
2. Identify the possible threats for the RSA algorithm and list their countermeasures.
3. Demonstrate man in the middle attack on Diffie Hellman key exchange algorithm.
4. Explain the digital signature algorithm with suitable diagrams.

Course Outcome 5 (CO 5):

1. Describe the various ways to distribute public keys in cryptography.
2. Sketch and explain the transmission and reception of PGP Messages.
3. Give the format of Authentication Header in IPSec.
4. Explain the features of any two types of firewalls.

Model Question Paper

Course Code: ITT402

Course Name: CRYPTOGRAPHY AND NETWORK SECURITY

Max.Marks :100 **Duration: 3 Hrs**

Part A

Answer all questions. Each question carries 3 marks (10 * 3 = 30 Marks)

1. Identify the number of primes less than 1,000,000.
2. Compute 33^{100} (mod 40) (use Euler's theorem).
3. With an example, explain the encryption and decryption process of Caesar Cipher.
4. Compare stream cipher and block cipher with example.
5. "The decryption mode of DES is inverse of its decryption mode". Justify the above statement with your comments.
6. Compare the round keys in DES and AES. In which cipher is the size of the round key the same as the size of the block?
7. Consider a Diffie Hellman scheme with a common prime q = 11 and primitive root α = 2. If user A has public key YA = 9 and user B has public key YB = 3, estimate A's private key and the shared secret key K between A and B.
8. Explain the steps for the verifying process in RSA digital signature scheme.
9. Discuss about the various types of firewalls.
10. Distinguish between Direct DDoS and Reflector DDoS.

Part B

Answer all questions. Each question carries 14 marks. (5 * 14 = 70 Marks)

11 a. Compute gcd(85,289).
Using Euclid's extended algorithm, obtain x and y such that
85x+ 289y = gcd(85, 289). 7

b. Find the particular and general solutions to the equation 21x+14y=35. 7

OR

12 a. Solve the system of simultaneous congruences using Chinese remainder theorem
$x \equiv 6 \pmod{11}$
$x \equiv 13 \pmod{16}$
$x \equiv 9 \pmod{21}$
$x \equiv 19 \pmod{25}$ 8

b. Using Fermat theorem evaluate the following:
$6^{10} \bmod 11$
$3^{12} \bmod 11$
$5^{984} \bmod 7$ 6

13 a. List and explain the security mechanisms defined by X.800. 8

b. Illustrate the encryption of given message using Playfair cipher with the keyword "GUIDANCE".
Message: MEET ME AT THE TOGA PARTY 6

OR

14 a. Describethe various cryptanalytic attacks on cryptosystems. 10

b. Consider the encryption key in a transposition cipher is (3,2,6,1,5,4). Determine the corresponding decryption key. 4

15 a. Demonstrate the single round operation in the DES algorithm. 10

b. List and briefly describe the design objectives of HMAC. 4

OR

16 a. Outline the following round operations in AES cipher: 10
i. Substitute Bytes Transformation
ii. ShiftRows Transformation
iii. MixColumns Transformation
iv. AddRound Key Transformation

b. Distinguish between HMAC and CMAC. 4

17 a. Illustrate in detail about the message authentication code and its requirements. 7

b. Alice and Bob agreed to use RSA algorithm for the secret communication. Alice securely chooses two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. Bob uses this public key and sends a cipher text 18 to Alice. Obtain the plain text. 7

OR

18 a. Consider an ElGamal scheme with a common prime p =71 and a primitive

root x =7.

1. If Bob has public key y = 3 and Alice chose the random integer k = 2, Find the ciphertext of M = 30.

2. If Alice now chooses a different value of k, so that the encoding of M = 30 is C = (59, C2), determine the integer C2. 8

b. Describe signing and verification in Digital Signature Algorithm. 6

19 a. Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagrams. 10

b. Sketch and explain IPSec ESP Format. 4

OR

20 a Illustrate the working of Secure Electronic Transaction (SET) in detail. 7

b. Summarize any two techniques proposed for the distribution of public keys. 7

Syllabus

Module 1: Basics of Algebra and Number Theory (7 Hours)
Integer Arithmetic -Divisibility - Greatest Common Divisor - Extended Euclidean Algorithm- Linear Diophantine equation, Modular Arithmetic - Modulo Operator - Congruence - Addition and multiplicative inverse, Algebraic structures - Field - Finite fields of the form GF(p) and GF(2^n) - Polynomial arithmetic, Prime Numbers - Fermat's and Euler's Theorem - Prime Factorization by Trial Division Method - Chinese Remainder Theorem.
Module 2: Introduction to Security (8 Hours)
Security Goals, Security Services-Confidentiality -Integrity - Authentication- Non-repudiation- Access control, Security Mechanisms–Encipherment- Data Integrity- Signature-Authentication Exchange-Traffic Padding- Routing Control- Notarization- Access Control, Introduction to Cryptography -Classification of Cryptosystems, Cryptanalytic attacks, CipherProperties - Confusion- Diffusion. Classical Cryptosystems - Substitution Techniques - Monoalphabetic Cipher - Caesar Cipher- AffineCipher, Polyalphabetic Ciphers - Autokey Cipher- Playfair Cipher-Hill Cipher-VigenereCipher- One Time Pad Cipher, Stream and Block Ciphers, Modern Secret Key Ciphers - Substitution Box-Permutation Box-Product Ciphers.
Module 3: Private Key Cryptography and Hash Function (7 Hours)
Data Encryption Standard - DES - Structure of DES - DES Attacks - 2-DES - 3-DES, Advanced Encryption Standard - AES - Structure-Analysis, Cryptographic Hash Functions - Properties - Secure Hash Algorithm - SHA-512 Logic - SHA-512 Round Function, Message Authentication Code -Hash-based Message Authentication Code -HMAC - Cipher-based Message Authentication Code - CMAC.
Module 4: Public Key Cryptography and Digital Signature (7 Hours)
Public Key Cryptosystems -PKC - Types of PKC - Trapdoor - One-way functions, RSA Cryptosystem -Key Generation – Encryption- Decryption,ElGamal Cryptosystem - Key Generation – Encryption-Decryption, Diffie-Hellman Key Exchange Protocol- Man in the Middle attack on Diffie-Hellman Protocol. Digital Signature- Signing - Verification, Digital signature forgery-Existential forgery-Selective forgery- Universal forgery, RSA Digital Signature Scheme -ElGamal Signature Scheme.

Module 5: Key Distribution and Network Security (6Hours)
Symmetric Key Distribution using Symmetric and Asymmetric Encryption - Distribution of public keys -Public announcement- Public available directory-Public-key authority- Public-key Certificates. Electronic Mail Security -Pretty Good Privacy- PGP message format - Transmission and Reception of PGP Messages, IP Security Overview - IP Authentication Header - Encapsulating Security Payload - Distributed Denial of Service attacks, Secure Electronic Transaction - PaymentProcessing - Dual Signature, Firewalls - Firewall Design Principles.

Text Books

1. Stallings W., Cryptography and Network security: Principles and Practice, 7/e, Pearson Education Asia, 2017.
2. Stallings W., Cryptography and Network security: Principles and Practice, 4/e, Pearson Education Asia, 2006.
3. Behrouz A Forouzan&DebdeepMukhopadhyay, "Cryptography and Network. Security", Second Edition, Tata McGraw Hill Education Pvt Ltd Publication, 2010.

Reference Books

1. AtulKahate, "Cryptography and Network Security, 4e", Tata McGraw Hill,2019.
2. Bernard Menezes, Network Security and Cryptography-Cengage Learning India, 2011
3. Thomas Mowbray, "Cybersecurity: Managing Systems Conducting Testing, and Investigating Intrusions", John Wiley, 2014
4. Charles P. Pleeger, Shari Lawrence Pfleeger, "Security in Computing", Pearson Education Asia, 5thEdition, 2018.
5. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: PRIVATE Communication in a PUBLIC World, Pearson Education India, 2016.

Course Contents and Lecture Schedule

Sl. No.	Topic	No. of Lectures
1	**Basics of Algebra and Number Theory**	**7Hours**
1.1	Integer Arithmetic - Divisibility - Greatest Common Divisor	1
1.2	Extended Euclidean Algorithm	1
1.3	Linear Diophantine equation	1
1.4	Modular Arithmetic - Modulo Operator - Congruence - Addition and multiplicative inverse	1
1.5	Algebraic structures - Field - Finite fields of the form GF(p) and GF(2^n) - Polynomial arithmetic	1
1.6	Prime Numbers - Fermat's and Euler's Theorem- Prime Factorization by Trial Division Method	1
1.7	Chinese Remainder Theorem	1

2	**Introduction to Security**	**8 Hours**
2.1	Security Goals, Security Services - Confidentiality- Integrity- Authentication- Non-repudiation- Access control, Security Mechanisms - Encipherment- Data Integrity - Signature- Authentication Exchange-Traffic Padding- Routing Control - Notarization-Access Control	1
2.2	Introduction to Cryptography -Classification of Cryptosystems, Cryptanalytic attacks, Cipher Properties-Confusion- Diffusion.	1
2.3	Classical Cryptosystems - Substitution Techniques - Monoalphabetic Cipher	1
2.4	Caesar Cipher- Affine Cipher	1
2.5	Polyalphabetic Ciphers - Autokey Cipher- Playfair Cipher	1
2.6	Hill Cipher- Vigenere Cipher- One Time Pad Cipher	2
2.7	Stream and Block Ciphers, Modern Secret Key Ciphers- Substitution Box-Permutation Box-Product Ciphers	1
3	**Private Key Cryptography and Hash Function**	**7 Hours**
3.1	Data Encryption Standard -DES- Structure of DES- DES Attacks - 2-DES - 3-DES	2
3.2	Advanced Encryption Standard -AES -Structure-Analysis	2
3.3	Cryptographic Hash Functions - Properties	1
3.4	Secure Hash Algorithm - SHA-512 Logic - SHA-512 Round Function	1
3.5	Message Authentication Code - Hash-based MessageAuthentication Code -HMAC - Cipher-based Message Authentication Code - CMAC	1
4	**Public Key Cryptography and Digital Signature**	**7 Hours**
4.1	Public Key Cryptosystems -PKC - Types of PKC - Trapdoor - One-way functions- RSA Cryptosystem -Key Generation-Encryption-Decryption	2
4.2	ElGamal Cryptosystem - Key Generation – Encryption-Decryption	2
4.3	Diffie-Hellman Key Exchange Protocol- Man in the Middle attack on Diffie-Hellman Protocol.	1
4.4	Digital Signature- Signing - Verification, Digital signature forgery- Existential forgery- Selective forgery- Universal forgery	1

4.5	RSA Digital Signature Scheme - ElGamal Signature Scheme.	1
5	**Key Distribution and Network Security**	**6 Hours**
5.1	Symmetric Key Distribution using Symmetric and Asymmetric Encryption	1
5.2	Distribution of public keys -Public announcement- Public available directory-Publickey authority- Publickey Certificates	1
5.3	Electronic Mail Security - Pretty Good Privacy- PGP message format - Transmission and Reception of PGP Messages	1
5.4	IP Security Overview - IP Authentication Header - Encapsulating Security Payload,Distributed Denial of Service attacks	1
5.5	Secure Electronic Transaction- Payment Processing -Dual Signature	1
5.6	Firewalls - Firewall Design Principles	1