CODE	COURSE NAME	CATEGORY	L	T	P	CREDIT
20MCA263	**CYBER SECURITY & CRYPTOGRAPHY**	**ELECTIVE**	**3**	**1**	**0**	**4**

Preamble: This course is designed to provide theoretical concepts used in cryptography and to introduce the students to various cryptographic algorithms and techniques used for implementing data security and protection. This course also discusses common web application security vulnerabilities.

Prerequisite: Student is expected to have studied mathematics courses that cover Elementary Number Theory, Finite Field, Discrete Logarithm and Euclidean Algorithm.

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

CO No.	Course Outcome (CO)	Bloom's Category Level
CO 1	Explain various types of security attacks, security mechanisms, security services and classical encryption techniques.	Level 2: Understand
CO 2	Make use of Symmetric and Asymmetric encryption techniques to solve cryptographic problems.	Level 3: Apply
CO 3	Describe the concepts of message authentication codes, hash functions and digital signing techniques for ensuring secure transactions.	Level 2: Understand
CO 4	Discuss security services in Application, Transport and Network layers.	Level 2: Understand
CO 5	Explain common web application security vulnerabilities and various prevention mechanisms.	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	2	1	1				1					
CO 2	2	2	2	1			1					
CO 3	2	1	1				1					
CO 4	2	1	1			2	1					
CO 5	2	1	1			2	1					

3/2/1: High/Medium/Low

Assessment Pattern

Bloom's Category Levels	**Continuous Assessment Tests**		**End Semester Examination**
	1	**2**	
Level 1: Remember	15	15	20
Level 2: Understand	35	35	40
Level 3: Apply			
Level 4: Analyse			
Level 5: Evaluate			
Level 6: Create			

Mark distribution

Total Marks	**Continuous Internal Evaluation (CIE)**	**End Semester Examination (ESE)**	**ESE Duration**
100	40	60	3 hours

Continuous Internal Evaluation Pattern:

Attendance	: 8 marks
Continuous Assessment Test (2 numbers)	: 20 marks
Assignment/Quiz/Course project	: 12 marks

End Semester Examination Pattern: There will be two parts; Part A and Part B. Part A contains 10 compulsory short answer questions, 2 from each module. Each question carries 3 marks. Part B contains 2 questions from each module of which student should answer any one. Each question can have a maximum of 2 sub-divisions and carry 6 marks.

Sample Course Level Assessment Questions

Course Outcome 1 (CO 1):

1. Briefly explain each component of OSI security architecture.
2. Compare Substitution and Transposition techniques in cryptography.
3. Explain how steganography is used in cryptography.

Course Outcome 2 (CO 2):

1. Explain block cipher modes of operation.
2. Compare DES and AES

3. Perform encryption and decryption using RSA Algorithm with parameters: P=17, q = 11, e = 7, M = 88.

Course Outcome 3 (CO 3):

1. Compare the features of HMAC and CMAC algorithms.
2. Explain important steps in DSS.
3. Describe the terms (a) birthday attack (b) hashcash (c) blind signature

Course Outcome 4 (CO 4):

1. Explain any one protocol used in E-mail for security.
2. Explain how security is provided in Network Layer using IPsec.
3. Describe the process of securing electronic transactions.

Course Outcome 5 (CO 5):

1. Discuss any four Application Security Risks.
2. Which are the different forms of XSS and how to prevent these?
3. Explain the attack scenario of any four web application security vulnerabilities.

Model Question Paper

Course Code: 20MCA263

Course Name: CYBER SECURITY & CRYPTOGRAPHY

Max. Marks :60 **Duration: 3 Hrs**

Part A

Answer all questions.

Each question carries 3 marks (10 x 3 = 30 Marks)

.

1. Compare phishing and ransomware attacks.
2. What is OSI security architecture?
3. List out the advantages and disadvantages of Output Feed Back mode.
4. Explain round functions used in DES.
5. Explain important steps in DSS.
6. Describe the terms (a) birthday attack (b) hashcash (c) blind signature.
7. Describe security association of IPSec.
8. Explain about S/MIME.

9. How can we prevent Injection attack?

10. What is XXE? How to prevent it?

(10 x 3=30 marks)

Part B

Answer all questions. Each question carries 6 marks. (5 * 6 = 30 Marks)

11. Explain Network security model with the help of a neat diagram (6)

OR

12. Describe the working of Playfair cipher and Hill cipher. (6)

13. Apply Diffie-Hellman key exchange algorithm to compute the shared private key using the values P = 23, g = 9, a= 4, b= 3. Explain the steps in detail. (6)

OR

14. Perform encryption and decryption using RSA Algorithm with parameters: P=17, q = 11, e = 7, M = 88. Explain the steps in detail. (6)

15. Compare HMAC and CMAC protocol with suitable diagrams. (6)

OR

16. Compare various signature schemes with suitable diagrams. (6)

17. Explain PGP cryptographic functions with diagram. (6)

OR

18. Explain Secure Electronic Transaction Protocol. (6)

19. Briefly explain any four Application Security Risks. (6)

OR

20. Explain the attack scenarios of any four web application security vulnerabilities. (6)

(5 x 6=30 Marks)

Syllabus

Module 1: (7 Hours)

Introduction to Cryptography, OSI security architecture: Security Services, Mechanisms and attacks- Phishing, Ransomware, DoS attack. Network security model. Classical Encryption techniques - Symmetric cipher model, substitution techniques, transposition techniques. Steganography.

Module 2: (10 Hours)

Conventional Symmetric Key Encryption: Block ciphers and Stream Ciphers, Block Cipher Design Principles, Modes of operation, Data Encryption Standard, Advanced Encryption Standard (AES), Multiple Encryption, Triple DES.

Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key exchange - Elliptic curve arithmetic - Elliptic curve cryptography.

Module 3: (10 Hours)

Hash Functions and MAC: Properties of hash functions, birthday attack, hashcash, Message Authentication Code Algorithms, MAC protocols: HMAC, CMAC.

Digital Signatures: Classification of signature schemes: RSA signature, Digital Signature Standard, Overview of ElGamal and Schnorr schemes, One time signature schemes, Attacks on Digital Signatures, Blind Signatures.

Module 4: (10 Hours)

Introduction to Cyber Security: Email Security: Security Services for email, Attacks possible through email, Establishing keys privacy, authentication of the source, Message Integrity, Non-repudiation, Pretty Good Privacy, S/MIME.

IP Security: Overview of IPSec, IPv4 and IPv6, Authentication Header, Encapsulation Security Payload (ESP), Internet Key Exchange.

Transport Level Security: SSL/TLS Basic Protocol, computing the keys, client authentication, PKI as deployed by SSL, Attacks fixed in v3, Exportability, Encoding, Secure Electronic Transaction (SET).

Module 5: (8 Hours)

Common web application security vulnerabilities: Injection flaws, Broken authentication, Sensitive data exposure, XML External Entities (XXE), Broken access control, Security misconfiguration, Cross-Site Scripting (XSS), Insecure deserialization, Using components with known vulnerabilities, Insufficient logging & monitoring.

Example attack scenarios of each of the vulnerabilities listed; how to prevent them

Text Book

1. William Stallings, “Cryptography and Network Security,” 6th Edition, Pearson Education, March (2013).
2. Behrouz A. Forouzan, “Introduction to Cryptography and Network Security”, Tata McGraw-Hill Publishing 2nd Edition (2011).

Reference Books

1. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.
2. Manuel Mogollon, “Cryptography and Security Services – Mechanisms and Applications”, Cybertech Publishing, 2008
3. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, “Firewalls and Internet Security” Addison- Wesley, 2003

Web References

1. http://www.hashcash.org/hashcash.pdf [Reference for hashcash]
2. https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf. [Reference for Module 5]
3. https://www.coursera.org/learn/crypto
4. https://www.coursera.org/learn/crypto2

Course Contents and Lecture Schedule

Sl. No.	Topic	No. of Lectures
1	**Introduction to Cryptography**	**7 Hours**
1.1	What is cryptography, Related Terms, Need of cryptosystems	1
1.2	OSI security architecture: Security Services, Mechanisms	1
1.3	Security attacks- Phishing, Ransomware, DoS attack.	1
1.4	Network security model	1
1.5	Classical Encryption techniques, Symmetric cipher model	1
1.6	Substitution techniques	1
1.7	Transposition techniques, Steganography	1
2	**Conventional Symmetric and Public Key Encryption**	**10 Hours**
2.1	Block ciphers and Stream Ciphers, Block Cipher Design Principles	1
2.2	Modes of operation	1
2.3	Data Encryption Standard	1
2.4	Advanced Encryption Standard (AES)	1
2.5	Multiple Encryption, Triple DES	1
2.6	Public key cryptography: Principles of public key cryptosystems	1
2.7	The RSA algorithm	1

2.8	Key management	1
2.9	Diffie Hellman Key exchange	1
2.10	Elliptic curve arithmetic - Elliptic curve cryptography.	1
3	**Hash Functions and MAC**	**10 Hours**
3.1	Properties of hash functions, birthday attack	1
3.2	Hashcash, Message Authentication Code Algorithms	1
3.3	MAC protocols: HMAC, CMAC	1
3.4	Digital Signatures: Classification of signature schemes	1
3.5	RSA signature	1
3.6	Digital Signature Standard	1
3.7	Overview of ElGamal and Schnorr schemes	1
3.8	One time signature schemes	1
3.9	Attacks on Digital Signatures	1
3.10	Blind Signatures	1
4	**Introduction to Cyber Security**	**10 Hours**
4.1	Email Security: Security Services for email, Attacks possible through email	1
4.2	Establishing keys privacy, authentication of the source, Message Integrity, Non-repudiation	1
4.3	Pretty Good Privacy, S/MIME	1
4.4	IP Security: Overview of IPSec	1
4.5	IPv4 and IPv6, Authentication Header	1
4.6	Encapsulation Security Payload (ESP), Internet Key Exchange	1
4.7	Transport Level Security: SSL/TLS Basic Protocol	1
4.8	computing the keys, client authentication, PKI as deployed by SSL	1
4.9	Attacks fixed in v3, Exportability, Encoding	1
4.10	Secure Electronic Transaction (SET)	1
5	**Common web application security vulnerabilities**	**8 Hours**
5.1	Common web application security vulnerabilities	1
5.2	Injection flaws, Broken authentication	1
5.3	Sensitive data exposure, XML External Entities (XXE)	1
5.4	Broken access control, Security misconfiguration	1
5.5	Cross-Site Scripting (XSS), Insecure deserialization	1
5.6	Using components with known vulnerabilities, Insufficient logging & monitoring.	1
5.7	Example attack scenarios of each of the vulnerabilities listed	1
5.8	How to prevent each of the vulnerabilities.	1