Department of Artificial Intelligence and Machine learning

Subject Name:Data Security and Privacy **SubjectCode: BAD703**

SEM :7 **DIV : A**

Faculty :Asghar Pasha

Module-1 Question Bank

SL No	Question	CO	Level	Marks
1	Draw and explain a general model for network security.	CO1	L2	10
2	Describe the working of the Playfair cipher. Encrypt the message **SECURITY** using the key **NETWORK**.	CO1	L3	10
3	Explain monoalphabetic and polyalphabetic ciphers with example	CO1	L2	10
4	With neat diagram , explain Fiestel structure	CO1	L2	10
5	Using Hill cipher technique encrypt and decrypt the plaintext " crypto" using the key $K=\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}$.	CO1	L3	10
6	Explain the working of the Autokey cipher and compare it with the Vigenère cipher.	CO1	L3	10
7	Using Playfair cipher and key **CIPHER**, encrypt the plaintext **NETWORK SECURITY**. Show construction of key square.	CO1	L3	10
8	Consider Hill cipher=3(block size=3) with key k shown below: $k=\begin{pmatrix}25 & 3 & 7\\ 5 & 9 & 21\\ 11 & 8 & 13\end{pmatrix}$ a) What is the ciphertext corresponding to plaintext = VOW b) What is the plaintext corresponding to ciphertext = TOX ?	CO1	L3	10
9	What are polyalphabetic ciphers? Illustrate Vigenère cipher encryption with an example.	CO1	L2	10
10	Explain the DES algorithm with a neat diagram.	CO1	L2	10
11	Explain the key design principles for a secure block cipher.	CO1	L2	10

12	Differentiate between stream ciphers and block ciphers with suitable examples.	CO1	L4	10

Module 2 – Question Bank

SL#	Question	CO	Level	Marks
1	Explain the working of a **Linear Congruential Generator (LCG)**. Generate the first four pseudorandom numbers using $X_0 = 5, a = 7, c = 3, m = 11.$	CO2	L2	10
2	Describe the **Blum BlumShub Generator**. Why is it considered cryptographically secure compared to LCG?	CO2	L3	10
3	Discuss the **principles of public key cryptosystems**. How do they differ from symmetric key systems?	CO2	L3	10
4	State and explain the **requirements for public key cryptography**.	CO2	L2	10
5	With the help of a diagram, explain the **RSA algorithm**. Show the encryption and decryption of the plaintext $P = 7$ using $p = 3, q = 11, e = 7.$	CO2	L2	10
6	Discuss the **security advantages of RSA**.	CO2	L3	10
7	Explain the **Diffie–Hellman key exchange algorithm** with an example, taking small prime numbers to illustrate key generation.	CO2	L2	10
8	Explain the concept of **exponentiation in modular arithmetic** and its importance in cryptography.	CO2	L2	10
9	Describe the **man-in-the-middle attack** in Diffie–Hellman key exchange with a neat diagram.	CO2	L3	10
10	Describe the **process of elliptic curve cryptography and** Discuss the **security advantages of ECC**.	CO2	L3	10

Module 3

SL#	Question	CO	Level	Marks
1	Discuss the importance key length recommendations when implementing a cryptosystem	CO 3	L3	10
2	How are key length and key lifetime interdependent in practice? Why limiting key life time is important?	CO 3	L2	10

3	List and explain the benefits of enforcing limited lifetimes for cryptographic keys in an organization	CO 3	L2	10
4	Explain the concept of **key derivation** in cryptography	CO 3	L2	10
5	Explain the stages of the cryptographic key life cycle and discuss their significance in maintaining security	CO 3	L2	10
6	Explain the concept of Key Hierarchies in detail	CO 3	L2	10
7	List and explain the benefits of enforcing limited lifetimes for cryptographic keys in an organization	CO 3	L2	10
8	Explain advantages of deriving keys from other keys	CO 3	L2	10
9	What is a Unique Key Per Transaction (UKPT)? Explain the motivation behind using UKPT and discuss its applications	CO 3	L3	10
10	Illustrate generic UKPT scheme with neat diagram.	CO 3	L3	10
11	Compare **Racal UKPT scheme and Derived UKPT scheme**	CO 3	L4	8
12	Explain steps involved in BB84 protocol	CO 3	L2	8
13	List the limitations of Quantum Key Establishment	CO 3	L2	8
14	Explain concept of Key storage in Software and Hardware	CO 3	L2	10
15	Explain the risk involved in Key storage	CO 3	L2	10
16	Explain concept of Key separation	CO 3	L2	10
17	Explain the need and impact of key change	CO 3	L2	10
18	Write a note on Key activation and Key destruction	CO 3	L1	10
19	Briefly explain Certificate life cycle	CO 3	L2	10
20	Write note on Certificate creation	CO 3	L2	5
21	Illustrate Public key management models with neat diagram	CO 3	L3	10

Module 4

SL#	Question	CO	Level	Marks

1	What are the major web security threats commonly faced by modern web applications, and how do they impact data confidentiality and integrity?	CO 4	L1	5
2	Explain the architecture of the Transport Layer Security (TLS) protocol with TLS session state and Connection state parameters	CO 4	L2	10
3	Describe the operation of the TLS Record Protocol and TLS Record format with neat labeled diagram.	CO 4	L3	10
4	Explain the TLS Alert Protocol. Discuss its purpose, alert levels, and common alert messages.	CO 4	L2	10
5	Explain the TLS Handshake Protocol and describe the sequence of steps involved in establishing a secure session	CO 4	L2	10
6	Discuss the TLS Heartbeat Protocol, highlighting its purpose, message types	CO 4	L3	8
7	List and explain the applications of IPsec. What are the main benefits of deploying IPsec in an organization	CO 4	L3	8
8	Illustrate Transport Mode and Tunnel Mode in IPsec ESP	CO 4	L3	10
9	List the main parameters stored in the Security Association Database.	CO 4	L2	8
10	Describe how IPsec uses the SAD during inbound and outbound packet processing.	CO 4	L3	10
11	Describe the ESP packet format with a neat diagram. Explain the role of each field.	CO 4	L3	10
12	Discuss how ESP works in Transport Mode and Tunnel Mode with examples.	CO 4	L3	10
13	Discuss the role of the Key Determination Protocol within the IKE (Internet Key Exchange) framework.	CO 4	L3	**10**
14	Describe the message flow in IKEv2 exchanges with a neat diagram.	CO 4	L3	10
15	Describe the IKE header format with a neat diagram. Explain the significance of each field.	CO 4	L3	10

Module 5

SL#	Question	CO	Level	Marks
1	Explain the applications andbasic features of data hiding in text with suitable examples.	CO 5	L2	10
2	Explain intuitive methods used for hiding data in text.	CO 5	L2	10
3	Describe the syntactic method and semantic method of data hiding in text	CO 5	L3	10
4	Examine the role of innocuous text in steganography with a suitable example.	CO 5	L3	10

5	Explain how CFG helps in creating statistically similar mimic text for hiding messages.	CO 5	L3	10
6	What is LSB encoding and how is it used in image steganography	CO 5	L1	10
7	Explain BPCS steganography briefly.	CO 5	L2	10
8	What is lossless data hiding	CO 5	L1	5