P P SAVANI UNIVERSITY

Fifth Semester of B. Sc. IT Examination

December 2021

SSIT3520 Computers & Network Security

09.12.2021, Thursday **Time: 09:00 a.m. To 11:30 a.m.** **Maximum Marks: 60**

Instructions:

1. The question paper comprises of two sections.
2. Section I and II must be attempted in separate answer sheets.
3. Make suitable assumptions and draw neat figures wherever required.
4. Use of scientific calculator is allowed.

SECTION – I

Q - 1 Answer the Following: (Any Five) **[05]**

(i) _____means information needs to be hidden from unauthorized access.

(ii) Which of the following is an attack on integrity of data?
a. Snooping b. Spoofing c. Denial of Service d. None of the above

(iii) Playfair cipher is a stream cipher. True/False

(iv) What is steganography?

(v) Which of the following component is self-invertible?
a. P-Box b. S-Box c. XOR d. None of the above

(vi) Which of the following is not monoalphabetic cipher?
a. Ceaser Cipher b. Playfair Cipher c. Multiplicative cipher d. affine cipher

(vii) _____ means hiding the relationship between plaintext and ciphertext.

Q - 2 (a) List out various security services. Explain any three. **[05]**

Q - 2 (b) Consider a to z alphabets and 0 to 9 numbers for construction of Playfair matrix. Consider i and j in separate cell. Construct a 6*6 Playfair matrix with key="ppsu123". Perform the encryption of the message "established in 2017" **[05]**

OR

Q - 2 (a) What are the three security goals? Explain in detail. Enlist the various attacks threatening the three security goals. **[05]**

Q - 2 (b) Find the multiplicative inverse of 132 in Z_{180} using Extended Euclidean Algorithm **[05]**

Q - 3 (a) Consider encryption key $K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$ in Hill Cipher. Perform the encryption of message "security" **[05]**

Q - 3 (b) Encrypt the message "Enemy attacks tonight" using Keyed Transposition cipher having permutation key [3 1 4 5 2]. **[05]**

OR

Q - 3 (a) Use the Vigenère cipher with the keyword "HEALTH" to encipher the message "Life is full of surprises" **[05]**

Q - 3 (b) Explain ciphertext-only attack **[05]**

Q - 4 Attempt any one: **[05]**

(i) What are the components of Modern Block Ciphers? Distinguish them between invertible, self-invertible and non-invertible components.

(ii) Distinguish between a Monoalphabetic and a Polyalphabetic cipher. List three Monoalphabetic ciphers. List three Polyalphabetic ciphers.

SECTION – II

Q - 1 Answer the Following: (Any Five) **[05]**

(i) Define a session key.

(ii) In RSA if Bob chooses 7 and 11 as p and q then what is the value of n and Ø(n).

(iii) Asymmetric Key Cryptography is faster than Symmetric Key Cryptography. True/False

(iv) In asymmetric key cryptography, the private key is kept by _____

a. Sender b. receiver c. sender and receiver d. all the connected devices to the network

(v) What is data size in DES?

a. 64 b. 28 c. 32 d.196

(vi) Out of following, RSA is mainly used to encrypt _____.

a. Numbers b. Characters c. Numbers and Characters d. Numbers, Characters and Symbols

(vii) What is one-way function?

Q - 2 (a) Draw and explain the structure of round in DES. [05]

Q - 2 (b) Define the weak keys, semi weak keys and possible weak keys in DES. [05]

OR

Q - 2 (a) Explain the diffusion and confusion in block cipher with example. [05]

Q - 2 (b) Draw the structure of Key Expansion Process in AES. [05]

Q - 3 (a) Assume that g = 7 and p = 23. Alice chooses x = 3 and Bob chooses y = 6. Show the Diffie-Hellman Key agreement process through which Alice and Bob agree to same key for encryption and decryption. [05]

Q - 3 (b) Explain the process through which public keys are distributed by Certification Authority. [05]

OR

Q - 3 (a) What is Trapdoor One-Way Function. Explain the Trapdoor One-Way Function in context of Knapsack Cryptosystem. [05]

Q - 3 (b) Explain the Key Generation Process in RSA. [05]

Q - 4 Attempt any one: [05]

(i) Draw and explain the format of X.509 Digital Certificate.

(ii) Explain the different types of Malware threatening the security of system.

****

P P SAVANI UNIVERSITY

Fifth Semester of B. Sc. IT Examination

December 2021

SSIT3520 Computers & Network Security

09.12.2021, Thursday **Time: 09:00 a.m. To 11:30 a.m.** **Maximum Marks: 60**

Instructions:

1. The question paper comprises of two sections.
2. Section I and II must be attempted in separate answer sheets.
3. Make suitable assumptions and draw neat figures wherever required.
4. Use of scientific calculator is allowed.

SECTION – I

Q - 1	Answer the Following: (Any Five)	**[05]**
(i)	Which of the following is an attack on integrity of data? a. Snooping b. Spoofing c. Denial of Service d. None of the above	
(ii)	Which of the following is not monoalphabetic cipher? a. Ceaser Cipher b. Playfair Cipher c. Multiplicative cipher d. affine cipher	
(iii)	What are the number of keys is required if m people want to communicate with each other in symmetric key cryptography?	
(iv)	What is Kerchoff's principal?	
(v)	To be resistant to exhaustive-search attack, a modern block cipher needs to be designed as a substitution cipher. True/False	
(vi)	What is Cryptanalysis?	
(vii)	Playfair cipher is a block cipher. True/False	
Q - 2 (a)	List out various security services. Explain any three.	**[05]**
Q - 2 (b)	List and explain various cryptanalysis attacks	**[05]**
	OR	
Q - 2 (a)	List out various security mechanisms. Explain any three.	**[05]**
Q - 2 (b)	Explain the additive cipher with example.	**[05]**
Q - 3 (a)	Use the Playfair cipher to encipher the message "The key is hidden under the door pad". The key is "GUIDANCE". Use 5*5 key matrix having i and j in same cell.	**[05]**
Q - 3 (b)	Draw and explain Feistel Cipher design with two rounds.	**[05]**
	OR	
Q - 3 (a)	Encrypt the message "Enemy attacks tonight" using keyed transposition cipher having permutation key [3 1 4 5 2].	**[05]**
Q - 3 (b)	Explain the diffusion and confusion in block cipher with example.	**[05]**
Q - 4	Attempt any one:	**[05]**
(i)	Find the multiplicative inverse of 132 in Z_{180} using Extended Euclidean Algorithm	
(ii)	Explain the various components of modern block ciphers	

SECTION – II

Q - 1	Answer the Following: (Any Five)	**[05]**
(i)	List the two classes of product cipher.	
(ii)	What is Avalanche Effect?	
(iii)	Which of the round in DES used two bits shift in round key generation? a. 1 b. 2 c. 3 d.16	
(iv)	The state in AES consists of how many bytes? a. 4 b.8 c.16 d.32	
(v)	Which of the following attack is possible on Diffie-Hellman key exchange? a. Discrete Logarithm b. Man in the middle c. Both (a) and (b) d. None of the above	

(vi)	What are the three variations of P-Box?	
(vii)	Define a session key.	
Q - 2 (a)	What is the size of plaintext, cipher text and key in DES? How many rounds are there in DES? Draw the general structure of DES.	**[05]**
Q - 2 (b)	Define the weak keys, semi weak keys and possible weak keys in DES	**[05]**
	OR	
Q - 2 (a)	What is the size of plaintext, cipher text and key in AES? How many rounds are there in AES? Draw the general structure of AES.	**[05]**
Q - 2 (b)	Draw the structure of Key Expansion in AES	**[05]**
Q - 3 (a)	In RSA, given p=19, q=23 and e=3, find n, Ø(n) and d. Perform the encryption of plaintext P=15.	**[05]**
Q - 3 (b)	Explain the man-in-the-middle attack on Diffie-Hellman Key Agreement Protocol.	**[05]**
	OR	
Q - 3 (a)	Explain the Diffie-Hellman Key Agreement protocol.	**[05]**
Q - 3 (b)	Prove that in RSA, encryption and decryption process are inverse of each other.	**[05]**
Q - 4	Attempt any one/two.	**[05]**
(i)	Assume that a= [17,25,46,94,201,400] and s=272. Apply the inv_knapsackSum algorithm to find the value of tuple x.	
(ii)	Define the following terms: Virus, Trojan Horse, Spyware, Adare, Worms	

****