Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION, DECEMBER 2018

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORK SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1		Differentiate between computationally secure cipher and unconditionally secure cipher. Write examples with reasoning.	(4)
2		Encrypt the message "this is an exercise" using the additive Cipher with key=20	(4)
3		What is the necessity of block cipher modes of operation? List out the advantages and disadvantages of ***output feedback*** mode.	(4)
4		Generate the key attributes for the values p = 11 and q = 3. Also encrypt the message m = 2 with the generated keys.	(4)
5		Find gcd (1970, 1066)	(4)
6		Discuss digital signature scheme using RSA	(4)
7		Write the general structure of Private Key Ring used in Pretty Good Privacy (PGP).	(4)
8		What are the functionalities provided by Secure MIME (S/MIME)?	(4)
9		What is the significance of Alert Protocol in Transport Layer Security?	(4)
10		Why the attacker is not able to recognize the actual sender of the message in encrypted tunnels?	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Use Playfair Cipher with key COMPUTER to encrypt the message "CRYPTOGRAPHY".	(5)
	b)	How key generation is done in DES.	(4)
12	a)	Discuss the stream cipher RC4 in detail	(4)
	b)	Illustrate the round transformation of IDEA.	(5)
13	a)	Encrypt the text "LOVE" using Hill Cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$	(4)
	b)	Illustrate S box creation in AES	(5)

PART C

Answer any two full questions,each carries 9 marks.

14 a) Define Euler's Totient Function. Prove that, $\phi(pq) = (p-1)(q-1)$, where p and q are prime numbers. (5)

b) Demonstrate Diffie Hellman Key exchange algorithm. (4)

15 Illustrate the working of SHA-1 with diagrams. (9)

16 a) What are the Security Requirements of message authentication? (4)

b) Give the encryption/decryption procedures using Elliptic Curve Cryptography. (5)

PART D

Answer any two full questions, each carries 12 marks.

17 a) Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagrams. (8)

b) List out the security association (SA) parameters in IPSec. (4)

18 a) Illustrate the working of Secure Electronic Transaction (SET) in detail. (8)

b) Compare Packet filter and Application Level Gateways. (4)

19 a) Explain the method of protecting IP datagram from replay attack using IPsec. (6)

b) Explain the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol. (6)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION(S), MAY 2019

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORK SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1		How the nonlinearity is achieved in DES.	(4)
2		Differentiate Confusion and Diffusion.	(4)
3		Discuss the key expansion procedure in AES	(4)
4		State and prove Fermat's Theorem	(4)
5		In a public key system using RSA, you intercept the cipher text C=8 sent to a user whose public key is e=13, n=33. What is the plain text M?	(4)
6		Compare the strength of MAC and Encryption against brute-force attack	(4)
7		Give the header format of ESP in IPSec	(4)
8		Give the authentication methods used in Oakley algorithm	(4)
9		What are the services provided by Record Layer Protocol for Secure Socket Layer connections?	(4)
10		What are the characteristic features of stateful inspection firewall?	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Differentiate between monoalphabetic ciphers and polyalphabetic ciphers and give one example for each.	(5)
	b)	Give different techniques used in steganography	(4)
12	a)	How key generation is performed in IDEA	(4)
	b)	Discuss Mix Column transformation in AES	(5)
13	a)	Using rail fence cipher, encrypt the text *meet me after the toga party* using the key *4 3 1 2 5 6 7*.	(4)
	b)	Illustrate inverse S box creation in AES.	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	Find gcd(240, 46) using Extended Euclid's Algorithm	(4)
	b)	Discuss the key exchange procedure using Elliptic Curves.	(5)

15 Illustrate MD 5 hash algorithm in detail (9)

16 a) Consider a Diffie Hellman scheme with a common prime q = 11 and primitive root α = 2. (5)

i. Show that 2 is a primitive root of 11.

ii. If user A has public key $Y_A = 9$, what is A's private key?

iii. If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A

b) Discuss Digital Signature Algorithm (4)

PART D

Answer any two full questions, each carries 12 marks.

17 a) What are the steps used for preparing an enveloped data and signed data in MIME entity? (6)

b) Discuss the message format of PGP. (3)

c) How the integrity is achieved using ICV in Authentication Header. (3)

18 a) Illustrate the relevance of dual signature in SET. (4)

b) Discuss SSL record protocol operations. (6)

c) What are the requirements of Encrypted Tunnels? (2)

19 a) Give the significance of SA selectors in IPSec. (4)

b) Why compression is done before encryption in PGP? (2)

c) Discuss different Firewall configurations. (6)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION(R&S), DECEMBER 2019

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORKSECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1		Explain confusion and diffusion properties of modern block ciphers	(4)
2		Differentiate between symmetric and asymmetric cryptosystem	(4)
3		Explain the mix column operation in AES algorithm	(4)
4		Compute 3^{61} mod 7.	(4)
5		What are the requirements of a good hash function	(4)
6		How digital signature is implemented using RSA approach	(4)
7		What are the steps for preparing a SignedData MIME entity?	(4)
8		Give the format of Authentication Header in IPSec	(4)
9		Explain the handshake protocol in SSL	(4)
10		List the various attacks that can be made on packet filtering routers and mention appropriate counter measures	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Use Playfair cipher to encrypt the message 'THE HOUSE IS BEING SOLD TONIGHT ' with the key 'GUIDANCE'	(4)
	b)	Differiante between monoalphabetic and polyalphabetic ciphers with example	(5)
12	a)	Explain the S-box design of DES algorithm.	(4)
	b)	Illustrate RC4 algorithm	(5)
13	a)	Explain the key generation in AES algorithm	(5)
	b)	How round transformation is performed in IDEA.	(4)

PART C

Answer any two full questions,each carries 9 marks.

14	a)	Explain the algorithm for generating keys in RSA algorithm. Perform encryption and decryption using RSA Alg. for the following.. P=7; q=11; e=13; M=8	(6)
	b)	Illustrate man in the middle attack on Diffie Hellman key exchange algorithm	(3)
15		Illustrate the working of SHA-1 algorithm with diagram	(9)

16	a)	How signing and verification is done in Digital Signature algorithm.	(5)
	b)	Illustrate Elliptic Curve Encryption/Decryption	(4)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Explain in details about the message generation and reception in Pretty Good privacy with neat diagram	(8)
	b)	Explain the construction of dual signature in SET protocol	(4)
18	a)	Explain the various protocols used in SSL	(8)
	b)	Draw and explain IPSec ESP Format	(4)
19	a)	Explain the role of Security Association and SA selectors in IPSec.	(6)
	b)	Discuss about the various types of firewalls	(6)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh semester B.Tech examinations (S), September 2020

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORKSECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks.

			Marks
1		Which parameters and design choices determine the actual algorithm of a Fiestel Cipher.	(4)
2		Encrypt the message **"the house is being sold tonight"** using Vigenere cipher with key "*dollars*". Ignore the space between words. Decrypt the message to get the plain text.	(4)
3		Compare stream cipher and block cipher with example.	(4)
4		Find gcd(252,105).	(4)
5		List different types of attacks addressed by message authentication.	(4)
6		Illustrate Needham and Schroedor protocol for mutual authentication.	(4)
7		Compare transport mode and tunnel mode functionalities in IPSec.	(4)
8		List out the five header fields and their meaning defined in MIME.	(4)
9		What are the steps involved in the SSL record protocol transmission?	(4)
10		Compare SSL and TLS.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Discuss about different polyalphabetic cipher substitution techniques.	(4)
	b)	Explain single round of DES algorithm.	(5)
12	a)	Differentiate between Confusion and Diffusion.	(4)
	b)	Explain the key generation in IDEA.	(5)
13		Explain AES algorithm in detail.	(9)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	Alice and Bob agreed to use RSA algorithm for the secret communication. Alice securely choose 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. Find the plain text.	(6)
	b)	State and prove Euler's theorem.	(3)

15	a)	Explain three different Arbitrated Digital Signature Techniques.	(9)
16	a)	What is suppress replay attack in authentication? Explain the protocol used to eliminate this attack.	(4)
	b)	Explain the key exchange procedure using Elliptic Curves.	(5)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Explain the sequence of steps involved in the message generation and reception in PGP with block diagrams.	(8)
	b)	List out the benefits of IPSec.	(4)
18	a)	Explain the features of any two types of firewalls.	(6)
	b)	Explain the sequence of operations required for Secure Electronic Transaction.	(6)
19	a)	Explain the format of IPSec ESP Packet.	(6)
	b)	Illustrate the overall operation of SSL Record Protocol.	(6)

****

Reg No.:_____ **00000CS409121901** Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree Examination (Regular and Supplementary), December 2020

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORKSECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1		What are the two approaches to attack a cipher? Give example for each.	(4)
2		Use **autokey** system of Vigenere cipher to encrypt the message "*meet me after the toga party*" using the key **"largest".**	(4)
3		Illustrate the key expansion procedure of IDEA.	(4)
4		Define Euler's Totient Function. Compute ϕ (41) and ϕ (115).	(4)
5		Distinguish between conventional encryption and public key encryption system.	(4)
6		Explain any two ways in which a hash code can be used to provide message authentication.	(4)
7		Why PGP generate a signature before applying compression	(4)
8		List out the security association parameters in IPSec.	(4)
9		What is the significance of Alert protocol in SSL and list out any three Alert messages and their use?	(4)
10		What are the key features provided by SET?	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Encrypt the word "Semester Result" with the keyword "Examination" using play fair cipher. List the rules used	(5)
	b)	Depict a block cipher mode that can be used to convert block cipher to stream cipher.	(4)
12	a)	Explain AES key expansion procedure.	(4)
	b)	Explain the primitive operations of RC4.	(5)
13	a)	Using double stage columnar transposition technique, encrypt the text "Cryptography and Network Security" using the key "43125".	(4)
	b)	Explain the construction of S-box in AES algorithm.	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	User A and B exchange the key using Diffie -Hellman algorithm. Assume α=5, q=11, X_A =2, X_B =3. Find the values of Y_A, Y_B, and K.	(3)
	b)	Summarize the RSA algorithm with example.	(6)
15		Illustrate MD5 hash algorithm in detail.	(9)
16	a)	State and prove Fermat's Theorem. Use Fermat's theorem to find 3^{62} mod 7	(5)
	b)	Explain message authentication code based on DES.	(4)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	What are the five principal services provided by PGP and explain how authentication and confidentiality are provided?	(6)
	b)	Explain the functionalities provided by S/MIME.	(6)
18	a)	Compare the features of three types of Firewall.	(9)
	b)	What is the significance of dual signature in SET?	(3)
19	a)	Define the parameters that define an SSL session state.	(6)
	b)	Give the format of IPSec Authentication header.	(6)

****