Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Ninth Semester MCA Integrated Degree Regular and Supplementary Examination December 2021

Course Code: RLMCA305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1	Identify and define with example two classical encryption techniques?	(3)
2	Define Group and Ring with examples	(3)
3	What is Data Encryption Standard?	(3)
4	How authenticity and confidentiality achieved in encryption by using public key?	(3)
5	What are the properties of hash functions?	(3)
6	What is bitcoin script? Explain its processing procedure.	(3)
7	What is Encapsulating Security Payload (ESP)?	(3)
8	What is Non-Repudiation? Explain Non-Repudiation based on Public Key Technology.	(3)

PART B

Answer six questions, one full question from each module and carries 6 marks.

Module I

9	a)	Explain active attacks and passive attacks.	(3)
	b)	Given the key ‘MONARCHY’, apply the Playfair cipher to the plaintext ‘FACTIONAISM’. Decrypt the ciphertext also.	(3)

OR

10	a)	Explain one-time pad. What are the two problems with the one-time pad?	(3)
	b)	Explain the symmetric cipher model.	(3)

Module II

11 State and prove Euler’s theorem. (6)

OR

12 Explain the Miller- Rabin algorithm for testing primality. (6)

Module III

13 With a suitable diagram explain Cipher Block Chaining (CBC) mode. (6)

OR

14 Discuss the different attacks on RSA. (6)

Module IV

15 What do you mean by Message Authentication? Explain Cipher-Based Message Authentication code (CMAC). (6)

OR

16 Explain Digital Signature Algorithm (DSA) in detail. (6)

Module V

17 a) Explain Scrooge Coin. (2)

b) What are the two kinds of transactions in Scrooge Coin? (4)

OR

18 Explain bitcoin transactions. (6)

Module VI

19 a) Explain S/MIME. (3)

b) Explain Exportability in SSLv2 and Exportability in SSLv3. (3)

OR

20 Explain Object formats and Primitive Object formats in PGP. (6)

****

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Ninth Semester MCA Dual Degree (Integrated) Regular Examination December 2020

Course Code: RLMCA305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each question carries 3 marks. Marks

1 Illustrate symmetric cipher model in cryptography. (3)

2 Compute the multiplicative inverse of 23 in Z_{100}. (3)

3 Write short note on modern stream ciphers. (3)

4 Compare and contrast symmetric and asymmetric key encryption. (3)

5 List out the classification of digital signature schemes. (3)

6 Discuss the features of Bitcoin. (3)

7 Illustrate PGP message format in Email security. (3)

8 Explain security services for Email. (3)

PART B

Each question carries 6 marks.

Module I

9 Explain security services and mechanisms in cryptography. (6)

OR

10 Explain steganography method with text covering process. (6)

Module II

11 Explain Euclidean algorithm and find the multiplicative inverse of 11 in Z_{26} using the algorithm. (6)

OR

12 Give a short note on the following. (6)

i) Fermat's theorem

ii) Euler's theorem

iii) Testing for Primality

Module III

13 Define Asymmetric key Cryptography and explain about the RSA cryptosystem with suitable example. (6)

OR

14 Explain Data Encryption Standard with a neat diagram. (6)

Module IV

15 Define hash functions? What is its significance? (6)

OR

16 Describe various attacks on digital signature. (6)

Module V

17 Discuss the process of storing and usage of Bitcoins in network. (6)

OR

18 Illustrate and explain Bitcoin transaction in network. (6)

Module VI

19 Discuss the protocols of SSL. (6)

OR

20 Explain two modes of IPSEC. (6)

****

C M192013 Pages:2

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER MCA DEGREE EXAMINATION, DECEMBER 2019

MCA(SECOND YEAR DIRECT) S3 (R&S)

Course Code: RLMCA 305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1 Define steganography with an example. (3)

2 Find multiplicative inverse of 7 in Z_{180} using the extended Euclidean algorithm. (3)

3 Compare and contrast block and stream ciphers. (3)

4 Illustrate the structure of symmetric key encryption and decryption. (3)

5 Write short note on blind signatures. (3)

6 Discuss the various applications of bitcoin scripts. (3)

7 Illustrate the architecture of SSL protocol. (3)

8 Illustrate PGP message format in Email security. (3)

PART B

Each question carries 6 marks.

9 Explain security services and mechanisms in cryptography. (6)

OR

10 Discuss on various substitution ciphers with examples. (6)

11 Write short notes on the following. (6)

i) Group

ii) Ring

iii) Field

OR

12 Give a short note on the following. (6)

i) Fermat’s theorem

ii) Euler’s theorem

iii) Testing for primality

13 Explain RSA cryptosystem with example. (6)

OR

14 With a neat diagram explain AES algorithm. (6)

15 Define MAC and explain any one MAC algorithm with suitable diagram. (6)

OR

16 Explain the RSA digital signature scheme in cryptography. (6)

17 Describe the role of distributed consensus in bitcoin transactions. (6)

OR

18 Define crypto currency. Explain scrooge coin and goofy coin. (6)

19 Explain S/MIME protocol with its applications. (6)

OR

20 Write short notes on the following. (6)

i) Handshake protocol

ii) Alert protocol

iii) Record protocol

iv) Change cipherspec protocol

****

Reg No.:_______________ Name:____________________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER REGULAR AND THIRD SEMESTER SECOND YEAR DIRECT MCA DEGREE EXAMINATION(S) MAY 2019

Course Code: RLMCA305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries3 marks. Marks

1	Explain Distributed Denial of Service (DDoS) attack on network security.	(3)
2	Discuss on Euler Totient function.	(3)
3	Draw the block diagram of Cipher block chaining mode(CBC) in Block ciphers. Give one of its advantage compared to Electronic code book(ECB).	(3)
4	Explain birth day attack.	(3)
5	Explain Scrooge Coin.	(3)
6	Describe the main applications of Public key cryptography.	(3)
7	Briefly explain the Authentication header format in IP security.	(3)
8	Briefly describe the different PGP services.	(3)

PART B

Answer six questions, one full question from each module and carries 6 marks.

Module I

9	With the help of a neat diagram, explain network security model.	(6)
	OR	
10	Construct a Playfair matrix with the key *largest* , Using this playfair matrix encrypt the message “Happiness is a Journey not a destination”	(6)

Module II

11	Discuss on Miller Rabin Algorithm for primality testing.	(6)
	OR	
12	Determine the GCD of the polynomials $x^6+x^5+x^4+x^3+x^2+x+1$ and x^4+x^2+x+1 over GF(2).	(6)

Module III

13 Explain an Diffie-hellman key exchange algorithm (6)

OR

14 With the help of block diagram explain DES. (6)

Module IV

15 With a neat diagram explain HMAC algorithm. (6)

OR

16 With the help of a block diagram explain the RSA algorithm for digital signature. (6)

Module V

17 Explain how bitcoin Achieves Decentralization. (6)

OR

18 Explain the different methods used for bitcoin storage. (6)

Module VI

19 With the help of neat diagram explain SSL protocol stack. (6)

OR

20 Draw the top-level format of an ESP packet and explain the different fields (6)

****

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER MCA DEGREE EXAMINATION, DECEMBER 2018

Course Code: RLMCA 305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1	List out the security services provided in cryptography.	(3)
2	Determine the multiplicative inverse of X^2+1 in $GF(2^4)$ with $m(x)=X^4+X+1$.	(3)
3	Compare and contrast DES and AES.	(3)
4	Discuss any three modes of operation in block ciphers.	(3)
5	List out criteria of a cryptographic hash function.	(3)
6	Define a simple crypto currency with examples.	(3)
7	Describe security association of IPSEC.	(3)
8	Write short note on S/MIME services.	(3)

PART B

Each question carries 6 marks.

9 Explain in detail about the Substitution ciphers with suitable examples. (6)

OR

10 Illustrate and explain symmetric cipher model with various attacks. (6)

11 Write short notes on the following. (6)

i) Group

ii) Ring

iii) Field

OR

12 Explain extended Euclidean algorithm and apply extended Euclidean algorithm to calculate gcd(161,28). (6)

13 List out and explain the components of block ciphers in symmetric key encryption. (6)

OR

14 Discuss the four types of transformations used by AES. (6)

15 Explain various digital signature schemes with suitable diagram. (6)

OR

16 Describe the various components used for message integrity in cryptography. (6)

17 Define a bitcoin. Explain how bitcoin achieves decentralization. (6)

OR

18 Explain the process of splitting and sharing keys in bitcoin network. (6)

19 Name the seven types of packets used in PGP and explain their purpose. (6)

OR

20 Explain in detail about the SSL architecture and SSL message format with suitable diagram. (6)

****

C C7416

Total Pages: 1

Reg No.:______________ Name:________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

THIRD SEMESTER MCA DEGREE EXAMINATION, DECEMBER 2017

Course Code: RLMCA305

Course Name: CRYPTOGRAPHY AND CYBER SECURITY

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries3 marks. Marks

1	Explain about steganography.	(3)
2	Distinguish between groups and rings.	(3)
3	Explain the concept of public key cryptography.	(3)
4	What is Cipher Feed Back mode (CFB)?	(3)
5	Write short notes on birthday attacks.	(3)
6	Define the term Goofy coin.	(3)
7	Explain about S/MIME.	(3)
8	Define the term pretty good privacy.	(3)

PART B

Answer six questions, one full question from each module and carries6 marks.

Module I

9 Explain network security model with the help of a neat diagram. (6)

OR

10 Explain about play fair cipher and Hill cipher. (6)

Module II

11 Explain Chinese remainder theorem with example. (6)

OR

12 State and prove Fermat’s theorem. (6)

Module III

13 Explain Diffie Hellman key exchange algorithm. (6)

OR

14 Explain RSA algorithm with example. (6)

Module IV

15 Explain about Message Authentication Code algorithm. (6)

OR

16 Explain about digital signature scheme. (6)

Module V

17 What is bitcoin script? Explain applications of Bitcoin scripts. (6)

OR

18 What are bitcoin exchanges? Explain about online wallets? (6)

Module VI

19 Explain about IP security. (6)

OR

20 Discuss web security in detail. (6)

****