University Exam DECEMBER 2021

Subject: Cryptography & Network Security
Semester: V
Year : Third Year

Course Code: ITC502
Branch: Information Technology
Marks : 80

1] All questions are Compulsory
2] Assume suitable data wherever required.

MCQ Section

Q1. Attempt all questions. [10*2=20M]

Q.	Question Statement	OPTION A:	OPTION B:	OPTION C:	OPTION D:
1	Which is a passive attack?	Traffic Analysis	Replaying	Denial of Service	Reputation
2	An…….algorithm transforms plaintext to ciphertext	Decryption	Encryption	Key	Cipher text
3	Cryptanalysis is used _____	to find some insecurity in a cryptographic scheme	to increase the speed	to encrypt the data	to make new ciphers
4	In RSA, if p=17, q=11, then, what is phi(n)?	189	187	160	161
5	…… is Hash Function Properties which measures how difficult to devise a message which hashes to the known digest and its message	duplication	Second preimage resistant	Collision resistant	Preimage resistant
6	Define Non-Repudiation	It means that sender and receiver expect privacy	It means that the data received at the receiver is exactly same as sent.	It means that a sender must not be able to deny sending a message that he sent	It means that the receiver is ensured that the message is coming from the intended sender, not an imposter.

6	Digital signature certification is needed by an independent authority because	private key claimed by a sender may not be actually his	it is safe	it gives confidence to a business	the authority checks and assures customers that the public key indeed belongs to the business which claims its ownership
7	Kerberos consists of__	Authorization Server	Client Server	Authentication server	Mail server
8	Which is not a Header Fields defined in MIME	Content-Log	Content-Type	Content-Transfer-Encoding	Content-Description
9	The Payload Data,_____ Pad Length, Next header fields are encrypted by the ESP service.	Anti -Replay Service	Sequence Parameters index	Sequence Numbers	Padding.
10	Malware which is independent self-contained program	Worm	Virus	Trojan Horse	Bomb

Descriptive Section

Attempt all questions. [60M]

Q2. Write Short note on (Any 4 each for 5 Marks)

A) Security Services
B) RC5 Algorithm
C) HMAC
D) Types of Firewalls
F) PKI

Q3. Attempt the following (Any 2 each for 10 Marks)

A) Explain keyed and keyless transposition ciphers with example.
B) Explain in details DES Algorithm and Compare with AES.
C) Explain principle NAC of enforcement methods.

Q4. Attempt the following (Any 2 each for 10 Marks)

A) Explain different malicious software with example.

B) Explain Email Security in detail.

C) In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35 and Message 12. Then find out the private key of A and Ciphertext C.