University of Mumbai
Examinations Summer 2022
Program: T.E. (Computer Engineering) (SEM-VI) (Choice Base Credit Grading System) (R2016)
Examination: TE Semester VI
Subject (Paper Code): 88904 / Cryptography and System Security

Time: 2 hour 30 minutes Max. Marks: 80

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	multiplicative inverse of 6 in Z10
Option A:	0
Option B.	4
Option C:	there is no multiplicative inverse
Option D:	1
2.	In DES algorithm if the input to S-box is 110011 then which row and column will select from the S-box for 4 bits representation?
Option A:	row 9, column 3
Option B:	row 3, column 9
Option C:	row 1, column 9
Option D:	row 3, column 9
3.	Aana wants to digitally sign her message and send it to Boby. For signing her message, she will use key and for verifying message Boby will use key
Option A:	Aana's Private Key, Aana's public key
Option B:	Boby's public Key, Aanna's public key
Option C:	Aana's public key, Boby's private key
Option D:	Boby's public key, Boby's private key
4.	The security service which is not provided by the Digital Signature is
Option A:	Authentication
Option B:	Confidentiality
Option C:	Integrity
Option D:	None of the above
5.	We cannot use hash function as an Encryption function because
Option A:	It's a one-way function
Option B:	It's a two-way function
Option C:	It's a subway function
Option D:	It's a trapdoor function
6.	Which of the following is a program capable of continually replicating with little or no user intervention?
Option A:	Viruses
Option B:	Trojan horses
Option C:	Bots
Option D:	Worms
7.	The mechanism for safeguarding private networks from outside attacks is ...
Option A:	Firewall
Option B:	Antivirus
Option C:	Digital signature
Option D:	Formatting
8.	Which of the following statement are true (i) Block Ciphers can use particular key for many encryption (ii) ECD mode is more suitable than CBC mode while encrypting a long bit string
Option A:	Only i
Option B:	Only ii
Option C:	Both
Option D:	None of them

9.	A small change in plaintext results in the very great change in the ciphertext.
Option A:	Avalanche effect
Option B:	Completeness
Option C:	Incompleteness
Option D:	Illusion
10.	SSL full form is
Option A:	Secure Sockets Layer
Option B:	Socket Secure Layer
Option C:	Security Socket Layer
Option D:	Synchronous Socket Layer

Q2	**Solve any Two Questions out of Three** **10 marks each**
A	Using hill cipher perform following operation key is $K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ 1. Encrypt text "HELP" 2. Decrypt the encrypted text
B	Explain structure of DES wrt: 1. Fiestel structure and its significance 2. Significance of extra swap between left and right half blocks 3. Expansion 4. Significance of S-box 5. No of rounds
C	How does Kerberos work? Explain applications of it

Q3	**Solve any Two Questions out of Three** **10 marks each**
A	A and B wish to use RSA to communicate securely. A chooses public key as (17,321) B chooses public key as (5,321). 1. Calculate private keys of A 2. Calculate private keys of B 3. A wish to send message m=10 to B. What will be the cipher text? 4. With what key will A encrypt the message "m" if A needs to authenticate itself to B 5. Attacks possible on RSA
B	Explain MD 5 algorithm? List requirements of hash function.
C	Explain IPsec tunnel mode and give its applications.

Q4	**Solve any Two Questions out of Three** **10 marks each**
A	What is Firewall? compare different types of Firewall in network security
B	In a Diffie-Hellman Key Exchange, 1. Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? 2. Explain attack on Diffie-Hellman. 3. How to improve security of Diffie – Hellman
C	Explain with example 1. SQL injection 2. Buffer overflow