ID NO.	

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY, BENGALURU

SCHOOL OF ENGINEERING

Weightage: 40 % Max Marks: 80 Max Time: 2 hrs. 10 May 2018, Thursday

ENDTERM FINAL EXAMINATION MAY 2018

Even Semester 2017-18 **Course: CSE 215 Cryptography and Network Security** VI Sem. CSE

Instructions:

(i) *Read the question properly and answer accordingly.*
(ii) *Question paper consists of 3 parts.*
(iii) Scientific and Non-programmable calculators are permitted

---

Part A

(4 Q x 6 M = 24 Marks)

1. Define block cipher. Describe all modes of operation on block ciphers with the help of suitable diagrams
2. Using Euclidean algorithm find the gcd(2414,1676) and 7^{-1}mod19
3. Define the following terminologies with example
   a. Fermat's little theorem
   b. Process of Digital Signature
   c. Transposition ciphers
4. List out the differences between following
   a. DES, 3-DES, AES
   b. Active attack and passive attack
   c. Caeser, monoalphabetic and polyalphabetic ciphers

Part B

(4 Q x 8 M = 32 Marks)

5. Define Hash function. With the help of block diagram of SHA-512 algorithm briefly explain the steps involved in it.
6. Explain the following concepts with respect to DES algorithm

   a. 56 bits to 48 bits key generation
   b. Substitution box

7. Alice and Bob want use the Diffie-Hellman key exchange technique with a common prime number 23 and primitive root 5.
   a. Alice’s private key is 4. What is her public key?
   b. Bob’s private key is 3. What is his public key?
   c. Find the shared secret key
8. Explain the applications of hash function in Message authentication code (MAC). Also explain MAC based on hash function (HMAC)

Part C

(2 Q x 12 M = 24 Marks)

9. Explain Elgamal Cryptosystem with appropriate equations. Also explain how this scheme can be used to derive digital signature
10. Explain hill cipher algorithm. Consider the plaintext as “crypto” and the encryption key is

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

   a. Encrypt the above message by taking 3 characters each as one row separately (totally you have to perform encryption 2 times)
   b. Find the inverse of given matrix and decrypt cipher text which you obtained in previous step

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

ID NO:	

PRESIDENCY UNIVERSITY, BENGALURU
SCHOOL OF ENGINEERING

Weightage: 20% Max Marks: 40 Max Time:1 hr. 26 March Monday 2018

TEST - 2 **SET B**

Even Semester 2017-2018 Course: **CSE 215 Cryptography and Network Security** VI. Sem CSE

Instructions:

i. Write legibly; equations are mandatory for the relevant questions
ii. Scientific and non-programmable calculators are permitted
iii. Assume the data wherever necessary

Part A

(2Q x 6 M= 12 Marks)

1. Explain the concept of man in the middle attack problem with suitable equations

2. Define Hash function. Explain the use of hash function in Digital Signatures with suitable diagram

Part B

(2Q x 8 M= 16 Marks)

3. Using Euclidean Algorithm find the value of **17^{-1} mod 43** and **7^{-1} mod19**

4. Explain the concept of Elgamal Cryptosystem with appropriate equations

Part C

(1Q x 12M= 12 Marks)

5. Consider the following parameters with respect to RSA algorithm.
Two prime numbers are **17 and 11**
Exponent **(E) =7**
Plain text **(M) = 88**
Calculate the public and private key pair, also perform encryption and decryption

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

ID NO:	

PRESIDENCY UNIVERSITY, BENGALURU
SCHOOL OF ENGINEERING

Weightage: 20 %   Max Marks: 40   Max Time: 60 Mins   21 Feb Wednesday 2018

TEST 1

Even Semester 2017-2018   Course: **CSE 215 Cryptography and Network Security**   VI SEM CSE

Instructions:

i. Write legibly

ii. Scientific and non-programmable calculators are permitted

Part A

(3Q x 4 M= 12 Marks)

1. Write the block diagram of network security model and explain the basic terminologies involved in it
2. Define block cipher and stream cipher. Explain the Feistel structure of deriving block cipher
3. List out any 4 differences between DES, Triple-DES and AES

Part B

(2Q x 6 M= 12 Marks)

4. Using Fermat's little theorem prove that the numbers 5 is prime and 6 is not prime
5. What do you mean by a **'state'** in AES algorithm? Explain SubBytes and ShiftRow operations of AES algorithm

Part C

(2Q x 8M= 16 Marks)

6. Explain Hill Cipher. Encrypt the plain text "**ABCD**" with the key "**MNOP**" using Hill Cipher. Also perform decryption process.

7. Draw the block diagram of DES algorithm and list out all the steps involved in DES. Also explain 32 bits to 48 bits data block expansion and concept of substitution boxes.