Roll No.											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

TEST - 1

Even Semester: 2018-19 | **Date**: 05 March 2019

Course Code: CSE 215 | **Time**: 1 Hour

Course Name: Cryptography & Network Security | **Max Marks**: 40

Programme & Sem: B.Tech (CSE) & VI Sem | **Weightage**: 20%

Instruction:

(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

Answer **all** the Questions. **Each** question carries **six** marks. (2Qx6M=12)

1. List all the security mechanisms defined in X.800.
2. What are the challenges of computer security?

Part B

Answer **all** the Questions. **Each** question carries **eight** marks. (2Qx8M=16)

3. Using the keyword "presidency" create the playfair matrix and obtain cipher text of the message "university". Also write the rules used.
4. Explain single round of DES along with key generation.

Part C

Answer the Question. Question carries **twelve** marks. (1Qx12M=12)

5. a. Encrypt the message "ambarisha" using the hill cipher using the key

$$K = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

Show calculations and results.

b. Show the calculation for the corresponding decryption of the cipher text to recover the original plaintext:-

Roll No.												

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

TEST - 2

Even Semester: 2018-19 | **Date**: 15 April 2019

Course Code: CSE 215 | **Time**: 1 Hour

Course Name: Cryptography and Network Security | **Max Marks**: 40

Program & Sem: B.Tech & VI Sem | **Weightage**: 20%

Instructions:

(i) ***Answer all the questions***

(ii) ***Assume the data if necessary; Non Programmable calculators are allowed***

Part A

Answer **both** the Questions. **Each** question carries **six** marks. (2Qx6M=12)

1. Briefly explain the concept of Public Key Cryptography with the block diagram of network security. State the differences between Symmetric and Asymmetric Key Cryptographic Algorithms
2. Determine the GCD (24140, 16762) using Euclidean Algorithm

Part B

Answer **both** the Questions. **Each** question carries **eight** marks. (2Qx8M=16)

3. Solve the following set of equations using Chinese Remainder Theorem

   $X \equiv 2 \pmod 7$ and

   $X \equiv 3 \pmod 9$

4. a) Explain Fermat's little theorem with each example to prime and non-prime

   b) Explain Euler Totient Function with an example

Part C

Answer the Question. The Question carries **twelve** marks. (1Qx12M=12)

5. In a public-key system using RSA, you intercept the cipher text $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M? Give step by step solution using appropriate equations.

Roll No													

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

END TERM FINAL EXAMINATION

Even Semester: 2018-19 | **Date**: 22 May 2019

Course Code: CSE 215 | **Time**: 3 Hours

Course Name: Cryptography and Network security | **Max Marks**: 80

Program & Sem: B. Tech - VI Sem | **Weightage**: 40%

Instructions:

(i) Read all instructions carefully
(ii) PART B and PART C have choices
(iii) All answers to question 1 must be on same page

Part A

Answer **all** the Questions. **Each** question carries **one** mark. (20Qx1M=20M)

All answers of question 1 must be in the SAME page.

1.

a) Hackers stole the bank account details of several account holders from www.bigbank.com by hacking this website. This is an attack on _____ component of CIA triad?

b) _____ provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

c) In a block cipher, if the input block size is n bits long, the total possible different plaintext blocks is equal to _____

d) The diffusion technique used in Feistal block cipher obscures the statistical relationships between cipher text and the key. True or False?

e) The S-box used in each round of DES, uses the first and last bit of the input to determine the column number and the inner four bits to determine the row number. True or False?

f) During the DES decryption, the round 7 uses the sub-key

i. K6 ii. K7 iii. K11 iv. K10

g) In AES encryption, during substitute bytes, using S-box operation, the S-Box is of size

i. 4 X 16 ii. 8 X 16 iii. 16 X 16. iv. 12 X 12.

h) In AES encryption, during the Shift row transformation, if the values on the third row of the input is 4A C3 46 E7, the output produced after shift row transformation is equal to

i.E7 46 C3 4A ii. C3 46 E7 4A iii. 46 E7 4A C3 iv. E7 4A C3 46.

i) If the input to the SHA-512 algorithm is 01010101 11001100, number of bits padded to this input is _____ bits.

j) In ElGamal digital signature, pair (S1, S2) the derived value component S2 does not depend on the input message. True or False?

k) In RSA, the GCD of (pq-p-q+1) and e is equal to 1, where p and q are the prime numbers and e is the encryption key. True or False?

l) If 12x is congruent to 36 mod 108, the lowest value solution for x = _____

m) If phi(n) = 48, then n = _____

n) If 7^{83} is congruent to 7 mod 83, then 7^{82} is congruent to _____

o) If additive inverse of (x+27) mod 52 is 20, then x = _____?

p) The difference between Cryptographic hash functions and Message authentication codes (MAC) is that Hash functions use key and MAC does not use key. True or False?

q) Alice uses the following values in an Elgamal digital signature scheme - alpha (primitive root) = 2, q = 19 and private key Xa = 5. The public key generated by Alice is {__,____,___}

r) In RSA encryption, the encryption value 'e' that we choose, falls in the range of 0 and phi(n) and it is relatively prime to phi(n). True or False?

s) If M is the message (plain text) and n is the product of 2 prime numbers, then RSA encryption will work if M > n. True or False?

t) In Message Authentication code algorithm must always be reversible. True or False?

Part B

Answer **any three out of the four** Questions. **Each** question carries **eight** marks. (3Qx8M=24)

2. Explain the Diffie-Hellman key exchange mechanism with all relevant formulas. Show mathematically, how both parties end up getting the same shared key K?

3. Using play-fair cipher, encrypt the sentence "**why, don't you?".** Use the keyword **MANGO.** Using the same keyword decrypt the text "**GLRKARTT**".

4. Bob sends a message to Alice putting his signature using ElGamal scheme, using the

following parameters. Was Alice able to verify that indeed the message was from Bob?

q = 19

α (primitive root of 19) = 2,

Xa (Bob's private key) = 3,

m = H(M) = 4 where M is the message and m is the hash of the message

K= 7 (a random integer)

5. Find the multiplicative inverse of 50 mod 71 using extended Euclidian algorithm.

Part C

Answer **any three out of the four** Questions. **Each** question carries **twelve** marks. (3Qx12M=36M)

6. Explain all the steps in Digital Signature Algorithm (DSA) with an example and diagrams. Show all the relevant formulas used in the entire algorithm. What is the assumption that supports the ...gument that it is difficult to break DSA by an intruder?

7. What is HMAC? Explain the structure of an efficient implementation of HMAC with a diagram. Describe the components of this structure in detail.

8. The following values were used as part of RSA encryption/decryption.

Encryption key (e) = 17

Φ(n) = 2668

p-1 = 46

Where n = p * q and both p and q are prime numbers.

What is the value of decryption key (d)?

What is the Public Key (e, n)?

What is the Private Key (d, n)?

Encrypt the text "2". What is the cipher text value?

Write the formula for decryption – No need to solve

9. Solve the following system of congruence using Chinese remainder theorem. Show all steps.

$$2X \equiv 5 \bmod 7$$
$$3X \equiv 4 \bmod 8$$
$$4X \equiv 3 \bmod 11$$

Roll No												

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING

SUMMER TERM / MAKE UP END TERM EXAMINATION

Semester: Summer Term 2019 **Date**: 22 July 2019

Course Code: CSE 215 **Time**: 2 Hours

Course Name: Cryptography and Network Security **Max Marks**: 80

Program & Sem : B.Tech, VI Sem (2015 Batch) **Weightage**: 40%

Instructions:

(i) ***Read all instructions carefully***

(ii) ***PART A and PART B have choices***

(iii) ***All answers to question 1 must be on same page***

Part A

I. Answer **all** the Questions. **Each** question carries **One** mark. (20Qx1M=20M)

a) An assault on system security that derives from an intelligent threat is called _____

b) Denial of Service is an example of passive attack. True or False?

c) In a Feistel structure of n-bit block length, k-bit key length, the total number of transformations is equal to _____

d) In diffusion, the statistical structure of the key is dissipated into long range statistics of the cipher-text. True or False?

e) Each S-BOX in a DES contains which of the following rows X columns.

i. 4 x 8 ii. 8 x 4 iii. 8 x 8 iv. 8 x 16

f) During the DES decryption, the round 13 uses the sub-key

i. K13 ii. K4 iii. K14 iv. K12

g) In AES encryption, during shift row transformation, the second row does the following circular shift.

i. 1 byte left ii. 1 byte right iii. 2 byte left iv. 2 byte right

h) The multiplicative inverse of 16 mod 11 is equal to _____

i) The input message size in SHA-512 algorithm is less than

i. 2^{128} ii. 2^{64} iii. 2^{32} iv. 2^{56}

j) The purpose of using cryptographic Hash functions during communication between two parties, is to ensure signature. True or False?

k) During RSA encryption and decryption, a message (plain text) M=2 was first encrypted and then decrypted to get the message back, using the following formula and values.

$$(2^7)^{343} \bmod 527 = 2 \bmod 527$$

What is the public key (e, n)? (__, __)? What is the private key(d,n)? (_,_)

l) If $(3x) \equiv (5 \bmod 8)$, what is the positive value of x?

m) If n = 91 then phi(n) = ____

n) If 7^{83} is congruent to 7 mod 83, then 7^{82} is congruent to _____

o) If multiplicative inverse of x mod 7 is 3, then x = _____?

p) The difference between Cryptographic hash functions and Message authentication codes (MAC) is that Hash functions do not use key and MAC uses key. True or False?

q) Using Fermat's little theorem, the value of $3^{201} \bmod 11$ = _____

r) In RSA algorithm, the encryption key can be used for decryption and decryption key can be used for encryption. True or False?

s) If M is the message (plain text) and n is the product of 2 prime numbers, then RSA encryption will work if M = n. True or False?

t) The difficultness of breaking Diffie-Hellman key exchange scheme by an intruder is based on the assumption that computing discrete logarithm is difficult. True or False?

Part B

Answer **any 3** Questions. **Each** question carries **ten** marks. (3Qx10M=30)

2. Explain the Diffie-Hellman key exchange mechanism with all relevant formulas. Show mathematically, how both parties end up getting the same shared key K?

3. Solve the following system of congruences using Chinese remainder theorem. Show all steps.

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod 9 \\ x &\equiv 4 \pmod{11}. \end{aligned}$$

4. Find the multiplicative inverse of 43 mod 64 using extended Euclidian algorithm.

5. What is the length of the output (in bits) produced after each of the following DES encryption scheme where plain text is of size 64 bits long and the initial key is 64 bits long.

   a) Initial permutation
   b) Permuted choice 1
   c) Permuted choice 2
   d) Round 1
   e) Inverse initial permutation
   f) Expansion permutation within a round (first step within a round)
   g) Substitution using S-Boxes within a round
   h) Permutation within a round (last step within a round)

Part C

Answer **any 2** Questions. **Each** question carries **fifteen** marks. (2Qx15M=30)

6. The following values were used as part of RSA encryption/decryption.

   Encryption key (e) = 223 $\Phi(n) = 66$ p-1 = 30

   Where n = p * q and both p and q are prime numbers.

   What is the value of decryption key (d)? Show the extended Euclidian algorithm to find the value of d.

   What is the Public Key (e, n)?

   What is the Private key (d, n)?

   Write the formula for encryption using the public key– No need to solve

   Write the formula for decryption using the private key– No need to solve

7. What is HMAC? Explain the structure of an efficient implementation of HMAC with a diagram. Describe the components of this structure in detail.

8. A binary plain text 0010 1100 was input to an encryption / decryption algorithm that follows Feistel block structure. The overall key for encryption/decryption is 0001. The sub-keys are generated by one bit circular right shift. The Feistel function F is defined as F = OR.

   Show the encryption process for the above plain text using Feistel block cipher using 3 rounds of encryption. Decrypt cipher text to get the plain text. Show all steps.