Total No. Pages: 1

Roll No .....

EIGHTH SEMESTER

B.E. (IT)

MID SEMESTER EXAMINATION, February-March-2016

IT-412: INFORMATION SECURITY

Time: 1:30 Hrs

Max. Marks: 20

Note: All questions are compulsory. Assume suitable missing data, if any.

1. [a] Find the multiplicative inverse of 23 in Z_{100} using extended Euclidean algorithm. [2]

   [b] Using quadratic residues solve the following congruences: [2]

   i. $x^2 \equiv 5 \bmod 11$

   ii. $x^2 \equiv 12 \bmod 17$

2. [a] For the group $G = <Z_{19}^*, \times>$

   i. Find the order of the group.

   ii. Find the number of primitive roots in the group.

   iii. Find the primitive roots in the group.

   iv. Show that the group is cyclic. [2]

   [b] Define information theoretically secure cryptosystem. Give an example with proof. [2]

3. [a] Show a Linear Feedback Shift Register (LFSR) with the characteristic polynomial $x^3 + x^2 + 1$. What is the period? [2]

   [b] Distinguish between passive and active attacks Name some passive attacks and active attacks. [2]

4. [a] Show how to multiply (10101) by (10000) in $GF(2^5)$. Use $(x^5 + x^2 + 1)$ as modulus. [2]

   [b] Use a Hill cipher to encipher the message "We live in an insecure world". Use the following key:

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$ [2]

5. What is double DES? What kind of attack on double DES makes it useless? [4]

Total No. of Page(s): 2

Roll No.....

EIGHTH SEMESTER **B.E. (IT)**

B.E. END SEM. EXAMINATION, May 2016

IT-412: INFORMATION SECURITY

Time: 3:00 Hours. **Max. Marks: 70**

Note: Attempt any five questions. All questions carry equal marks. Assume any missing data suitable.

1. (a) Define eight security mechanisms. Also, show the relation between security services and security mechanisms.
   (b) The plaintext "letusmeetnow" and the corresponding ciphertext "HBCDFNOPIKLB" are given. You know that the algorithm is a Hill cipher, but you don't know the size of the key. Find the key matrix.

2. (a) Define a product cipher and list two classes of product ciphers. Discuss the design of each class with two rounds.
   (b) AES defines three different cipher-key sizes (128, 192, and 256); DES defines only one cipher-key size (56).What are the advantages and disadvantages of AES over DES with respect to this difference?

3. (a) Generate the elements of the field $GF(2^3)$ using irreducible polynomial $f(x) = x^3 + x^2 + 1$.
   (b) State the Chinese Remainder Theorem. Solve the following simultaneous equations using this theorem:

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7$$

4. (a) In ElGamal cryptosystem, given the prime $p = 11$;
   i. Choose an appropriate e_1 and d, then find e_2.
   ii. Encrypt and decrypt the plaintext 7.
   (b) In elliptic curve cryptography, given $E_{67}(2, 3)$ as the elliptic curve over GF(p);
   i. Choose $e_1 = (2, 22)$ and $d = 4$, calculate e_2.
   ii. Encrypt the plaintext $P = (24, 26)$. Take $r = 2$. (Mention the formula used in each step)

166-A

5. (a) Differentiate between Modification Detection Code (MDC) and Message Authentication Code (MAC).
   (b) Using the RSA digital signature scheme, let p = 809, q = 751, and d = 23. Find the public key e. Then, sign and verify a message M = 100.

6. (a) Explain the working principle of the Kerberos protocol.
   (b) Discuss any two intrusion detection techniques.

7. Write the short notes on any two of the following:
   (a) SHA-512 cryptographic hash function
   (b) PGP
   (c) Linear and Differential cryptanalysis
   (d) Packet filters Firewall

———————x———————

Total No. Pages: 1

EIGHTH SEMESTER

Roll No .....

B.E. (IT)

MID SEMESTER EXAMINATION, March-2015

IT-412: INFORMATION SECURITY

Time: 1:30 Hrs

Max. Marks: 20

Note: All questions are compulsory. Assume suitable missing data, if any.

1. [a] Explain five security services. [2]

[b] Encrypt the message "We live in an insecure world" using the following ciphers. Ignore the space between words. Decrypt the message to get the original plaintext.

a) Vigenere cipher with key: "dollars"

b) Hill cipher with key

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$ [2]

2. Draw the general structure of DES and explain DES function in detail with diagram. [4]

3. What is cryptanalysis? Also, discuss four kinds of cryptanalysis attacks. [4]

4. Distinguish between differential and linear cryptanalysis. Which one is a chosen-plaintext attack? Which one is a known-plaintext attack? [4]

5. Alice uses Bob's RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Show how Eve can use the chosen-ciphertext attack if she has access to Bob's computer to find the plaintext. [4]

Total No. of Page(s): 2 Roll No.....

EIGHTH SEMESTER **B.E. (IT)**

B.E. END SEM. EXAMINATION, May 2015

IT-412: INFORMATION SECURITY

Time: 3:00 Hours. **Max. Marks: 70**

Note: Attempt any **five** questions. All questions carry equal marks. Assume any missing data suitable.

1. (a) Distinguish between passive and active security attack with examples. [5]
   (b) What is a monoalphabetic cipher? Explain four techniques of monoalphabetic ciphers with an example [6]
   (c) The encryption key in a transposition cipher is (3, 2, 6, 1, 5, 4). Find the decryption key. [3]

2. (a) What is double DES? What kind of attack on double DES makes it useless? [6]
   (b) In the elliptic curve E (1, 2) over the GF (11) field:
   i) Find the equation of the curve.
   ii) Find all points on the curve and plot them on a graph
   ii) Generate public and private keys for Bob [1+4+3]

3. (a) Using the Rabin cryptosystem with p=47 and q=11, encrypt p=17 to find the ciphertext. [7]
   (b) In RSA: [2+3+2]
   i) Given n = 221 and e = 5, find d.
   ii) Given p = 19, q = 23, and e = 3, find n, $\Phi(n)$, and d.
   iii) What is the problem in choosing 2 as the public key e?

4. (a) What is virus? Explain different types of viruses. [7]
   (b) Discuss the application layer firewall in detail. [7]

(161)

5. (a) Compare and contrast the attacks on digital signatures with attacks on cryptosystems [7]

(b) Using the ElGamal digital signature scheme, let p=881 and d=700. Find values of e_1 and e_2. Choose r=17.Find the value of S_1 and S_2 if M=400. [7]

6. (a) Discuss the general format of a PGP message. [7]

(b) List the main features of the SHA-512 cryptographic hash function explaining in detail the compression function used. [7]

7. Write the short notes on any two of the following:

(a) SSL

(b) Authentication protocol

(c) Kerberos

(d) AES [7+7]

----------x----------

Total No. of Page(s): 2 Roll No.....

EIGHTH SEMESTER **B.E. (IT)**

B.E. END SEM. EXAMINATION, May 2014

IT-412: INFORMATION SECURITY

Time: 3:00 Hours. **Max. Marks: 70**

Note: Attempt any **five** questions. All questions carry equal marks. Assume any missing data suitable.

1. (a) Explain different types of security mechanism in detail.
   (b) What is cryptanalysis? Explain different types of cryptanalysis attacks.

2. (a) Given the key 'GYBNQKURP', apply the Hill cipher to the plaintext 'ACT' to show how encryption and decryption are performed and prove authenticity.
   (b) Encrypt and decrypt the plaintext message 'honesty is the best' by using a 6-character key 'CENTRE' with Vigenere cipher.

3. (a) Distinguish between a Feistel and non-Feistel block cipher.
   (b) Explain key generation of DES with the help of a block diagram.

4. (a) Define Kerberos and name its servers. Briefly explain the duties of each server.
   (b) Discuss the packet-filtering router firewall in detail.

5. (a) Consider an RSA key set with p = 7, q = 11, n = 77, and e = 13. What value of d should be used in the secret key? What is the encryption and decryption of the message M = 5?
   (b) What is ElGamal Cryptosystem? Explain different types of attacks on it.

6. (a) Describe the idea of the Merkle-Damgard scheme in detail.

Total No. of Pages_____ Roll No._____

EIGHT SEMESTER **BE(IT)**

END SEM EXAMINATION MAY-2013

IT-412 INFORMATION SECURITY

Time: 3:00 Hours Max. Marks: 70

Note: Question No.1 is compulsory.
Answer any FOUR questions from the rest.
Assume suitable missing data, if any

1

a) Compute GCD of 252 and 189 by using extended Euclid's GCD algorithm.
b) How many elements have multiplicative inverses in Z_{pq} when p and q are primes?
c) What are DOS (Denial of Service) attacks?
d) Compute ϕ (n) Euler's phi function for $n = p^2q^3$ where p and q are distinct primes.
e) Use Chinese remainder theorem to solve the three simultaneous congruences

$N \equiv 3 \pmod 4$
$N \equiv 4 \pmod 5$
$N \equiv 3 \pmod 7$

f) What is factoring problem? Apply Polland's rho algorithm for n=8051.
g) Alice and Bob agree on prime number p =23 and base g=5, Alice secret integer a=6 and bob secret number b=15. Discuss Diffie Hellman protocol. [7X2]

2

a) Encrypt the message "This is an exercise" using the following ciphers. Ignore the space between the words.

i. Vignere cipher with key= "dollars "
ii. Affine cipher with key=(15,20)

b) Prove that the polynomial $F(x)= x^4 + x + 1$ is an irreducible polynomial. If yes then generate elements of the field $G(2^4)$ using the same. [2X7]

3

a) Consider elliptic curve E_{11} (1, 6), the curve is defined by $y^2 = x^3 + x + 6$ with a modulus of p=11. Determine all points in $E_{11}(1,6)$.
b) What are the different criteria for cryptographic hash functions? Distinguish between HMAC and CMAC.
c) Explain the concept of Blind Signature. [7, 5, 2]

4.

a) Discuss DSS scheme in detail. Also prove correctness of the verifying process.

b) Using RSA scheme let p=809, q=751, d=23. Calculate public key e. Then sign and verify a message M=100.

c) Discuss different attacks on RSA. |7, 3, 4|

5.

a) Differentiate between MDC and MAC.

b) How do ciphers change plaintext into numeric digits for computing?

c) What is the padding for SHA-512 if length of the message is 5120 bits? Give a broad overview of how a message digest created using SHA-512? |4, 3, 7|

6.

a) Discuss meet in middle attack and 3-DES.

b) Using the plain text and ciphertext given below, apply each of the following transformations on the plaintext to get the ciphertext in AES:

Plaintext: 00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19

Cipherkey : 24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87

a) SubBytes
b) ShiftRows
c) MixColumns
d) AddRoundKey |6, 8|

7. Write a note on (any FOUR):

a) Kerberos
b) Cycling attack
c) SSL
d) Zero knowledge proofs
e) PGP
f) Modern block ciphers |4X3.5|