U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

September / October 2022 Supplementary Examinations

Programme: B.E. **Semester: VI**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 20CS6PCCNS **Max Marks: 100**
Course: Cryptography and Network Security **Date: 28.09.2022**

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

SUPPLEMENTARY EXAMS 2022

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
Revealing of identification, appeal to evaluator will be treated as malpractice.

UNIT - I

1 a) Demonstrate with a suitable example how monoalphabetic substitution cipher is vulnerable to frequency analysis attack. **04**

b) Show the steps involved in multiplication of two polynomials: $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$ in $GF(2^8)$ using the efficient algorithm for multiplication using n-bit words. Consider $x^8 + x^4 + x^3 + x + 1$ as the irreducible polynomial. **08**

c) Given that $Z_7 = \{1, 2, 3, 4, 5, 6\}^*$ mod 7 is a group, write all the cyclic subgroups (different orders) of Z_7. Is Z_7 a cyclic group? **08**

OR

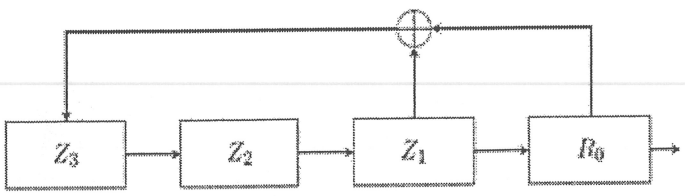
2 a) Suppose we are told that plaintext "**friday**" yields the ciphertext "**pqcfku**" where Hill cipher is used (m= 2). Find the KEY. Show all the steps clearly. **08**

b) Suppose you are told that the one time pad encryption of the message "attack at dawn" is 09e1c5f70a65ac51626bc3d25f17 (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key? **06**

c) Encrypt the message "**cryptography and network security see**" using the Affine Cipher with key (15, 20). Ignore the space between words. Decrypt the message to get the plaintext. **06**

UNIT - II

3 a) Consider the below diagram for the Linear Feedback Shift register (LFSR) **06**



i. Construct a table to produce the key stream generated using this LFSR with the key K=(1,0,1,1).What is its period?
ii. Write down the characteristic polynomial of this linear recurrence. Is it a primitive polynomial? Explain your answer.

b) Prove using mathematical induction, the equivalents observed during encryption and decryption in DES using neat diagrams. **06**

c) Explain Shift Rows operation used in AES algorithm with an example. **04**

d) Differentiate between Linear cryptanalysis and Differential cryptanalysis. Show if DES is vulnerable to Differential cryptanalysis or not. **04**

UNIT - III

4 a) Apply CRT to find an integer x which leaves a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively. **06**

b) Find the values of the following: **05**
- i. $\phi(29)$
- ii. $\phi(32)$
- iii. $\phi(80)$
- iv. $\phi(100)$
- v. $\phi(101)$

c) Apply Miller Rabin Test and check if 561 is a prime number or not. **05**

d) Apply Fermat's theorem to find the values of the following: **04**
- i. $5^{15} \bmod 13$
- ii. $15^{18} \bmod 17$

UNIT - IV

5 a) For RSA with parameters: e = 7 and n = 17*31. **10**
- i. Encrypt the message block M = 2.
- ii. Compute a private key corresponding to the given public key.
- iii. Perform the decryption of the ciphertext.
- iv. Show if low modulus attack is possible on this message with a suitable example demonstration.

b) In ElGamal cryptosystem, given the prime p = 31: **10**
- i. Choose an appropriate values for e_1 and d, then calculate e2.
- ii. Encrypt the message "HELLMAN". Use 00 to 25 for encoding. Use different blocks to make P < p.
- iii. Decrypt the ciphertext to obtain the plaintext.
- iv. Clearly show all the steps involved in encryption and decryption.

OR

6 a) In the elliptic curve $E(g^4, 1)$ over the $GF(2^4)$ field: **10**
- i. Find the equation of the curve.
- ii. Find all points on the curve and plot the points on the graph.
- iii. Generate public and private keys for Bob.

SUPPLIMENTARY EXAMS 2022

iv. Choose a point on the curve as a plaintext for Alice.
v. Create ciphertext corresponding to the plaintext in part iv for Alice.
vi. Decrypt the ciphertext for Bob to find the plaintext sent by Alice.

b) Demonstrate cycling attack on RSA cryptosystem with an example. **05**

c) Explain one-way function and trapdoor one way function with an example. **05**

UNIT - V

7 a) Using the RSA Digital Signature scheme, let p = 809, q = 751 and d = 23. Calculate the public key e. Then do the following: **10**
i. Sign and verify a message with M1 = 101 Calculate the signature S1.
ii. Sign and verify a message with M2 = 51. Calculate the signature S2.
iii. Show that if M = M1 × M2, then S = S1 × S2.

b) Explain the attacks on Digital Signature. **05**

c) Analyze how digital signature satisfy the property of non-repudiation. **05**

******

SUPPLEMENTARY EXAMS 2022