Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

Name:

Mid-Semester Examination (Aug-Dec 2024)

Course Name: Number Theory & Cryptography
Semester: 1st
Duration: 1 Hour 30 Minutes

Course Code: CS800
Course: M.Tech. (CSE-IS)
Marks: 40

Note: Answer all the questions.

Q1. (i) Given integers a and b, a number n is said to be of the form ak + b if there is an integer k such that ak + b = n. Thus the numbers of the form 3k + 1 are · · · - 8, - 5, - 2, 1, 4, 7, 10, · · · . Prove that every integer is of the form 3k or of the form 3k + 1 or of the form 3k + 2. [5]

(ii) Prove that (a, a + k) | k for all integers a, k not both zero. [5]

Q2. (i) If p is a prime and $p \mid (a^2 + b^2)$ and $p \mid (b^2 + c^2)$, then $p \mid (a^2 - c^2)$. [5]

(ii) Prove there is an infinite number of primes. [5]

Q3. (i) If (a, m) = 1, then there is an x such that $ax \equiv 1 \pmod m$. Any two such x are congruent (mod m). If (a, m) > 1, then no such x exists. [5]

(ii) Let p be a prime number. Then $x^2 \equiv 1 \pmod p$ if and only if $x \equiv \pm 1 \pmod p$. [5]

Q4. (i) Crack the following plaintext
TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB
What encryption key was used? [2]

(ii) Encrypt the message **RUN AWAY** using the ElGamal key (3137,2894,1505). [5]

(iii) In a public-key RSA system, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M? [3]

Dept. of Computer Science & Engg. aukaat dikha di saale ne.
NITK- Surathkal.

I^st Sem. M.Tech (CSE-15) Number theory & Cryptography

Surprise Test: 2.

Answer all the questions.

1. Which of the following congruences have solutions? How many?

(a) $x^2 \equiv 2 \bmod 61$ (b) $x^2 \equiv 2 \bmod 59$.

(c) $x^2 \equiv -2 \bmod 61$ (d) $x^2 \equiv -2 \bmod 59$. ✓

— 10 Marks

2. How many solutions are there to each of the congruences?

(a) $x^2 \equiv -1 \bmod 61$ (b) $x^2 \equiv -1 \bmod 59$

(c) $x^2 \equiv -1 \bmod 365$ (d) $x^2 \equiv -1 \bmod 3599$

(e) $x^2 \equiv -1 \bmod 122$.

— 10 Marks

3. Find all primes p such that $\left(\frac{10}{p}\right) = 1$. — 10 Marks

4. Find the values of $\left(\frac{p}{q}\right)$ in the nine ~~cases~~ cases obtained from all combinations of $p = 7, 11, 13$ and $q = 227, 229$ & 1009. — 10 Marks

5. Find all primes p such that $x^2 \equiv 13 \bmod p$ has a solution — 10 Marks.

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

M.Tech. (CSE-IS) Mid-Semester Examination

Odd Semester (August-December, 2022)

Course Name: Cryptography and Number Theory

Course Code: CS800

Duration: 90 minutes

Max. Marks: 50

Semester: 1st

Note: Answer all questions.

Roll No - 222IS015

Q1. Show that if a, b, and c are mutually relatively prime nonzero integers, then (a, bc) = (a, b) (a, c). [5]

Q2. Show that if a, b, and c are integers such that (a, b) = 1 and c | (a+ b), then (c, a) = (c, b) = 1. [5]

Q3. Show that if $a_1, a_2, \dots, a_n$ are integers that are not all 0 and c is a positive integer, then $(ca_1, ca_2, \dots, ca_n) = c(a_1, a_2 \dots, a_n)$. [5]

Q4. Show that if a, b, m, and n are integers such that $m > 0$, $n > 0$, $n \mid m$, and $a \equiv b \pmod m$, then $a \equiv b \pmod n$. [5]

Q5. Find the least positive residue of each of the following. [5×2]

a) 3^{10} modulo 11 b) 5^{16} modulo 17

Q6. Find all solutions of each of the following linear congruence's. [5×2]

a) $3x \equiv 2 \pmod 7$ b) $6x \equiv 3 \pmod 9$

Q7. Prove that $n^2 - 81n + 1681$ is a prime for $n = 1, 2, 3, \cdots, 80$, but not for $n = 81$. [10]

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

End-Semester Examination (November 2024)

Course Name: Number Theory & Cryptography
Semester: I[st]
Duration: 3 Hours

Course Code: CS800
Course: M.Tech. (CSE-IS)
Marks: 40

Note: Answer all the questions.

Q1. (i) Prove by using congruence that all squares of integers have remainders 0 or 1 upon dividing by 3. [5]

(ii) The set of all linear combinations of integers m and n is the set of all multiples of (m, n). [5]

Q2. (i) The following matrix was used as a key to a Hill cipher to encrypt a favorite vegetable of mine, and the resulting ciphertext was **YGFI**. What is the vegetable? [6]

$$\begin{pmatrix} 11 & 13 \\ 2 & 3 \end{pmatrix}$$

(ii) Use a rail fence cipher with three rails to encrypt the message by removing the rails from top to bottom. [5]

Q3. (i) Confusion is a fundamental concept in block ciphers: confusion aims to make the relationship between the ciphertext and key as complex as possible, usually using a complex substitution algorithm. In DES, select the component that provides the most confusion: [2]

a. Initial Permutation
b. S-Boxes
c. Expand and Permutation operation
d. Permutation of S-box outputs
e. Swapping the left and right halves
f. Exclusive OR operations

(ii) Consider ElGamal encryption with g = 7 and p=11. Bob chooses x = 4 as the private key. What is his public key? [5]

Q4. (i) RSA Algorithm: Let p = 23 and q = 29. Your encryption key e has to be at least 10 such that e is relatively prime to (p-1)*(q-1). [6]

a) Find the encryption and decryption keys.
b) Show the encryption for plaintext 18.
c) Show the decryption for ciphertext 16.

(ii) A shift cipher key is exchanged using the Diffie-Hellman method with g = 5 and p = 47. The actual numbers exchanged were X = 38 and Y = 3. Find the key. [6]

Department of Computer Science and Engineering, NITK-Surathkal
M.Tech (CSE-IS) End Semester Examination Dec 2023

Duration:3 Hrs **Max Marks: 100**
Subject: Number Theory & Cryptography **Course Code: CS 800**
Roll No:

Answer all Questions. Missing data may be suitably assumed

1. By using the Euclidean algorithm, find the greatest common divisor of 2689 and 4001. Also represent the GCD in the linear form. (5 Marks)
2. Show that if $p > 3$ is a prime, then $p^2 \equiv 1 \pmod{24}$ (5 Marks)
3. Use Pollards rho method to find a proper factor of 1313. (10 Marks)
4. Use Pollards $p-1$ method to find a proper factor p of 779, using list of primes 2, 3. (10 Marks)
5. A RSA cipher was set up with modulus 24163 and encryption exponent 13. What is the decryption exponent? (05 Marks)
6. Find all primes p such that $\left(\frac{10}{p}\right) = 1$ (10 Marks)
7. Evaluate the Jacobi Symbol (i) $\left(\frac{12125}{1211571}\right)$
   (ii) $\left(\frac{727491}{3713713}\right)$ (10 Marks)
8. Determine the number of solutions of the congruence $x^4 \equiv 61 mod 117$ (05 Marks)
9. Prove that if p is an odd prime then $x^2 \equiv 2\text{mod p}$ has solutions if and only if $p \equiv 1 or 7 \text{mod } 8$ (10 Marks)
10. Explain Shamirs (k, h) Secret sharing scheme with an example. (05 Marks)
11. For what integer n is $2n + 1/n + 7$ an integer? (05 Marks)
12. Find all primes which can be represented both as sums and as differences of two primes. (05 Marks)
13. Explain Miller-Rabim primality test with an example. (10 Marks)
14. Enplain Solovay-Strassen primality test with an example (05 Marks)

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

M.Tech. (CSE-IS) End-Semester Examination
Odd Semester (Aug-Dec, 2022)

Course Code: CS800 **Course Name:** Cryptography and Number Theory
Duration: 03 Hours **Max. Marks:** 50
Semester: 1st

Note: Answer all questions.

Q1. Solve the simultaneous congruences using Chinese Remainder Theorem. [5]

$x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$.

Q2. If P1 = (1, 3) and $P_2 = (0, 2)$ on the elliptic curve $y^2 = x^3 + 4x + 4$ modulo 5, find $P_1 + P_2$ and $P_1 + P_1$. [5]

Q3. If $n = p_1 p_2 \ldots p_h$ is a product of distinct primes, then

i) $\phi(n) = (p_1-1)(p_2-1)\ldots(p_h-1)$ [3]

ii) p_i-1 divides $\phi(n)$ for all i. [2]

Q4. Consider the following scheme by which B encrypts a message for A.

i. A chooses two large primes P and Q that are also relatively prime to $(P - 1)$ and $(Q - 1)$.
ii. A publishes $N = PQ$ as its public key.
iii. A calculates P' and Q' such that $PP' \equiv 1 \pmod{Q - 1}$ and $QQ' \equiv 1 \pmod{P - 1}$.
iv. B encrypts message M as $C = M^N \bmod N$.
v. A finds M by solving $M \equiv C^{P'} \pmod{Q}$ and $M \equiv C^{Q'} \pmod{P}$.

(a) Explain how this scheme works. [5]
(b) How does it differ from RSA? [5]
(c) Is there any particular advantage to RSA compared to this scheme? [5]

Q5. Use the following Playfair matrix and encrypt the message "*Must see you over Cadogan West. Coming at once*" [10]

25121502L

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

M.Tech. (CSE-IS) End-Semester Examination

Odd Semester (August-December, 2025)

Course Name: Cryptography and Number Theory **Course Code:** CS800

Duration: 03 Hours **Max. Marks:** 50

Semester: 1st

Note: Answer all questions.

Q1. (a) Explain why the (hexadecimel) key FEE0FEE0FEF1FEF1 would be a poor choice to encrypt a message using DES. [4]

(b) Suppose you know that using a Hill cipher with key $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ the plaintext *er* encrypts to the ciphertext *DE*, and the plaintext *re* encrypts to the ciphertext *DR*. Explain why this is not enough information for you to determine K. [3]

Q2. (a) Use the Euclidean Algorithm to find gcd (26, 14). Explain why 14 does not have a multiplicative inverse in Z_{26}. [2+2]

(b) Use the Euclidean Algorithm to find gcd (26, 23). [2]

(c) Find the multiplicative inverse of 23 in Z_{26}. [2]

Q3. (a) For all four modes of operations (ECB, CBC, OFB, CFB), analyze the effect on the decryption of remaining blocks if, for the sequence of ciphertext blocks $c_1, c_2, \ldots, c_n$, some ciphertext block c_j is erroneous, $1 \leq j < n$. That is, specify which of the plaintext blocks $x_j, x_{j+1}, x_{j+2}, \ldots, x_n$ are received incorrectly. [4]

(b) Prove that the number 31803221 is not a prime number using the following [4]

$$231803212 \equiv 27696377 \pmod{31803221}$$

Q4. Given are two protocols in which the sender's party performs the following operation:

Protocol 1:

$$y = e_{k1}(x \,||\, H(k_2 \,||\, x)),$$

where x is the message, H is a hash function such as SHA-1, e is a symmetric-key encryption algorithm, || denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver.

Protocol 2:

$$y = e_k(x \,||\, sig_{k_{pr}}(H(x))),$$

where k is a shared secret key, and k_{pr} is a private key of the sender (not shared with the receiver).

(a) Provide a step-by-step description of both protocols and explain what the receiver does upon reception of y. [3+3]

(b) State whether the following security properties can be ensured by both protocols.

(i) Confidentiality [2]

(ii) Integrity [2]

Q5. (a) Let u = 19500 and v = 11143. Use the Euclidean Algorithm to compute w = gcd(u, v). Perform the computation to determine R and S such that w = Ru + Sv. [5]

(b) Use the Chinese Remainder Theorem to find all solutions, if they exist, to the system of equivalences. [5]

$$2x \equiv 6 \pmod{14}$$
$$3x \equiv 9 \pmod{15}$$
$$5x \equiv 20 \pmod{60}$$

Q6. (a) If P1 = (1, 3) and P2 = (0, 2) on the elliptic curve $y^2 = x^3 + 4x + 4$ modulo 5, find $P_1 + P_2$ and $P_1 + P_1$. [4]

(b) Find the order of the point P = (1, 3) on the elliptic curve E: $y^2 = x^3 + 4x + 4$ modulo 5. [3]

252IS032

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

M.Tech. (CSE-IS) Mid-Semester Examination

Odd Semester (August-December, 2025)

Course Name: Cryptography and Number Theory **Course Code:** CS800

Duration: 90 minutes **Max. Marks:** 50

Semester: 1st

Note: Answer all questions.

Q1. Show that if a, b, and c are mutually relatively prime nonzero integers, then (a, bc) = (a, b) (a, c). [5]

Q2. Show that if a, b, and c are integers such that (a, b) = 1 and c | (a+b), then (c, a) = (c, b) = 1. [5]

Q3. Show that if $a_1, a_2, \ldots, a_n$ are integers that are not all 0 and c is a positive integer, then $(ca_1, ca_2, \ldots, ca_n) = c(a_1, a_2 \ldots, a_n)$. [5]

Q4. Show that if a, b, m, and n are integers such that m > 0, n > 0, n | m, and $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$. [5]

Q5. Find the least positive residue of each of the following. [5×2]

a) $3^{10} \bmod 11$ b) $5^{16} \bmod 17$

Q6. Find all solutions of each of the following linear congruences. [5×2]

a) $3x \equiv 2 \pmod{7}$ b) $6x \equiv 3 \pmod{9}$

Q7. Prove that $n^2 - 81n + 1681$ is a prime for $n = 1, 2, 3, \cdots, 80$, but not for $n = 81$. [10]
