



School of Computer Science and Engineering

Winter Semester 2023-24

Continuous Assessment Test – I

SLOT: E2 + TE2

Programme Name & Branch: B. Tech CSE

Course Name & Code: Cryptography and Network Security – BCSE309L

Class Number (s): Applicable to All

Faculty Name (s): Prof. S. Ramani

Exam Duration: 90 Min.

Maximum Marks: 50

General instruction(s):

Answer all the Questions.

Tables related to DES/AES are given in the question paper.

| Q. No. | Question | Max Marks |
|--------|--|------------|
| 1. | a) Find the greatest common divisor d of 412 and 54, and find integers x and y solving the equation $412x + 54y = d$. Ans: $d = 2$. The extended Euclidean algorithm gives $x = 8$ and $y = -61$. (There are other solutions for x and y ; these are not unique.) b) Solve the congruence $X^{103} \equiv 4 \pmod{11}$ to find the value of X using Fermat's theorem. Ans: By Fermat's Little Theorem, $x^{10} \equiv 1 \pmod{11}$. Thus, $x^{103} \equiv x^3 \pmod{11}$. So, we only need to solve $x^3 \equiv 4 \pmod{11}$. If we try all the values from $x = 1$ through $x = 10$, we find that $5^3 \equiv 4 \pmod{11}$. Thus, $x \equiv 5 \pmod{11}$. | 5 5 |
| 2. | a) Solve the given congruence equations to obtain the value of x $x \equiv 2 \pmod{5}$ $x \equiv 3 \pmod{7}$ $x \equiv 10 \pmod{11}$ Ans: $x \equiv 87 \pmod{385}$ b) Find $\phi(1200)$ Ans. 320 | 8 2 |
| 3. | a) Solve $7^{106} \pmod{143}$ using fast modular exponentiation | 5 5 |

| | | |
|----|---|-------------------|
| | <p>106 = 1101010 in binary</p> $106 = 2^1 + 2^3 + 2^5 + 2^6$ $106 = 2 + 8 + 32 + 64$ $7^{106} \bmod 143 = 7^{(2+8+32+64)} \bmod 143$ $7^{106} \bmod 143 = (7^2 \cdot 7^8 \cdot 7^{32} \cdot 7^{64}) \bmod 143$ <p>Step 2: Calculate mod C of the powers of two <= B</p> $7^1 \bmod 143 = 7 \bmod 143 = 7$ $7^2 \bmod 143 = (7^1 \cdot 7^1) \bmod 143 = (7^1 \bmod 143 \cdot 7^1 \bmod 143) \bmod 143 = (7 \cdot 7) \bmod 143 = 49 \bmod 143 = 49$ $7^4 \bmod 143 = (7^2 \cdot 7^2) \bmod 143 = (7^2 \bmod 143 \cdot 7^2 \bmod 143) \bmod 143 = (49 \cdot 49) \bmod 143 = 2401 \bmod 143 = 113$ $7^8 \bmod 143 = (7^4 \cdot 7^4) \bmod 143 = (7^4 \bmod 143 \cdot 7^4 \bmod 143) \bmod 143 = (113 \cdot 113) \bmod 143 = 12769 \bmod 143 = 42$ $7^{16} \bmod 143 = (7^8 \cdot 7^8) \bmod 143 = (7^8 \bmod 143 \cdot 7^8 \bmod 143) \bmod 143 = (42 \cdot 42) \bmod 143 = 1764 \bmod 143 = 48$ $7^{32} \bmod 143 = (7^{16} \cdot 7^{16}) \bmod 143 = (7^{16} \bmod 143 \cdot 7^{16} \bmod 143) \bmod 143 = (48 \cdot 48) \bmod 143 = 2304 \bmod 143 = 16$ $7^{64} \bmod 143 = (7^{32} \cdot 7^{32}) \bmod 143 = (7^{32} \bmod 143 \cdot 7^{32} \bmod 143) \bmod 143 = (16 \cdot 16) \bmod 143 = 256 \bmod 143 = 113$ <p>Step 3: Use modular multiplication properties to combine the calculated mod C values</p> $7^{106} \bmod 143$ $= (7^2 \cdot 7^8 \cdot 7^{32} \cdot 7^{64}) \bmod 143$ $= (7^2 \bmod 143 \cdot 7^8 \bmod 143 \cdot 7^{32} \bmod 143 \cdot 7^{64} \bmod 143) \bmod 143$ $= (49 \cdot 42 \cdot 16 \cdot 113) \bmod 143$ $= 3720864 \bmod 143$ $= 4$ $\therefore 7^{106} \bmod 143 = 4$ <p>b) Determine all integers in the set $\{1, \dots, 11\}$ that are primitive roots of modulo 11</p> <p>Ans: 2,6,7,8</p> | |
| 4. | <p>a) Differentiate Initialization vector and Nonce in Block cipher modes operations. Explain the reason that you should use block cipher CBC mode instead of block cipher ECB mode.</p> <p>An IV is a nonce with an additional requirement: it must be selected in a nonpredictable way. That is, the IV can't be sequential; it must be random. CBC has the advantage over the ECB mode in that the XORing process hides plaintext patterns. Even if the first plaintext block and third plaintext block were the exact same segment of plaintext, it is highly unlikely that the first ciphertext block and third ciphertext block would be the same.</p> | <p>3</p> <p>7</p> |

| | | |
|----|---|----|
| | <p>b) Discuss primitive operations and key expansion procedure in IDEA and also Explain the steps involved in one round of IDEA to encrypt the plain text.</p> <ul style="list-style-type: none"> Each rounds makes use of 6 subkeys ($8 \times 6 = 48$) and the final output transformation uses four subkeys ($48 + 4 = 52$ subkeys). 128-bit key is divided into 8 parts K1 to K8 each of 16 bits. Of which K1 to K6 is used for ROUND 1 operation. For the remaining round subkeys are generated by performing key shifting. The original key is shifted left circularly by 25 bits and hence 52 subkeys are generated. Operations performed are Addition, Multiplication, XOR <p>Each round involves a series of operation on the four data blocks using six keys.</p> <ol style="list-style-type: none"> Multiply P1 and K1 i.e, $S1 = P1 \times K1$ Add P2 and K2 i.e, $S2 = P2 + K2$ Add P3 and K3 i.e, $S3 = P3 + K3$ Multiply P4 and K4 i.e, $S4 = P4 \times K4$ XOR step 1 and step 3 i.e, $S5 = S1 \oplus S3$ XOR step 2 and step 4 i.e, $S6 = S2 \oplus S4$ Multiply step 5 with K5 i.e, $S7 = S5 \times K5$ Add step 6 and step 7 i.e, $S8 = S6 + S7$ Multiply step 8 with K6 i.e, $S9 = S8 \times K6$ Add step 7 and step 9 i.e, $S10 = S7 + S9$ XOR step 1 and step 9 i.e, $S11 = S1 \oplus S9$ XOR step 3 and step 9 i.e, $S12 = S3 \oplus S9$ XOR step 2 and step 10 i.e, $S13 = S2 \oplus S10$ XOR step 4 and step 10 i.e, $S14 = S4 \oplus S10$ | |
| 5. | <p>A person wants to share a plaintext "123456ABCD132536" to his friend in the opposite side through social network. He/she uses Data Encryption Standard (DES) algorithm for session encryption during his communication and assume that he/she uses, the key as "AABB 0918 2736 CCDD". Show the key generated for the first two rounds.</p> <p>Parity Drop Table</p> | 10 |

| | | | | | | | |
|----|----|----|----|----|----|----|----|
| 57 | 49 | 41 | 33 | 25 | 17 | 09 | 01 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 02 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 03 |
| 60 | 52 | 44 | 36 | 63 | 55 | 47 | 39 |
| 31 | 23 | 15 | 07 | 62 | 54 | 46 | 38 |
| 30 | 22 | 14 | 06 | 61 | 53 | 45 | 37 |
| 29 | 21 | 13 | 05 | 28 | 20 | 12 | 04 |

Compression Box Table

| | | | | | | | |
|----|----|----|----|----|----|----|----|
| 14 | 17 | 11 | 24 | 01 | 05 | 03 | 28 |
| 15 | 06 | 21 | 10 | 23 | 19 | 12 | 04 |
| 26 | 08 | 16 | 07 | 27 | 20 | 13 | 02 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

Key in Hexa to Binary

AABB 0918 2736 CCDD

1010 1010 1011 1011 0000 1001 0001 1000 0010 0111 0011 0110 1100 1100
1101 1101

Key 1: 000110010100110011010000011100101101111010001100

Key 2: 010001010110100001011000000110101011110011001110

PAJAMA PADHAI