Student Answer Script View

MIT MPL-BTech-M Sc - MCA - 1st-3rd-5th and 7th Semester - Mid Term Examination - Sep 2024

Answer Sheet

Student Name:	TEJESWAR POKURI . .
Roll Number:	220905236
Course:	Computer Science
Year/Sem:	Semester 5
Subject Name:	PRINCIPLES OF CRYPTOGRAPHY
Exam Date:	23-Sep-2024

24.00
30.00

Comments submitted by student.

Q.No : 1) **Score : 0.50 / 0.50**

Akshay sends a message 'hi' to Akash at 6pm. However, when Akshay and Akash meet in real at 8pm, Akshay denies that he had sent the message to Akash. Make use of the described scenario, the attacker and the security goal being breached are respectively:

Akshay, Authentication | Akash, Accountability, | Akshay, Accountability | Akash, Authentication

Q.No : 2) **Score : 0.50 / 0.50**

If x = remainder obtained by dividing 7^{886} by 300, then evaluate the value of x

x = 7 | x = 49 | x = 1 | x = 343

Q.No : 3) **Score : 0.00 / 0.50**

For a 7-bit to 7-bit Substitution Block Cipher (Ideal Block Cipher), select how many sets of transformations are possible from Plaintext Blocks to Ciphertext Blocks?

128! 7! 128 None of These

Q.No : 4) **Score : 0.50 / 0.50**

If x = Order of 44 (mod 19), then evaluate the value of x

x = 9 | x = 25 | x = 4 | x = 1

Q.No : 5) **Score : 0.50 / 0.50**

If GCD (651, 168) = 651*x+168*y (x, y ∈ Z), then (x, y)=

(4,-1) (-1,4) (-4,1) None of These

Q.No : 6) **Score : 0.00 / 0.50**

Which among the following Statements is True?

- 11 is a primitive root of 18
- 49 doesn't have any primitive root
- 4 is primitive root of 16
- 7 is a primitive root of 9

Q.No : 7) **Score : 0.00 / 0.50**

Choose the plaintext corresponding to the ciphertext '**QJDFFOFWRHDQTSPY**' using Vigenere Cipher which uses only alphabets as the character set (by ignoring the case, and mapping with their default numerical equivalents) with the key '**MODULO**' is

EVALUATIONSRIGHT | EVALUATIONSDONE | EVALUATIONMARKS | None of These

Q.No : 8) **Score : 0.00 / 0.50**

Select the minimum length of the key required to define all possible 5-bit to 5-bit mappings in an ideal block cipher:

32 Bits | 20 Bytes | 5! Bits | 5! Bytes

Q.No : 9) **Score : 0.50 / 0.50**

Which of the security mechanisms defined by X.800 is sufficient to counter any passive attack?

Notarization | Authentication Exchange | Traffic Padding | Digital Signature

Q.No : 10) **Score : 0.00 / 0.50**

A Plaintext '**HI**' has been encrypted to a Ciphertext '**EE**' with a key '**SOFTWARE**' using Vigenere Cipher (Assume that only alphabets by ignoring the case has been used for encryption). If the attacker captures the Ciphertext and has a knowledge that Vigenere Cipher has been used for encryption, compute the maximum number of keys he/she would have to try for a successful Brute Force Attack.

26^8 8^{26} 26 676

Q.No : 11) **Score : 2.00 / 2.00**

Explain the following security services defined by X.800 for data storages and data communications:- (a) Data Origin Authentication, (b) Access Control, (c) Non-Repudiation, (d) Peer Entity Authentication.

Page:1

Security services :- These are the services that are implemented to enhance the communication security and and obtain security goals

(a) Data Origin Authentication

This service is used to check the data packets coming from the legimate entity, this helps us to understand if source is real entity

Ex:- Gmail uses this to validate the source of the email is legimate or not.

(b) Access Control

This method is implemented for Confidentiality

This method is used
so that users can have restricted access
Ex:- restricted access control, they can access
the resources that they are allowed to

(c) Non-Repudiation
This method takes the accountability of the
senders for a communication
Ex:- Digital Signature

(d) Peer Entity Authentication
we authenticate between 2 peers to avoid
replaying.

Q.No : 12)	Score : 0.00 / 2.00
List and explain any 4 design features to be considered in Feistel Cipher.	

Page:1

12

Block is 64 bit

Then

Q.No : 13) **Score : 2.00 / 2.00**

Calculate Multiplicative Inverse of $(x^3 + 1)$ mod $(x^4 + x + 1)$ in $GF(2^4)$ by applying Extended Euclidean Algorithm (EEA) for Polynomials. (Show Long Division steps for all the iterations while calculating the quotients and remainders).

Page:1

MI (x^3+1) mod (x^4+x+1) in $GF2^4$

Iter-i	$q(x)$	a	b	$r(x)$	$v1(x)$	$v2(x)$	$v(x)$
		x^4+x+1	x^3+1	1	0	1	x
	x	x^3+1	1				

$$x^3+1 \overline{)\, x^4+x+1 \;(\, x}$$
$$x^4 + x$$
$$+1 \quad +1$$
$$1$$

$r(x) = 1$

$q(x) = x$

$v(x) = v1(x) - q(x)(v2(x))$

$= 0 - 1(x)$

$= -x$

following GF rules $\Rightarrow v(x) = x$

So,

q(x)	a	b	r	v1(x)	v2(x)	v(x)
x^3+1	x^3+1	1	0	1	x	x+1

$$
\begin{array}{r|l}
 & x^3+1 \\
\hline
1 & x^3+1 \\
 & x^3 \downarrow \\
\hline
 & 1 \\
 & -1 \\
\hline
 & 0
\end{array}
$$

$q(x) = x^3+1$

$r(x) = 0$

So, $v(x) = v_1(x) - q \times v_2(x)$

$1 - x(x^3+1) = -x^4$

Page:2

13

by following GF rules $v(x) = x^4$

mod with x^4+x+1

$$v(x) = x^4 \bmod (x^4+x+1)$$

$$x^4+x+1 \;\overline{)\;1}$$

$$x^4$$

$$-x^4-x-1$$

$$-x-1 \text{ in GF} \rightarrow x+1$$

So,

Ite-3

q(x)	a	b	r(x)	v1(x)	v2(x)	v(x)
-	1	0	-	x	x+1	-

Hence MI (x^3+1) in $GF(2^4)$ is x

Q.No : 14) **Score : 3.00 / 3.00**

Assume that Feistel Cipher uses 16 rounds. The output of the **14th** Round during Encryption is **0xAB**; **K_{15} = 0xD, K_{16} = 0xE**. The round function **F(x,y) = XOR(1-bit circular left shift of x, 1-bit circular right shift of y)**, where y is the Round Key (K_i). Evaluate the value of Ciphertext (CT).

Page:1 14

Given that,

Output for 14^{th} round $= 0xAB$

So, $LD_{14} = 0xA = (1010)_2$

$RD_{14} = 0xB = (1011)_2$

$K_{15} = 0xD = (1101)_2$

$K_{16} = 0xE = (1110)_2$

15^{th} Round

$LD_{15} = RD_{14} = (1011)_2$

$RD_{15} = LD_{14} \oplus F(RD_{14}, K_{15})$

$= LD_{14} \oplus ((1011)_2 \oplus (1110)_2)$

$= (1010)_2 \oplus (1001)_2$

$= (0011)_2$

Output for 15th round = 10110011 = 0xB3

16th round

$LD_{16} = RD_{15} = (0011)_2$

$RD_{16} = LD_{15} \oplus F(RD_{15}, K_{16})$

$= (1011)_2 \oplus ((0110)_2 \oplus (0111)_2)$

$= (1011)_2 \oplus (0001)_2$

$= (1010)_2$

Page:2

14

So, output of 16th round is 0x3A

So, Final Cipher text is 0x~~A~~3

Q.No : 15) **Score : 3.00 / 3.00**

Calculate Multiplicative Inverse of $(x^4 + 1)$ mod $(x^5 + x^2 + 1)$ in $GF(2^5)$ by applying Extended Euclidean Algorithm (EEA) for Polynomials. (Show Long Division steps for all the iterations while calculating the quotients and remainders).

Page:1 15

MI (x^4+1) mod (x^5+x^2+1)

Iteration ①

	$q(x)$	a	b	$r(x)$	$U_1(x)$	$U_2(x)$	$U(x)$
					0	1	x

$$x^4+1 \overline{)\, x^5+x^2+1 \,\big|\, x}$$

$$x^5 + x$$

$$+1 \qquad +1$$

$$x^2 - x + 1$$

$r(x) = x^2+x+1$

$q(x) = x$

in GF(2^5)

$= x^2+x+1$

$V(x) = U_1(x) - q\,U_2(x)$

$= 0 - x(1) = -1$ in GF(2^5)

$= x$

In ②

q(x)	a	b	r(x)	u1(x)	u2(x)	u(x)
x^2+x	x^4+1	x^2+x+1	$x+1$	1	x	x^3+x^2+1

$$x^2+x$$
$$x^2+x+1 \;\overline{)\; x^4+1}$$
$$x^4+x^3+x^2 \quad (+1, +1, +1)$$
$$-x^3-x^2+1 \quad \text{in GF}(2^5)$$
$$+1 \quad x^3+x^2+1$$
$$x^3+x^2+x \quad (+1, +1, +1)$$
$$1$$

$r(x) = x+1$

$q(x) = x^2+x$

Page:2

$1-x$ in $GF(2^5)$

$\Rightarrow x+1$

$V(x) = U1(x) - U2(x)q$

$= 1 - x(x^2+x)$

$= x^3+x^2+1$ ($\because$ in $GF(2^5)$)

In ③

q(x)	a	b	r(x)	$U_1(x)$	U2(x)	U(x)
					x^3+x^2+1	x^4+x^3
x	x^2+x+1	$x+1$	1	x		

$$x+1 \overline{)\, x^2+x+1 \,\big(\, x}$$

x^2+x

1

$q(x) = x$

$r(x) = 1$

$V(x) = V1(x) - q\,V2(x)$

$= x - x(x^3+x^2+1)$

$= x - x^4 - x^3 - x \quad = x^4 + x^3$ ($\because$ GF(2))

In (4)

q(x)	a	b	r(x)	U1(x)	U2(x)	U(x)
				x^3+x^2+1	x^4+x^3	0
$x+1$	$x+1$	1	0			

$$
\begin{array}{r|l}
 & x+1 \\
\hline
1 & x+1 \\
 & -x \\
\hline
 & 1 \\
 & -1 \\
\hline
 & 0
\end{array}
$$

$r(x) = 0$

$q(x) = x+1$

Page:3

$$V(x) = V_1(x) - q\,V_2(x)$$
$$= x^3 + x^2 + 1 - (x+1)(x^4 + x^3)$$
$$= x^3 + x^2 + 1 - x^5 - x^4 + x^4 + x^3$$
$$= x^5 + x^2 + 1 \quad (\because \text{in } GF(2^5))$$

Since it is same as the degree of irreducible polynomial

$$V(x) = x^5 + x^2 + 1 \bmod (x^5 + x^2 + 1) = 0$$

In ⑤

$q(x)$	a	b	$r(x)$	$V_1(x)$	$V_2(x)$	$V(x)$
–	1	0	–	$x^4 + x^3$	0	–

Hence MI is $x^4 + x^3$

Q.No : 16) **Score : 3.00 / 3.00**

When x (x ∈N) is divided by **32** and **55**, the remainders obtained are **7** and **14** respectively. Apply Chinese Remainder Theorem (CRT) to write the corresponding Linear Congruence equations and evaluate the value of x.

Page:1

Given that
Based on above information

$x \equiv 7 \pmod{32}$

$x \equiv 14 \pmod{55}$

so, $a_1 = 7$; $a_2 = 14$; $m_1 = 32$, $m_2 = 55$

$M = \sum m_i$

$M = 32 \times 55 = 1760$

$m_1 = 55$; $m_2 = 32$

$N_1 = MI(m_1) \bmod (m_1)$

$= MI(55) \bmod (32)$

q	a	b	r	v_1	v_2	v
0	32	55	32	0	1	0
1	55	32	23	1	0	1
1	32	23	9	0	1	-1
2	23	9	5	1	-1	3
1	9	5	4	-1	3	-4
1	5	4	1	3	-4	7
4	4	1	0	-4	7	-32
-	1	0	-	7	-32	-

Page:2

16

So, $N_1 = 7$

$N_2 = MI(M_2) \bmod (m_2)$

$= MI(32) \bmod (55)$

q	a	b	r	v1	v2	v
	55	32	23	0	1	-1
1	32	23	9	1	-1	2
1	23	9	5	-1	2	-5
2	9	5	4	2	-5	7
1	5	4	1	-5	7	-12
1	4	1	0	7	-12	-55
4						

$-10 - (-12)$

So, $MI = -12 \bmod (55) = 43$

So, $N_2 = 43$

$x = (a_1 M_1 N_1 + a_2 M_2 N_2) \bmod (n)$

$= (7 \times 55 \times 7 + 43 \times 14 \times 32) \bmod (1760)$

$= 21959 \bmod (1760)$

$= 839$

Q.No : 17) **Score : 3.00 / 3.00**

A Plaintext (PT) was encrypted using Triple-Stage Columnar Transposition Cipher with the key '**ENDSEM**'(Using only alphabets by ignoring the case and by using the padding '**X**' if necessary). The Ciphertext (CT) corresponding to the PT is '**TTOTESYIIHUXDRERITXSSMXM**'. Evaluate PT by discarding the padding '**X**' (if any, after final stage decryption).

Page:1

Given that
Triple stage Columnar
CT:- TTOTESYIIHUXDRERITXSSMXM

key:- ENDSEM

no. of rows = len(CT)/len(key)
= 24/6 = 4

ENDSEM so, order => 2 5 1 6 3 4
2 5 1 6 3 4

①	②	③	④	⑤	⑥
E	I	T	S	I	D
S	T	T	M	H	R

Stage-1

Y	X	O	X	U	E
I	S	T	M	X	R

So, First stage output :-

EITSIDSTTMHRYXOXUE

ITSTMXR

Stage-2

ENDSEM so, order => 2 5 1 6 3 4

2 5 1 6 3 4

Page:2

①	②	③	④	⑤	⑥
I	U	E	T	T	Y
D	E	I	M	M	X
S	T	T	X	M	O
T	S	S	R	R	X

Output after Stage-2

IUETTYDEIMMXSITXMOT

SSRRX

Stage-3

ENDSEM so, order => 2 5 1 6 3 4

2 5 1 6 3 4

① ② ③ ④ ⑤ ⑥

T	M	I	S	I	S
Y	O	U	R	M	I
O	T	E	R	M	T
E	S	T	X	X	X

So,
Encopted Text is

THIS IS YOUR MIDTERM TESTXXX
Ignore

So, final answer is
This is your midtermtest

Q.No : 18)	**Score : 3.00 / 3.00**

State and Prove Fermat's Theorem for prime numbers. Apply Fermat's Theorem to calculate the remainder obtained when $\mathbf{48^{783}}$ is divided by **79** .

Fermat's Theorem

This theorem states that, any positive integer power p-1, where p is an prime number, then it's remainder when divided by p is 1

$$a^{p-1} \pmod p \equiv 1$$

p = prime

since p is prime

GCD(p, a) = 1

proof :-

Assume a set of integers less than p like $X = \{1, 2, 3 \ldots, p-1\}$, now multiply with a mod p to all elements of x, it becomes $H = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$

in the new set of H, there are some

Conditions to be checked

(i) All numbers are below p
This is true because, mod p will always give less than p

(ii) There is no zero
This true because, since p is prime any multiplication can't generate p. So, none of the elements is zero

(iii) All elements are unique
Let us assume they are not unique, let these

be $aj \pmod p \equiv ak$

$\Rightarrow j \pmod p \equiv k$ (∵ since a & p are co primes)

This can't be possible as X has all unique values and $j, k \in X$

So, we can say that X & H have same elements but in a different orders.

So, if we multiply all and take mod p, it should be same

$\Rightarrow ((a \bmod p)(2a \bmod p) \ldots ((p-1) \bmod p)) \equiv$

$(1 \times 2 \times 3 \times \ldots p-1) \bmod p$

$\Rightarrow (a^{p-1} \times (p-1)!) \equiv (p-1)! \bmod p$

as $(p-1)!$ is co prime to p, we can cancel on both sides

$\therefore a^{p-1} \equiv 1 \pmod{p}$

hence Fermat's theorem is proved

To find :- $48^{783} \bmod 79$

79 is prime

so, $48^{78} \bmod 79 = 1$

Page:3

18

$$So, 48^{780} \bmod 79 \Rightarrow (48^{78})^{10} \bmod 79 = 1$$

$$So, 48^{783} = (48^{780} \times 48^3) \bmod 79$$

$$= 1 \times 48^3 \bmod 79$$

$$= 71$$

Q.No : 19) **Score : 2.00 / 4.00**

A Plaintext (PT) was encrypted using Hill Cipher with a Key Matrix (K) as displayed in Figure 1. The character set consists of only alphabets by ignoring the case (the alphabets are mapped with their default numerical equivalents). The Ciphertext (CT) corresponding to the PT is '**CPSAPOQLNZIU**'. Calculate the Inverse Key Matrix (K^{-1} mod 26). Also, Calculate the Plaintext (PT).

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Figure 1:- Key Matrix (K) for Hill Cipher

Page:1

19

$$Key = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

$$CT :- \begin{bmatrix} C & P & S \\ A & P & O \\ O & L & N \\ Z & I & U \end{bmatrix} = \begin{bmatrix} 2 & 15 & 18 \\ 0 & 15 & 14 \\ 16 & 11 & 13 \\ 25 & 8 & 20 \end{bmatrix}$$

Calculating K^{-1}

Det of $K = 441$

$$K^{-1} = \begin{bmatrix} 70 & -343 & 226 \\ 5 & 70 & -47 \\ -99 & 378 & -245 \end{bmatrix} \quad 441^{-1} \pmod{26}$$

$m_2(44\ 1) \bmod 26$

q	a	b	r	v_1	v_2	v
16	44	26	25	0	1	-16
1	26	25	1	1	-16	17
25	25	1	0	-16	17	-441
-	1	0	-	17	-441	0

Page:2

19

So,

$$\begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -26 \end{bmatrix} \times 17 \pmod{26}$$

$$= \begin{bmatrix} 20 & 23 & 12 \\ 7 & 20 & 9 \\ 7 & 4 & 20 \end{bmatrix} = K^{-1}$$

So, now, $CT \times K^{-1}$

So, $CT \times K^{-1} = \begin{bmatrix} 11 & 2 & 21 \\ 21 & 18 & 21 \\ 20 & 16 & 9 \\ 20 & 9 & 2 \end{bmatrix}$