MATH 233 Introduction to Cryptography

Midterm Exam

Mar 6, 2024

Name: ANSWER

UR ID: _____

Instructions for the midterm you will be taking:

- The presence of calculators, cell phones, and other electronic devices at this exam is strictly forbidden. Notes or texts of any kind are strictly forbidden. If you have questions, get the attention of your exam proctor; otherwise no communication is allowed during the exam.
- Show your work! You may not receive full credit for a correct answer if insufficient work or insufficient justification is given. For any question asks to find an integer (or an integer mod n), your final answer should be a single integer without any (modular) addition, multiplication, exponentiation, etc.
- The exam is 1 hour, 15 minutes and is worth 100 points.

COPY THE HONOR PLEDGE AND SIGN (Cursive is not required)

I affirm that I will not give or receive any unauthorized help on this exam, and all work will be my own.

_____

_____

_____

YOUR SIGNATURE: _____

QUESTION	VALUE	SCORE
1	20	
2	15	
3	15	
4	20	
5	20	
6	10	
TOTAL	100	

1. (20 pts) Encrypt the plaintext

asolareclipse

using each method, using the tables below. The plaintext and table (if applicable) will be given on each page for convenience.

a/A	b/B	c/C	d/D	e/E	f/F	g/G	h/H	i/I	j/J	k/K	l/L	m/M
0	1	2	3	4	5	6	7	8	9	10	11	12
n/N	o/O	p/P	q/Q	r/R	s/S	t/T	u/U	v/V	w/W	x/X	y/Y	z/Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(a) Shift cipher with encryption key $-5 \pmod{26}$.

0 18 14 11 0 17 4 2 11 8 15 18 4

$-5 \to$ 21 13 9 6 21 12 25 23 6 3 10 13 25

Answer: V N J G V M Z X G D K N Z

(b) Vigenère cipher with keyword 'total'. $\longrightarrow$ (19, 14, 19, 0, 11)

0 18 14 11 0 17 4 2 11 8 15 ~~X~~ 18 4

+ 19 14 19 0 11 19 14 19 0 11 19 14 19

$\equiv$ 19 6 7 11 11 10 18 21 11 19 8 ~~X~~ 6 23

Answer: T G H L L K S V L T I ~~X~~ G X

(c) Playfair cipher with the following matrix. Use z as a filler if needed.

r	o	c	h	e
s	t	a	b	d
f	g	i	k	l
m	n	p	q	u
v	w	x	y	z

`plaintext: asolareclipse`

as → BT
ol → EG
ar → SC
ec → RH
li → FK
ps → MA
ez → DE

Answer: BT EG SC RH FK MA DE

(d) Hill cipher with the following matrix (mod 26). Use z as a filler if needed.

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ -1 & -1 & 0 \end{pmatrix}$$

plaintext: asolareclipse

a/A	b/B	c/C	d/D	e/E	f/F	g/G	h/H	i/I	j/J	k/K	l/L	m/M
0	1	2	3	4	5	6	7	8	9	10	11	12
n/N	o/O	p/P	q/Q	r/R	s/S	t/T	u/U	v/V	w/W	x/X	y/Y	z/Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$(0 \quad 18 \quad 4)\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ -1 & -1 & 0 \end{pmatrix} \equiv (12 \quad 4 \quad 18)$$

$$(11 \quad 0 \quad 17)\begin{pmatrix} \cdot\cdot & & \end{pmatrix} \equiv (20 \quad 24 \quad 0)$$

$$(4 \quad 2 \quad 11)\begin{pmatrix} \cdot\cdot & & \end{pmatrix} \equiv (19 \quad 13 \quad 2)$$

$$(8 \quad 15 \quad 18)\begin{pmatrix} \cdot\cdot & & \end{pmatrix} \equiv (16 \quad 15 \quad 15)$$

$$(4 \quad 25 \quad 25)\begin{pmatrix} \cdot\cdot & & \end{pmatrix} \equiv (5 \quad 22 \quad 25)$$

Answer: MESUYATNCQPPFWZ

2. (15 pts) A secret organization communicates by the one-time pad (OTP) with different encryption keys at each time (the keys are distributed in a different secure channel). The messages (plaintexts) are composed of 7-bit blocks of ASCII codes corresponding to uppercase letters, digits, and space, summarized below.

	0	1	2	3	4	5	6	7
0110	000	001	010	011	100	101	110	111
	8	9						
0111	000	001						
		A	*B*	*C*	*D*	*E*	*F*	*G*
1000		001	010	011	100	101	110	111
	H	*I*	*J*	*K*	*L*	*M*	*N*	*O*
1001	000	001	010	011	100	101	110	111
	P	*Q*	*R*	*S*	*T*	*U*	*V*	*W*
1010	000	001	010	011	100	101	110	111
	X		*Y*		*Z*		space	
	1011000		1011001		1011010		0100000	

At one moment, the organization becomes unable to securely distribute the encryption key. Therefore, they decide to keep using the last key which was distributed securely. You realize this fact, and you also figure out that any message always begins with the blocks corresponding to the following form.

(three-letter location) (two-digit number)

(Note that there is also a space between letters and digits.) The three-letter location, indicating the branch sending the message, is one of the followings:

BOS, CHI, DAL, DET, HOU, LAX, NYC, PHL, ROC, SFO, SJC.

The two-digit number, known to be one of $01, 02, \ldots, 29$, includes a very important information about the message. Suppose that you intercept two ciphertexts which begin with

0011010 0011010 1110010 1110110 1100100 0010001

and

0011010 0011110 1101010 1110110 1100100 0010001,

respectively.

(a) Determine the locations of two messages, regardless of the order. If it is impossible, explain why.

$C_1 \oplus C_2 =$ 0000000 0000100 0011000 ...

↓

First letters are the same

⇒ SFO & SJC or DAL & DET.

A ⊕ E = 0000100

L ⊕ T = 0011000 ✓

F ⊕ J = 0001100

O ⊕ C = 0001100

Answer: DAL & DET

(b) Determine the numbers of two messages, regardless of the order. If it is impossible, explain why.

$C_1 \oplus C_2 =$ ... 0000000 0000000

The numbers are the same, but we don't know what they are (they can be any of 01, ..., 29)

Answer: Not determined.

3. (15 pts) Let

$$n = 2^{32} + 1 = 4,294,967,297.$$

(a) Compute the value of Jacobi symbol

$$\left(\frac{3}{n}\right).$$

(*Hint.* Quadratic reciprocity law)

$n \equiv (-1)^{32} + 1 \equiv 2 \pmod 3.$

$n \equiv 1 \pmod 4$

$\Rightarrow \left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$ (QRL)

$= \left(\frac{2}{3}\right)$ $(n \equiv 2 \pmod 3)$

$= -1$ (3 : prime, $x^2 \equiv 2 \pmod 3$ has no soln)

Answer: -1

(b) Using the fact that

$$3^{2^{16}} \equiv 2,259,349,256 \pmod n.$$

show that n is a composite number. Completely justify your answer.

$\gcd(3, n) = \gcd(3, 2) = 1$, $3^{\frac{n-1}{2}} \equiv 3^{2^{16}} \not\equiv -1 \equiv \left(\frac{3}{n}\right) \pmod n$

Answer: $\Rightarrow n$: composite by Solovay-Strassen test.

4. (20 pts) Consider an RSA cryptosystem using $N = 143$ and $e = 17$.

(a) Encrypt a message $m = 10$. (*Hint.* $143 \cdot 7 = 1001$.)

$\rightarrow 10^3 \equiv -1 \pmod N$

$$C \equiv m^e \equiv 10^{17} \equiv (10^3)^5 \cdot 10^2 \equiv (-1)^5 10^2 \equiv -100 \equiv 43 \pmod N$$

Answer: 43

(b) Using the prime factorization $N = 11 \cdot 13$, determine the decryption exponent d and decrypt a ciphertext $c = 100$.

$\phi(N) = (11-1)(13-1) = 120$

$d \equiv e^{-1} \pmod{120}$.

$120 - 17 \cdot 7 = 1 \Rightarrow d \equiv -7 \equiv 113 \pmod{120}$.

$$M \equiv C^d \equiv (10^2)^{113} \equiv 10^{226} \equiv (10^3)^{75} \cdot 10 \equiv (-1)^{75} \cdot 10 \equiv -10 \equiv 133 \pmod N$$

Answer: $d = 113$. $M = 133$.

5. (20 pts) Let $p = 809$ be a prime number. Note that

$$p - 1 = 808 = 2^3 \cdot 101,$$

where 101 is a prime number. Below is the table of some powers of 2 and 3 mod p.

n		8	100	138	272	404	446	450	504	807
2^n	(mod p)	256	650	529	46	1	18	288	A	B
3^n	(mod p)	89	619	2	40	808	350	35	C	D

(a) Determine the values of A, B, C, D.

$A \equiv 2^{504} \equiv 2^{100} \cdot 2^{404} \equiv 650 \cdot 1 \equiv 650$

$C \equiv 3^{504} \equiv 3^{100} \cdot 3^{404} \equiv 619 \cdot (-1) \equiv -619 \equiv 190$

$B \equiv 2^{807} \equiv 2^{-1} \quad (2^{808} \equiv 1)$

$\equiv 405 \quad (2 \cdot 405 = 809 + 1)$

$D \equiv 3^{807} \equiv 3^{-1} \quad (3^{808} \equiv 1)$

$\equiv 270 \quad (3 \cdot 270 = 809 + 1)$

Answer: $(A, B, C, D) = (650, 405, 190, 270)$

(b) Based on the given values, determine whether 2 and/or 3 is a primitive root mod p. Briefly describe the reason for each.

2 is a primitive root mod p: YES / (NO)

Reason: $2^{404} \equiv 1$, so $\text{ord}_p(2) \neq p-1$.

3 is a primitive root mod p: (YES) / NO

Reason: $3^{404} \cdot 3^8 \neq 1 \Rightarrow \text{ord}_p(3) = p-1$.

(c) Based on the given values, determine $L_3(7)$. If it does not exist, explain why.

Exists. because 3 is a PR

$L_3(2) \equiv 138$

$L_3(40) \equiv 3L_3(2) + L_3(5) \equiv 272$

$40 = 2^3 \cdot 5$

$\Rightarrow L_3(5) \equiv 272 - 3 \cdot 138$
$\equiv -142 \equiv 666 \pmod{808}$

$L_3(35) \equiv L_3(5) + L_3(7) \equiv 450$ $\longrightarrow$ $L_3(7) \equiv 450 + 142 \equiv 592 \pmod{808}$

Answer: 592

6. (10 pts) Alice and Bob are using the ElGamal cryptosystem with $p = 29$ and $a = 2$. Bob chooses a secret key $b = 5$ and published $\beta \equiv a^b \equiv 3 \pmod{p}$. Alice sent Bob a ciphertext $(r, t) = (13, 2)$. Decrypt the ciphertext to find Alice's plaintext m. You may use the following table.

n	1	2	3	4	5	6	7	8	9
$13^n \pmod{29}$	13	24	22	25	6	20	28	16	5

$m \equiv t \cdot r^{-b} \equiv 2 \cdot 13^{-5} \pmod{p}$.

$\equiv 2 \cdot (13^5)^{-1}$

$\equiv 2 \cdot 6^{-1}$.

$\equiv 2 \cdot 5 \equiv 10$

$6 \cdot 5 = 29 + 1$.

Answer: 10

THIS PAGE INTENTIONALLY LEFT BLANK. Do not tear this page off. You may use this page if you run out of space. Make sure to label your solution(s) on this page and also include a note on the problem page(s) telling the grader(s) to look for your work here.