

Fall 2019 CIS 3362 Exam #1: Classical Cryptographic Schemes Solutions

Date: 9/23/2026

1) (8 pts) The ciphertext "XIRTVWLC" was encrypted via the shift cipher using an encryption key of 17. What is the corresponding plaintext?

$$\begin{array}{cccccccc} X & I & R & T & V & W & L & C \\ 23 & 8 & 17 & 19 & 21 & 22 & 11 & 2 \\ - & 17 & 17 & 17 & 17 & 17 & 17 & 17 \\ \hline & 6 & -9 & 0 & 2 & 4 & 5 & -6 & -15 & \text{--> mod 26} \\ & 6 & 17 & 0 & 2 & 4 & 5 & 20 & 11 & \\ \hline G & R & A & C & E & F & U & L \end{array}$$

GRACEFUL (Grading: 1 pt per letter no exceptions.)

2) (2 pts) What is the index of coincidence of the set of letters in the ciphertext from question #1? **Please answer as a fraction in lowest terms.** (This can be solved with almost no work.)

Note: Index of coincidence by definition is the probability that two objects chosen from a multiset are the same. Since no letter appears more than once in the given ciphertext, the probability that two randomly selected letters are the same (when selecting out of the 8 letters in the ciphertext) is 0.

0/1 (Grading: all or nothing, an answer of 0 is also acceptable.)

3) (6 pts) The encryption keys for an Affine Cipher are $a = 17$ and $b = 5$, what are the corresponding decryption keys. (Note: Please use the formula sheet to reduce the amount of manual computation as necessary.)

Swap x and y in the affine function:

$$x \equiv (17y + 5)(\text{mod } 26)$$

Grading: 1 pt

$$17y \equiv (x - 5)(\text{mod } 26)$$

Grading: 1 pt

On the reference sheet, we see that $17^{-1} \equiv 23 (\text{mod } 26)$, multiply the equation through by 23

$$23(17y) \equiv 23(x - 5)(\text{mod } 26)$$

Grading: 1 pt

$$y \equiv 23x - 115 (\text{mod } 26)$$

Grading: 1 pt

$$y \equiv 23x + 15 (\text{mod } 26)$$

It follows that the corresponding decryption keys are $a = 23$ and $b = 15$, respectively.

$$a = \underline{23} \quad b = \underline{15}$$

Grading: 2 pts, 1 for each answer.

4) (10 pts) Determine the value of $83^{-1} \pmod{177}$ via the Extended Euclidean Algorithm. (Note: 1 pt for the correct answer, 9 points for the work using the steps shown in class.)

$$177 = 2 \times 83 + 11$$

$$83 = 7 \times 11 + 6$$

$$11 = 1 \times 6 + 5$$

$$6 = 1 \times 5 + 1$$

Grading Euclidean: 2 pts

$$6 - 1 \times 5 = 1$$

$$6 - 1(11 - 6) = 1$$

$$6 - 1 \times 11 + 1 \times 6 = 1$$

$$2 \times 6 - 1 \times 11 = 1$$

$$2(83 - 7 \times 11) - 1 \times 11 = 1$$

$$2 \times 83 - 14 \times 11 - 1 \times 11 = 1$$

$$2 \times 83 - 15 \times 11 = 1$$

$$2 \times 83 - 15(177 - 2 \times 83) = 1$$

$$2 \times 83 - 15 \times 177 + 30 \times 83 = 1$$

$$32 \times 83 - 15 \times 177 = 1$$

Grading: 1 pt

Grading: 1 pt

Grading: 1 pt

Grading: 2 pts

Take this equation mod 177 to obtain

$$32 \times 83 - 15 \times 177 \equiv 1 \pmod{177}$$

$$32 \times 83 - 15 \times 0 \equiv 1 \pmod{177}$$

$$32 \times 83 \equiv 1 \pmod{177}$$

Grading: 1 pt

Grading: 1 pt

It follows that $83^{-1} \equiv 32 \pmod{177}$

Grading: 1 pt

32

5) (10 pts) The ciphertext "DNSKTXVYJVZVISBNLOZX" was encrypted via the Vigenere Cipher with the keyword "KNIGHTS". What is the corresponding plaintext?

D	N	S	K	T	X	V	Y	J	V	Z	V	I	S	B	N	L	O	Z	X
3	13	18	10	19	23	21	24	9	21	25	21	8	18	1	13	11	14	25	23
K	N	I	G	H	T	S	K	N	I	G	H	T	S	K	N	I	G	H	T
-10	13	8	6	7	19	18	10	13	8	6	7	19	18	10	13	8	6	7	19

-7	0	10	4	12	4	3	14	-4	13	19	14	-11	0	-9	0	3	8	18	4
19								22				15	17						
T	A	K	E	M	E	D	O	W	N	T	O	P	A	R	A	D	I	S	E

Take me down to paradise

Grading: 10 pts if correct, 4 pts if added instead of subtracted, if used the correct process but made arithmetic errors, take 1 point off per each pair of wrong letters. (1 pt for 1 or 2 letters, 2 pts off for 2 or 3 letters, etc.)

6) (8 pts) The set X contains 10 As, 20 Bs, 50 Cs and 20 Ds. The set Y contains 30 As, 5 Bs, 10 Cs and 5 Ds. What is the mutual index of coincidence between the set X and the set Y. Please express your answer as a fraction in lowest terms.

Note that $10 + 20 + 50 + 20 = 100$ and $30 + 5 + 10 + 5 = 50$. The mutual index of coincidence between the sets is:

$$\frac{10 \times 30 + 20 \times 5 + 50 \times 10 + 20 \times 5}{100 \times 50} = \frac{300 + 100 + 500 + 100}{5000} = \frac{1000}{5000} = \frac{1}{5}$$

Grading: 2 pts original numerator, 2 pts original denominator, 2 pts to get to 1000/5000 or any other fraction that isn't in lowest terms, 2 pts to reduce to get to 1/5.

7) (10 pts) Use the Hill cipher with the key $\begin{pmatrix} 11 & 4 \\ 7 & 5 \end{pmatrix}$ to encrypt the plaintext "HORSESHOES".

Note: HORSESHOES converted to numbers is 7, 14, 17, 18, 4, 18, 7, 14, 4, 18. Also note that $17 \equiv -9 \pmod{26}$ and $18 \equiv -8 \pmod{26}$

$$\begin{pmatrix} 11 & 4 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 11 \times 7 + 4 \times 14 \\ 7 \times 7 + 5 \times 14 \end{pmatrix} \equiv \begin{pmatrix} -1 + 56 \\ -3 + 70 \end{pmatrix} \equiv \begin{pmatrix} 55 \\ 67 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 15 \end{pmatrix} \rightarrow DP$$

$$\begin{pmatrix} 11 & 4 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} -9 \\ 18 \end{pmatrix} = \begin{pmatrix} 11 \times (-9) + 4 \times 18 \\ 7 \times (-9) + 5 \times 18 \end{pmatrix} \equiv \begin{pmatrix} -99 + 72 \\ -63 + 90 \end{pmatrix} \equiv \begin{pmatrix} -27 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 25 \\ 1 \end{pmatrix} \rightarrow ZB$$

$$\begin{pmatrix} 11 & 4 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 11 \times 4 + 4 \times 18 \\ 7 \times 4 + 5 \times 18 \end{pmatrix} \equiv \begin{pmatrix} 44 + 72 \\ 28 + 90 \end{pmatrix} \equiv \begin{pmatrix} 116 \\ 118 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 14 \end{pmatrix} \rightarrow MO$$

Notice that the last two pairs are the same as previously computed pairs, so the final encryption is

DPZBMODPMO

Grading: 3 pts total for setting up each of the 3 products (so 1 pt each)

3 pts total to expand out each of the sum of products

3 pts total to simplify each of those expressions down to 3, 14, 25, 1, 12, 14

1 pt total to convert the numbers to letters

If there's a tiny error and it's mostly correct, just take off 1 pt.

8) (4 pts) In every Enigma message, the day code was used to encrypt several characters.

(a) (2 pts) How many characters of every message were encrypted with the day code?

6 (Grading: 2 pts all or nothing)

(b) (2 pts) What characters were encrypted in each message with the day code?

The six characters encrypted by the day code were the three letter message code, followed by the same three letter message code. (Grading: 1 pt for stating the message code, 1 pt for stating it's send twice.)

9) (10 pts) Decrypt the following ciphertext, which was created via column transposition with the keyword "VIGENERE". A grid is provided to help you out. **Note: There are 70 characters total (so you don't have to count); you need this information to decrypt.**

A T I W I I E D E T F W R E T H N S E I S T S E N D W S S E T H
S A K T E E H F C A E C S O T O M S W I N H T A S S H E G I B M
T O U C R I

V	I	G	E	N	E	R	E
7	4	3	0	5	1	6	2
I	T	W	A	S	T	H	E
B	E	S	T	O	F	T	I
M	E	S	I	T	W	A	S
T	H	E	W	O	R	S	T
O	F	T	I	M	E	S	S
U	C	H	I	S	T	H	E
C	A	S	E	W	H	E	N
R	E	A	D	I	N	G	D
I	C	K	E	N	S		

$70/8 = 8$ and $70\%8 = 6$, this means that the columns for R and E will contain 8 letters and all of the other columns will contain 9 letters. Copy the letters in order and write them vertical, down the column labeled 0, then 1, etc.

It was the best of times, it was the worst of times. Such is the case when reading Dickens =)

Grading: 10 pts if correct message only, 3 pts for correct numeric labels of columns, 3 pts if contiguous letters from the ciphertext are copied in columns, 2 more points if the column lengths are all either 8 or 9.

10) (6 pts) The Navajo Code Talkers used one of three strategies to encrypt each word in a message, in a preferential order. (If possible, strategy #1 was used. If not, then strategy #2 was used. If not, then strategy #3 was used.) List each of the three strategies in the order that they were applied.

1. If a Navajo word exists for the term, just use it.
2. If there is no Navajo word, then see if the word belongs to one of the memorized code words (this list eventually grew to about 700 words)
3. If there's no Navajo word, AND the word isn't on the list of memorized code words, then use the letter by letter codes and spell out the word.

Grading: 2 pts each, must get the first to get points for the second, must get both of the first two to get the third.

11) (1 pts) What type of sweet treat can you buy at Night Owl Cookies? **Cookies (Give to all)**