

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN-MADISON
Math/CS/E C E 435 — Midterm Exam I — Spring 2026 — Solutions

NAME: (as it appears on Canvas)

EMAIL: @wisc.edu

PROFESSOR: MIKHAIL IVANOV

INSTRUCTIONS

- Time: **90 minutes**.
- This exam paper contains 10 pages.
- Please write your name on every page.
- No Calculators, No Notecards, No Notes
- With the exception of the True/False questions, Multiple Choice questions, and Short Answer questions you must justify your claims and use complete sentences in proofs.
- You must use correct notation to receive full credit.
- For multiple choice questions with answers listed by $\bigcirc$, choose one answer and completely fill the circle.
- Letters A, B, Z are represented by $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$ as usual.

Alphabet mapping

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Modular arithmetic

Number a has a multiplicative inverse modulo n (i.e $a \in \mathbb{Z}_N^*$) if and only if $\gcd(a, N) = 1$.

Shift cipher

$P = C = K = \mathbb{Z}_N$, encryption: $e_k(x) = x + k \bmod N$, decryption: $d_k(y) = y - k \bmod N$.

Affine cipher

$P = C = \mathbb{Z}_N$, $K = \mathbb{Z}_N^* \times \mathbb{Z}_N$, $k = (a, b)$, encryption: $e_k(x) = ax + b \bmod N$, decryption: $d_k(y) = a^{-1}(y - b) \bmod N$.

Monoalphabetic substitution cipher

$P = C = \mathbb{Z}_N$, $K = \Sigma_N$, $k = \sigma \in K$ is a permutation of the alphabet, encryption: $e_\sigma(x) = \sigma(x)$, decryption: $d_\sigma(y) = \sigma^{-1}(y)$.

Vigenère cipher

$P = C = K = \mathbb{Z}_N^n$, encryption: $e_k(x)_i = x_i + k_i \bmod N$, decryption: $d_k(y)_i = y_i - k_i \bmod N$.

Hill cipher

$P = C = \mathbb{Z}_N^n$, key space consists of invertible $n \times n$ matrices with coefficients from $\mathbb{Z}_N$, i.e. matrices K such that $\gcd(\det(K), N) = 1$, encryption: $e_K(X) = KX$, decryption: $e_{K(Y)} = K^{-1}X$.

Frequencies of letters of English language

E	T	A	O	I	N	S	R	H	L	D	C	U
12.51	9.25	8.04	7.60	7.26	7.09	6.54	6.12	5.49	4.14	3.99	3.06	2.71
M	F	P	G	W	Y	B	V	K	X	J	Q	Z
2.53	2.30	2.00	1.96	1.92	1.73	1.54	0.99	0.67	0.19	0.16	0.11	0.09

Cryptanalytic attack types:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack

Problem 1. (10 points) Answer Only

1) One-time pads are inconvenient because the keys can never be reused and need to be at least as long as the plaintext.

☐ TRUE

☐ FALSE

Solution: TRUE

2) For encryption to be IND-CPA secure, it must be deterministic.

☐ TRUE

☐ FALSE

Solution: FALSE

3) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is a valid key for the Hill cipher.

☐ TRUE

☐ FALSE

Solution: FALSE

4) Letters in the key for Vigenère cipher should be distinct.

☐ TRUE

☐ FALSE

Solution: FALSE

5) Never a one software random number generator can replace true random number sequence.

☐ TRUE

☐ FALSE

Solution: TRUE

Problem 2. (8 points) Consider a variant of the Vigenere cipher where instead of a word or short phrase, the key instead consists of a book or some other English language text that is much longer than the message to be encrypted. Now assume that Bob is a sleeper agent and Alice is his handler. Alice, using this cipher, has sent Bob a ciphertext that reads

ZSFGSJVTSPSNZYCRVC.

The plaintext is known to contain the day of the week that Bob is supposed to receive the dead drop, followed by the day of the week he is supposed to flee the country. Determine which plaintext Alice sent to Bob, and explain how you reached your answer.

Weekdays: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.

Solution: Length of the ciphertext is 17, so we need two words with 17 symbols total. It means its $9 + 8$, so one word is Wednesday and another is Thursday or Saturday. Total 4 possibilities. There are different ways to test them, one is to find position of Wednesday first:

Ciphertext:	25	18	5	6	18	9	21	19	15	18	13	25	24	2	17	21	2
Wednesday:	22	4	3	13	4	18	3	0	24								
Key:	3	14	2	19	14	19	18	19	17								
Key word:	d	o	c	t	o	r	s	t	r								

Or

Ciphertext:	25	18	5	6	18	9	21	19	15	18	13	25	24	2	17	21	2
Wednesday:									22	4	3	13	4	18	3	0	24
Key:									19	14	10	12	20	10	14	21	4
Key word:									t	o	k	m	u	k	o	v	e

First one looks good. Now second part can be Thursday or Saturday:

Ciphertext:	25	18	5	6	18	9	21	19	15	18	13	25	24	2	17	21	2
Thursday:										19	7	20	17	18	3	0	24
Key:										25	6	5	7	10	14	21	4
Key word:										z	g	f	h	k	o	v	e

Or

Ciphertext:	25	18	5	6	18	9	21	19	15	18	13	25	24	2	17	21	2
Saturday:										18	0	19	20	17	3	0	24
Key:										0	13	6	4	11	14	21	4
Key word:										a	n	g	e	l	o	v	e

Answer is clear, plaintext is WednesdaySaturday.

Another approach is to check possible positions for “day”.

Problem 3. (8 points) Determine all keystreams generated by LFSR with characteristic polynomial

$$x^4 + x^2 + 1.$$

Note that the sum of periods of all sequences generated by each of the LFSRs should add up to $2^4 - 1$.

Solution: We have LFSR of degree 4 with $c_0 = c_2 = 1$, $c_1 = c_3 = 0$. We can feed it with 0001:

$$\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}$$

We have a sequence with period 6: (0, 0, 0, 1, 0, 1). Now let's find a state, which we didn't have yet to obtain a new sequence, for example 0011:

$$\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \end{array}$$

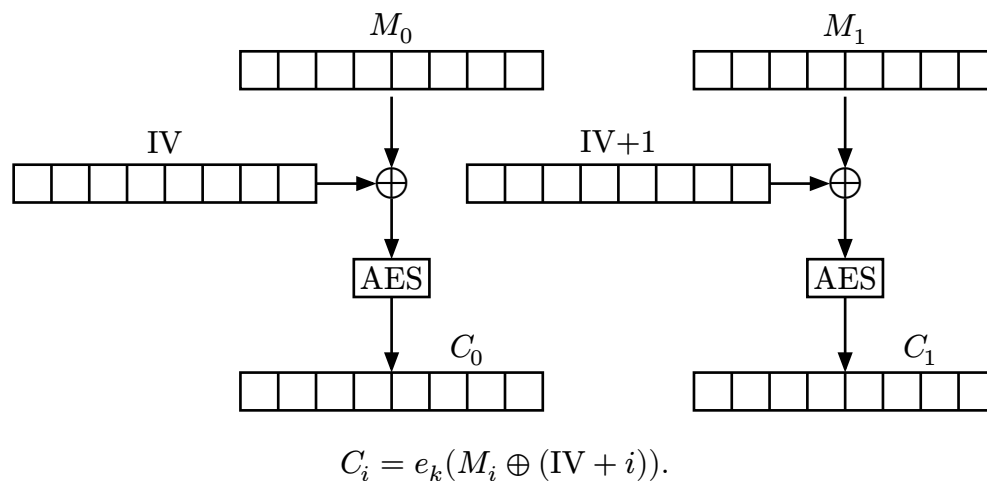
We have a sequence with period 6: (0, 0, 1, 1, 1, 1). Now let's find a state, which we didn't have yet to obtain a new sequence, for example 0110:

$$\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \end{array}$$

We have a sequence with period 3: (0, 1, 1). Totally sum of periods 15, so we cover all possible states of the LFSR (except 0000).

Problem 4. (10 points) Consider the following 128 bits encryption scheme. To encrypt message $M = (M_0, M_1, \dots)$

- Alice generate random 128 bits IV (“initial value”) and make it public.
- Alice compute $M_0 \oplus \text{IV}$ (**XOR of two 128 bits strings**) and encrypt is using AES-128 (good cipher, you can’t break it).
- Increase IV by 1.
- Compute $M_1 \oplus \text{IV}$.
- Encrypt it.
- Increase IV by 1
- etc.



- 1) Can you see the difference from HW3 problem?
- 2) Write down correct decryption formula for the given scheme.

Solution:

$$M_i = d_k(C_i) \oplus (\text{IV} + i)$$

You want to devise a strategy to win the IND-CPA game. First, the adversary (that’s you!) sends two different challenge messages, $M \neq M'$, to the challenger. For your strategy, you can assume M and M' are each **two blocks** long. Then, the challenger randomly encrypts either M or M' . The resulting two-block ciphertext $C = (C_0, C_1)$ is returned to you. Finally, you guess whether M or M' was encrypted. In this strategy, the query phase is not needed (i.e. you never have to ask the challenger to encrypt messages of your choosing beforehand).

- 3) What value should you pick for M and M' ?

Solution: For example $M = (1, 0)$, $M' = (0, 0)$.

- 4) Explain how you would determine whether M or M' was encrypted. Your answer can use these values:
 $M = (M_0, M_1)$, $M' = (M'_0, M'_1)$, $C = (C_0, C_1)$.

Solution:

$$C_0 = C_1 \implies M$$

$$C_0 \neq C_1 \implies M'$$

(there are another possible strategies)

- 5) What is the probability (excluding negligible factors) that an optimal attacker (i.e. using the correct answer to previous question) wins the IND-CPA game? Justify your answer.

Solution: For the strategy in the previous part: If $IV \equiv 0 \pmod{2}$ then $M_0 \oplus IV = M_1 \oplus (IV + 1)$, so $C_0 = C_1$. If $M'_0 = M'_1$ then $M'_0 \oplus IV \neq M'_1 \oplus (IV + 1)$, so $C_0 \neq C_1$. Totally, our strategy gives us:

	M_0	M_1
IV even	$C_0 = C_1$, win	$C_0 \neq C_1$, win
IV odd	$C_0 \neq C_1$, lose	$C_0 \neq C_1$, win

As result $P(\text{Attackew wins}) = \frac{3}{4}$.

Problem 5. (6 points) At first glance it seems as though an exhaustive key search is possible against an One Time Pad system. Given is a short message, let's say 5 ASCII characters represented by 40 bit, which was encrypted using a 40-bit One Time Pad. Explain exactly why an exhaustive key search will not succeed even though sufficient computational resources are available. This is a paradox since we know that the One Time Pad is unconditionally secure. That is, explain why a brute-force attack does not work.

Note: You have to resolve the paradox! That means answers such as “The One Time Pad is unconditionally secure and therefore a brute-force attack does not work” are not valid.

Solution: To brute force one time pad we will apply all 2^{40} keys, i.e. all 5-characters sequences. After XORing we will have all possible plaintexts, i.e all 2^{40} bit strings, i.e. all 5-characters sequences, including all possible “meaningful” 5 characters messages. We don't have any information, which one is the correct plaintext.

Problem 6. (8 points) Suppose Alice starts with a plaintext message and encrypts it using a shift cipher with a shift of k letters. Since she is just learning about cryptography at the moment, she explores what happens when she encrypts the encrypted ciphertext, using the same shift of k . She does this repeatedly, and eventually she finds that she has decrypted the message. In terms of k , how many times did Alice have to encrypt the message before it became decrypted? (You may assume that the message is in English this time, so that the alphabet has 26 letters. Your answer should cover all possible k .)

Solution:

If Alice did encryption n times. we will have

$$e_k(e_k(\dots e_k(x))) \equiv x + nk \pmod{26}.$$

Result is original text, so $x + nk \equiv x \pmod{26} \implies nk \equiv 0 \pmod{26}$, so nk is the smallest number divisible by 26.

Now we can just do cases depends on common divisors of 26 and k .

$k \pmod{26}$	1	3	5	7	9	11	15	17	19	21	23	25	2	4	6	8	10	12	14	16	18	20	22	24	13	0
n							26													13					2	1

There are formulas for n too:

$$n = \frac{26}{\gcd(26, k)} = \frac{\text{lcm}(26, k)}{k}.$$

Problem 7. (10 points) Answer briefly but carefully.

1) What is known plaintext attack?

Solution: The known-plaintext attack is an attack model for cryptanalysis where the attacker has access to both the plaintext and its ciphertext. The goal is to decrypt more ciphertext without the correct key or recover key itself.

2) Suppose we have the known plaintext attack on Hill cipher of dimension 2. Plaintext is in English language written usual way modulo 26. How long message needed to have positive probability of successful attack for the key. Is it always enough?

Solution: Key is a 2 by 2 matrix, $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$, it contain 4 parameters, so we need as minimum as 4 equations, i.e. 2 blocks. Now suppose we have plaintext (p_1, p_2, p_3, p_4) and corresponding ciphertext (c_1, c_2, c_3, c_4) with

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}, \quad \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} p_3 \\ p_4 \end{pmatrix} = \begin{pmatrix} c_3 \\ c_4 \end{pmatrix} \implies \begin{cases} p_1x + p_2y = c_1 \\ p_3x + p_4y = c_3 \end{cases} \quad \begin{cases} p_1z + p_2t = c_2 \\ p_3z + p_4t = c_4 \end{cases}$$

$$\implies \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c_1 \\ c_3 \end{pmatrix}, \quad \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} c_2 \\ c_4 \end{pmatrix}$$

so, if matrix $\begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}$ is invertible, we can recover the key.

In reality, matrix may not be invertible, for example $p_1 = p_2 = p_3 = p_4$ [probability of random matrix from $\mathbb{Z}_{26}$ be invertible is $756/2197$], so we 4 letters is not enough.