

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN-MADISON
Math/CS/E C E 435 — Midterm Exam II — 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.

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

Cipher Block Chaining mode (CBC)

$y_0 = IV$, $y_n = e_k(x_n \oplus y_{n-1})$ for $n \geq 1$.

Counter Mode (CTR)

$y_n = e_k(IV \parallel n) \oplus x_n$, for $n \geq 0$

Problem 1. (8 points) Answer Only

1) Plain RSA encryption without padding is IND-CPA secure.

- ☐ TRUE
☐ FALSE

Solution: FALSE

2) To communicate confidentially through insecure channel, Alice and Bob can use the Diffie–Hellman protocol to exchange RSA public keys that they then use for public key encryption.

- ☐ TRUE
☐ FALSE

Solution: FALSE

3) Modern stream ciphers produce 1 bit of key stream per CPU cycle.

- ☐ TRUE
☐ FALSE

Solution: FALSE

4) Meet-in-the-middle attack decrease time compare to brute-force, but increase required memory.

- ☐ TRUE
☐ FALSE

Solution: TRUE

Problem 2 (8 points) Answer Only

1) Alice and Bob use the Diffie–Hellman key exchange to derive a shared secret g^{ab} . After each session, they erase both their private exponents (a, b) and the derived value g^{ab} before starting a new session. Does this provide *forward secrecy*, i.e. can Oscar decrypt old messages if at some moment he learns the current values of g , a and b ?

- ☐ Yes, because forward secrecy concerns the ability to predict future session keys after the compromise, not before.
- ☐ Yes, because a compromise of future secrets would not reveal past session keys, as they were derived from discarded temporary secrets.
- ☐ No, because the attacker can perform a man-in-the-middle attack during the initial exchange, which retroactively breaks forward secrecy.
- ☐ No, because if the public parameters g and p are ever revealed, all past sessions become insecure.

Solution: Second

2) In a message encrypted with CBC mode, ciphertext block C_5 is corrupted, but C_6 and C_7 are received intact. Will the corresponding plaintext block P_7 be decrypted correctly?

- ☐ Yes, because the decryption of P_7 does not depend on the corrupted C_5
- ☐ Yes, because P_7 is only dependent on C_7 and the original IV.
- ☐ No, because the “chaining” in CBC mode means an error in one block corrupts all subsequent plaintext blocks.
- ☐ No, because decrypting P_7 requires a correctly decrypted P_6 , which is impossible since C_5 was corrupted.

Solution: First

Problem 3. (8 points) Determine the state graph of non-linear Feedback Shift Register with

$$n = 3, \quad F(x_2, x_1, x_0) = x_2 + x_1 x_0.$$

Solution:

$$\begin{array}{c} (0, 1, 0) \rightarrow (0, 0, 1) \rightarrow (0, 0, 0) \curvearrowright \\ (1, 0, 0) \rightarrow (1, 1, 0) \rightarrow (1, 1, 1) \rightarrow (0, 1, 1) \rightarrow (1, 0, 1) \rightarrow (1, 1, 0) \rightarrow \dots \\ \underbrace{\hspace{10em}}_{\text{cycle}} \end{array}$$

Problem 4. (6 points) Compute $(X^2 + 1) \cdot (X^3 + X^2 + 1)$ in $\text{GF}(2^4)$ using the irreducible polynomial $f(x) = X^4 + X + 1$.

Solution:

$$\begin{aligned}(X^2 + 1)(X^3 + X^2 + 1) &= X^5 + X^4 + X^3 + 2X^2 + 1 \equiv_{\text{mod } 2} X^5 + X^4 + X^3 + 1 \\ &\stackrel{X^4 = X+1}{=} X(X+1) + (X+1) + X^3 + 1 = X^3 + X^2 + 2X + 2 \equiv_{\text{mod } 2} X^3 + X^2.\end{aligned}$$

Problem 5. (6 points) Feistel cipher is a primitive taking double length block (L, R) and function f as

$$\begin{cases} L' = R \\ R' = L + f(R). \end{cases}$$

Everything is modulo 2, $+$ is XOR.

Let $\text{Feistel}_{f_1, f_2}$ denote a two-round Feistel network using functions f_1 and f_2 (in that order).

Define $\text{swap}(L, R) = (R, L)$.

Show that if

$$(L_2, R_2) = \text{swap}(\text{Feistel}_{f_1, f_2}(L_0, R_0))$$

then

$$(L_0, R_0) = \text{swap}(\text{Feistel}_{f_2, f_1}(L_2, R_2)).$$

Solution:

$$\begin{pmatrix} L_0 \\ R_0 \end{pmatrix} \xrightarrow{f_1} \begin{pmatrix} R_0 \\ L_0 + f_1(R_0) \end{pmatrix} \xrightarrow{f_2} \begin{pmatrix} L_0 + f_1(R_0) \\ R_0 + f_2(\text{first item}) \end{pmatrix} \xrightarrow{\text{swap}} \begin{pmatrix} R_0 + f_2(\text{second item}) \\ L_0 + f_1(R_0) \end{pmatrix} = \begin{pmatrix} L_2 \\ R_2 \end{pmatrix}$$

so

$$\begin{cases} L_2 = R_0 + f_2(R_2) \\ R_2 = L_0 + f_1(R_0). \end{cases}$$

Let's rewrite it (we do computations modulo 2)

$$\begin{cases} R_0 = L_2 + f_2(R_2) \\ L_0 = R_2 + f_1(R_0). \end{cases}$$

This is exactly previous formulas with $0 \leftrightarrow 2$ in L and R and $1 \leftrightarrow 2$ in f .

Solution:

$$\text{Feistel}_f(X, Y) = (Y, X + f(Y)) = (X_1, Y_1),$$

so

$$\begin{cases} Y = X_1 \\ X = Y_1 + f(Y) = Y_1 + f(X_1) \end{cases} \implies (X, Y) = \text{swap}(\text{Feistel}_f(\text{swap}(X_1, Y_1)))$$

Now we just apply it twice.

Problem 6. (6 points) Alice and Bob set up RSA systems with the same modulus N , but different encryption exponents a, b respectively. Suppose that a and b are coprime. Charles sends them each the same message m ($1 < m < N$). Show that if Eve intercepts both of Charles' transmissions, then she can compute m .

[Hint: Extended Euclidean algorithm produces integers u, v such that $ua + vb = 1$.]

Solution: Eve intercepts $c_1 = m^a \bmod N$ and $c_2 = m^b \bmod N$ and she can compute $u, v \in \mathbb{Z}$ such that $ua + vb = 1$. Now she compute

$$c_1^u \cdot c_2^v \equiv m^{au+bv} = m^1 = m.$$

Problem 7. (8 points)

Suppose Alice and Bob use Diffie–Hellman key exchange with $p = 13$ and $g = 2$. They exchange public keys 3 and 5. Find their shared secret key.

Solution: We know both public keys, $A = 2^a = 3$ and $B = 2^b = 5$. Let's find one private key.

$$2^0 = 1 \bmod 13$$

$$2^1 = 2 \bmod 13$$

$$2^2 = 4 \bmod 13$$

$$2^3 = 8 \bmod 13$$

$$2^4 = 16 = 3 \bmod 13,$$

so $a = 4$ and $k_{AB} = B^a = 5^4 = 25^2 = (-1)^2 = 1 \bmod 13$.

Solution: We know both public keys, $A = 2^a = 3$ and $B = 2^b = 5$. Let's find both private key.

$$2^0 = 1 \bmod 13$$

$$2^1 = 2 \bmod 13$$

$$2^2 = 4 \bmod 13$$

$$2^3 = 8 \bmod 13$$

$$2^4 = 16 = 3 \bmod 13$$

$$2^5 = 16 = 6 \bmod 13$$

$$2^6 = 16 = 12 \bmod 13$$

$$2^7 = 16 = 11 \bmod 13$$

$$2^8 = 16 = 9 \bmod 13$$

$$2^9 = 16 = 5 \bmod 13$$

$$2^{10} = 16 = 10 \bmod 13$$

$$2^{11} = 16 = 7 \bmod 13$$

$$2^{12} = 16 = 1 \bmod 13$$

so $a = 4$, $b = 9$, and $k_{AB} = 2^{ab} = 2^{36} = (2^{12})^3 = (1)^3 = 1 \bmod 13$.

Problem 8. (10 points) Design Man-in-the-Middle attack for the case when Alice and Bob use RSA system. Suppose they can request other's public keys from trusted server (open channel, no encryption), but Oscar can intercept traffic and replace some part of it.

Solution: We do not assume school book RSA here.

Alice requests Bob's public key B_{pub} from trusted server.

Oscar generates new public, private RSA keys O_{pub} and O_{pr} and replace Bob's public key with O_{pub}

Alice receives " B_{pub} " = O_{pub} (after Oscar change). Now she can send messages to Bob.

Similarly with Bob.

From here on, Oscar has much control over the encrypted traffic between Alice and Bob. As an example, here is how he can read encrypted messages in a way that goes unnoticed by Alice and Bob:

Alice wants to send message m . She computes $y = \text{RSA}_{O_{pub}}(m)$

Oscar intercept y , decrypt $m = \text{RSA}_{O_{pr}}(y)$, re-encrypt $y' = \text{RSA}_{B_{pub}}(m)$, send y' to Bob.

Bob decrypt $x = \text{RSA}_{B_{pr}}(y')$.