Department of Mathematics, University of Wisconsin-Madison

# Math 435 — Final Exam — Solutions — Spring 2024

NAME : (as it appears on Canvas)

EMAIL: @wisc.edu

PROFESSOR: MIKHAIL IVANOV

**INSTRUCTIONS:**

Time: **120 minutes**

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 ○, choose one answer and completely fill the circle.

For multiple choice questions with answers listed by □, choose all of the answers that you believe are correct and completely fill each square.

| Question: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Points: | 8 | 4 | 9 | 12 | 6 | 8 | 4 | 4 | 6 | 10 | 10 | 81 |

# Historic Ciphers

## Shift Cipher

$P = C = K = \mathbb{Z}_N$, $e_k(x) = x + k \bmod N$.

## Affine Cipher

$P = C = \mathbb{Z}_N$, $K = \mathbb{Z}_N^* \times \mathbb{Z}_N$, $e_k(x) = (ax + b) \bmod N$.

## General Substitution Cipher

$P = C = \mathbb{Z}_N$, $K = \Sigma_N$, $e_k(x) = \sigma(x)$.

## Vigenère Cipher

$P = C = K\mathbb{Z}_N^n$, $e_k(x_1, x_2, x_n) = (x_1 + k_1, x_2 + k_2, \ldots, x_n + k_n) \bmod N$.

## Hill Cipher

$P = C = \mathbb{Z}_N^n$, The key space consists of invertible $n \times n$ matrices $M$ with entries in $\mathbb{Z}_N$. $e_k(x) = Mx$.

## Letters $\longleftrightarrow$ Numbers

| 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 |

## 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 |

## Analysis of English text

$$H(\{p_i\}) = \sum_{i=1}^{n} -p_i \log(p_i), \qquad R = \log N - H, \qquad r = 1 - \frac{H}{\log N}$$

## Key Equivocation

$$E_n = H(P_n) + H(K) - H(C_n)$$

1. Are the following statements true or false?

   (a) (2 points) Elliptic curve cryptography uses a form of Diffie–Hellman key exchange.

   ● **True**<br>
   ○ False

   (b) (2 points) Hill ciphers acting on blocks of length two have perfect secrecy.

   ○ True<br>
   ● **False**

   (c) (2 points) A cryptographic hash function must be a 1-to-1 function, i.e. send different inputs to different outputs.

   ○ True<br>
   ● **False**

   (d) (2 points) In $\mathbb{Z}_{15}$, there are exactly two square roots of 1.

   ○ True<br>
   ● **False**

2. Let $p$ be a large prime and $g$ be a generator of $\mathbb{Z}_p^*$. Suppose we are considering the function $h : \mathbb{Z} \to \mathbb{Z}_p^*$ for use as a hash function for messages $m \in \mathbb{Z}$, where $h(m) = g^m \bmod p$.

   (a) (2 points) Does this function has the preimage resistance (it is hard to find a message that hashes to a particular value).

   ● **True**<br>
   ○ False

   (b) (2 points) Does this function has the strong collision resistance (it be hard to find any two messages with the same hash).

   ○ True<br>
   ● **False**

3. Choose one answer

(a) (3 points) To encrypt a series of plaintext blocks $p_1, p_2, \ldots, p_n$ using a block cipher $E$ operating in electronic code book (ECB) mode, each ciphertext block $c_1, c_2, \ldots, c_n$ is computed as $c_i = E_k(p_i)$.

Which of the following is **NOT** a property of this block cipher mode?

○ Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.

○ Decryption can be fully parallelized.

● **If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.**

○ None of the above; that is, (a), (b), and (c) are all properties of the ECB block cipher mode.

(b) (3 points) To encrypt a series of plaintext blocks $p_1, p_2, \ldots, p_n$ using a block cipher $E$ operating in cipher block chaining (CBC) mode, each ciphertext block $c_1, c_2, \ldots, c_n$ is computed as $c_i = E_k(p_i \oplus c_{i-1})$, where $c_0$ is a public initialization vector (IV) which should be different for each encryption session.

Which of the following is a property of this block cipher mode?

○ Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.

● **Decryption can be fully parallelized.**

○ If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.

○ None of the above; that is, neither (a), (b), nor (c) are properties of the CBC block cipher mode.

(c) (3 points) The Diffie–Hellman protocol is used to generate a shared secret key between two parties using a public channel. Which of the following public key encryption and digital signature schemes is most similar to the Diffie–Hellman protocol?

○ RSA encryption.

○ RSA signatures.

● **Elgamal encryption.**

○ Elgamal signatures.

4. Suppose that a block cipher is defined as follows. Encrypt bit strings of length 6 by mapping $x_1$, $x_2$, $x_3$, $x_4$, $x_5$, $x_6$ to $x_4$, $x_5$, $x_6$, $x_1 + x_5 + x_6$, $x_2 + x_4 + x_6$, $x_3 + x_4 + x_5$.

   (a) (4 points) What is this kind of cipher called?

   **Solution:** A Feistel cipher. (Hill cipher — 2 points)

   (b) (4 points) Encrypt 100111.

   **Solution:** 1, 1, 1, 1+1+1=1, 0+1+1=0, 0+1+1=0, so 111100.

   (c) (4 points) (ANSWER ONLY) If $y_1$, $y_2$, $y_3$, $y_4$, $y_5$, $y_6$ is the ciphertext, what is the corresponding plaintext?

   **Solution:** $x_4 = y_1$, $x_5 = y_2$, $x_6 = y_3$, $x_1 + x_5 + x_6 = y_4$, $x_2 + x_4 + x_6 = y_5$, $x_3 + x_4 + x_5 = y_6$, we solve to get $x_4 = y_1$, $x_5 = y_2$, $x_6 = y_3$, $x_1 = y_4 + y_2 + y_3$, $x_2 = y5 + y1 + y3$, $x_3 = y_6 + y_1 + y_2$, so decryption is

   $$y_2 + y_3 + y_4, \quad y_1 + y_3 + y_5, \quad y_1 + y_2 + y_6, \quad y_1, \quad y_2, \quad y_3.$$

5. (6 points) Consider a degree 6 LFSR where only $c_5$ and $c_0$ are set to 1. What are the first 10 bits output by this LFSR if it starts in initial state $(x_0, x_1, x_2, x_3, x_4, x_5) = (1, 1, 1, 1, 1, 1)$?

**Solution:**

$$\begin{array}{cccccc}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 1
\end{array}$$

This is enough. Now the first 10 bits of output is 1111110101.

6. (a) (4 points) Give in detail the steps needed to create an instance of RSA, assuming encryption exponent 3, making sure you indicate what are the encryption and decryption functions and what is made public and what kept secret.

**Solution:** Establish distinct large primes $p$ and $q$, keep secret. Let $N = pq$, make public

Establish integer $d$ such that $3d \equiv 1 \bmod (p-1)(q-1)$, keep secret.

Public key $(N, 3)$, private key $(N, d)$.

Encryption function $e(x) = x^3 \bmod N$.

Decryption function $d(y) = y^d \bmod N$.

(b) (4 points) Explain how Alice can send a signed message to Bob using RSA, how Bob verifies the signature, and how Alice can use a secure hash function to sign a long message quickly.

**Solution:** Suppose Alice has RSA privite key $k_{pr}$, public key $k_{pub}$, and hash function $h$.

Now Alice can sign message $m$ by

$$s = e_{k_{pr}}(h(m))$$

and send $(m, s)$ to Bob.

Now Bob can verify the signature by computing

$$e_{k_{pub}}(s)$$

and comparing with $h(m)$.

7. (4 points) Consider the RSA cryptosystem where $N = 35$ and the encryption exponent is 11. Compute the decryption exponent. Encrypt message $x = 6$.

**Solution:** $\varphi(N) = (5-1)(7-1) = 24$. $11d \equiv 1 \bmod 24 \Rightarrow \boxed{d = 11}$.

$6^{11} \equiv 36^5 \cdot 6 \equiv \boxed{6} \bmod 35$.

8. (4 points) Consider the DHKE where prime is 11 and generator is 2. Alice generated private key 4 and receive Bob's public key 6. Compute Alice's public key and message key.

**Solution:** Alice's public key: $k_A = 2^4 = \boxed{5} \bmod 11$.

Message key: $k_{AB} = 6^4 = 36^2 = 2^2 = \boxed{9} \bmod 11$.

9. (6 points) Alice knows that she will want to send a single 128-bit message to Bob at some point in the future. To prepare, Alice and Bob first select a 128-bit key $k$ uniformly at random. When the time comes to send a 128-bit message $x$ to Bob, Alice considers two ways of doing so.

   She can use the key as a one-time pad, sending Bob $k \oplus x$ (meaning bit-by-bit addition). Alternatively, she can use AES-128 to encrypt $x$ as a single block and send Bob its encryption $AES_k(x)$.

   Assume Eve will see either $k \oplus x$ or $AES_k(x)$, that Eve knows an initial portion of $x$ (a standard header), and that she wishes to recover the remaining portion of $x$. If Eve has time to try out every possible $k$, which scheme would be more secure? Compare and evaluate the following arguments and indicate which one you agree with.

   (a) The one-time pad would be more secure. Even if Eve tried all possible keys, she would not be able to recover the unknown portion of $x$. If AES was used, Eve could eventually learn the unknown portion of $x$.

   (b) AES would be more secure. Even if Eve tried all possible keys, she would not be able to recover the unknown portion of $x$. If the one-time pad was used, Eve could eventually learn the unknown portion of $x$.

   (c) They would be equally secure. Either way, Eve could eventually learn the unknown portion of $x$.

   (d) They would be equally secure. Either way, Eve would not be able to learn the unknown portion of $x$.

**Solution:** The correct answer is (d). Even after trying every possible key (including the actual one), Eve will have no way of recognizing the correct plaintext or even narrowing down the possibilities in any way. Why is this? Well, since AES is a distinct permutation on $\{0,1\}^{128}$ under each possible key, and the key was selected uniformly at random, given any plaintext, each possible ciphertext is equally likely. So when AES is used for a single block with a random key of the same length, the effect is exactly the same as using a one time pad: the ciphertext reveals no information about the plaintext.

10. Let $E$ be the elliptic curve $y^2 = x^3 + 2x + 4 \pmod 5$.

(a) (4 points) Write down all the points of $E(\mathbb{Z}_5)$.

**Solution:** Bruteforce: $\boxed{\{\mathcal{O}, (0,2), (0,3), (2,1), (2,4), (4,1), (4,4)\}}$

(b) (6 points) Choose any non trivial point $P$ from part (a) and find $P$, $2P$, $3P$, …

**Solution:** Suppose $P = (0,2)$.
$2P = P + P = (4,1)$
$3P = 2P + P = (2,1)$
$4P = 2P + 2P = (2,4) = -3P$, so $7P = \mathcal{O}$ and $5P = -2P = (4,4)$, $6P = -P = (0,3)$, $8P = P$, …

| $P$ | $2P$ | $3P$ | $4P$ | $5P$ | $6P$ | $7P$ | $8P$ | … |
|---|---|---|---|---|---|---|---|---|
| $(0,2)$ | $(4,1)$ | $(2,1)$ | $(2,4)$ | $(4,4)$ | $(0,3)$ | $\mathcal{O}$ | $(0,2)$ | … |

Other choice $P = (2,1)$ gives

| $P$ | $2P$ | $3P$ | $4P$ | $5P$ | $6P$ | $7P$ | $8P$ | … |
|---|---|---|---|---|---|---|---|---|
| $(2,1)$ | $(0,3)$ | $(4,1)$ | $(4,4)$ | $(0,2)$ | $(2,4)$ | $\mathcal{O}$ | $(2,1)$ | … |

11. (a) (4 points) Describe in two to three sentences the main points about how DES works.

**Solution:** DES is a block cipher with blocks of length 64 and a key of length 56, consisting of 16 Feistel rounds combined with various permutations to mix up the bits. A key schedule produces the 16 48-bit subkeys from the main key.

(b) (6 points) When DES was compromised, why did they turn to triple DES instead of just double DES? Explain carefully why encrypting twice with different DES keys does not yield as much security as one might hope.

**Solution:** Double DES: $y = DES_{k_2}(DES_{k_1}(x))$ is no more secure than DES due to "meet in the middle" attack. Suppose we have known plaintext attack using two plaintext/ciphertext pairs: $(x_1, y_1)$, $(x_2, y_2)$. In this situation, we have

$$DES_{k_2}^{-1}(y_1) = DES_{k_1}(x_1)$$
$$DES_{k_2}^{-1}(y_2) = DES_{k_1}(x_2)$$

Now we can find $k_2$ and $k_1$ by bruteforce of size $2^{56}$.