Department of Mathematics, University of Wisconsin-Madison

Math 435— Midterm Exam— 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.

Letters `A`, `B`, ..., `Z` are represented by $\mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$ as usual.

Question:	1	2	3	4	5	6	7	8	Total
Points:	9	9	6	11	6	6	6	16	69

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

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

First Name: _____ Last Name: _____

1. (9 points) Which of the following is a legitimate cipher?

   (a) $x \to x^{-1} \bmod 26$ if $x \neq 0$, $0 \mapsto 0$.

   ◯ Yes, legitimate

   ◯ No

   (b) $x \to 15x + 13 \bmod 26$.

   ◯ Yes, legitimate

   ◯ No

   (c) $x \to x^2 \bmod 26$.

   ◯ Yes, legitimate

   ◯ No

2. (9 points) (a) DES cipher uses block size of 64 bits and key size of 56 bits. Can it provides perfect security?

   ◯ Yes,

   ◯ No.

   (b) Consider an encryption scheme, where the plaintext and ciphertext are $2n$-bit strings. The key generation algorithm works as follows: generate a n-bit random string s and the key is $k = s\|s$ (where $\|$ is concatenation). Encryption and decryption work exactly as one-time pad $c = m \oplus k$ and $m = c \oplus k$. Can this scheme be perfectly secret?

   ◯ Yes,

   ◯ No.

   (c) When choosing a password, high entropy is desirable.

   ◯ Yes,

   ◯ No.

3. (6 points) Using the Hill cipher with key

$$\begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix}$$

(all entries are modulo 26), encrypt `MATH`.

4. (11 points) ANSWERS ONLY. Consider the class of monoalphabetic substitution ciphers that send vowels (`A`, `E`, `I`, `O`, `U`, `Y`) to vowels and consonants to consonants,

   (a) Calculate how many keys there are (leaving factorials in your answer)?

   (b) Suppose entropy of English text is 2.5 bits per symbol. What is the (nominal) unicity point for this class of ciphers (don't simplify your answer)?

   (c) If we use this cipher to encrypt a single letter, do we have perfect secrecy?

   ◯ Yes,

   ◯ No.

5. (6 points) An affine cipher produces ciphertext `SBQDS`. We know the plaintext starts `DA`. Find the plaintext.

6. (6 points) Determine sequence generated by LFSR with $n = 3$, $c_0 = c_1 = 1$, $c_2 = 0$, $x_0 = x_2 = 0$, $x_1 = 1$.

7. (6 points) Consider a variant of the Vigenère 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. Using this cipher, the key is never repeated, so Kasiski's attack will fail.

   Now assume that Alice, using this cipher, sends Bob a ciphertext that reads

   `JLQJRYFQEKL`.

   The plaintext is known to be either `VEGETARIANS` or `BACONGREASE`. Determine which plaintext Alice sent to Bob, and explain how you reached your answer.

8. (16 points) (a) Describe briefly how frequency analysis is used to break a monoalphabetic cipher.

(b) In particular, which of the three kinds of attack is this used for?

(c) The ciphertext `PDAPAOP` was produced using a shift cipher. Using frequency analysis find the plaintext (which should make sense in English).