Cryptography
Assignment 2

Dr. Charlie Obimbo **Due: February 11th, 2025**

Name: Tyler Janvrin **To be done in LaTeX**
Assignment is out of 10

1 One-Time Pad

Recall that in class we demonstrated how using the One-time pad was secure. In effect we showed how, in an effort to try and decrypt the cipher-text:

“ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS”

One cryptanalyst came up with the decryption: “MR MUSTARD WITH THE CANDLESTICK IN THE HALL”; while another: “MISS SCARLET WITH THE KNIFE IN THE LIBRARY.

1. Demonstrate how, using the character as the atomic operand, given the cipher-text:

   JACAOYOABLCYOUPOYTBN

   One may get:

   (a) COMMANDER IN CHIEF [1 mark]

   The first step is to calculate values for the ciphertext and plaintext.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
J	A	C	A	O	Y	O	A	B	L	C	Y	O	U	P	O	Y	T	B	N
9	0	2	0	14	24	14	0	1	11	2	24	14	20	15	14	24	19	1	13
C	O	M	M	A	N	D	E	R	I	N	C	H	I	E	F				
2	14	12	12	0	13	3	4	17	8	13	2	7	8	4	5				

Since the one-time pad operates on the text like so: PLAINTEXT + PAD = CIPHERTEXT, we can find the desred plaintext by subtracting the plaintext from the ciphertext: PAD = CIPHERTEXT - PLAINTEXT.

I did the computations in Excel and copied them over to this document. The final result for the pad that gives this ciphertext is is: HMQOOLLWKDPWHMLJ

I ignored spaces, which I’m pretty sure is correct. If I hadn’t, I would have gotten a slightly different result.

9	0	2	0	14	24	14	0	1	11	2	24	14	20	15	14				
M	I	N	U	S															
2	14	12	12	0	13	3	4	17	8	13	2	7	8	4	5				
E	Q	U	A	L	S														
7	-14	-10	-12	14	11	11	#	-16	3	-11	22	7	12	11	9				
M	O	D	2	5															
7	12	16	14	14	11	11	#	10	3	15	22	7	12	11	9				
H	M	Q	O	O	L	L	W	K	D	P	W	H	M	L	J				

(b) `THE SERGEANT AT ARMS` [1 mark]

The process for this one is exactly the same:

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

The final result for the pad that will produce JACAOYOABLCYOUPOYTBN from THE SERGEANT AT ARMS is QTYIKHIWBYJYVUYCG

2. Joseph sends Aisha a message using a One-time pad. He also sends David another message using the same key. You were able to get both messages, as:

   `0809 0302 0607 1A17 1A08 1C07 141D` and [2 marks]

   `0005 1311 1911 1907 0D09 1B08 130B`

   If the atomic operand is the bit, decrypt both messages and find the potential key.

   Consider that one of the phrases may be from the following list:

GORGEOUS SUSAN	SHE ADORES JOHN
NICOTINE IS BAD	MARIJUANAS LEGAL
JUSTINE TRUDEAU	FLOYD MAYWEATHER
ANGELINA JOLIE	EMBEZZLED FUNDS
NANETTE WORKMAN	ELIZABETH MAY
GRANT US PEACE	WE'RE AWESOME

   When you're using a binary pad, you're using XOR. You go PLAINTEXT xor PAD = CRYPTEXT. XOR inverts the bits in the pad based on the bits in the plaintext, so if you have the message, you can go PLAINTEXT xor CRYPTEXT = PAD to derive the pad.

   Since there were only 12 possibilites for the plaintext, I just brute-forced it, using:

   https://www.dcode.fr/xor-cipher to do the xor calculations.

   I computed all twelve possible values for the pad for each of the plaintexts (24 total), and then using each possible pad against each plaintext until I encountered a message that made sense (if the message hadn't made sense, it wouldn't have been possible to find the correct pad).

   When I decrypted 0005 1311 1911 1907 0D09 1B08 130B using the pad generated from EMBEZZLED FUNDS xor 0809 0302 0607 1A17 1A08 1C07 141D, I got the phrase MARVELOUS!AZIR. That's clearly not random, so I think I must have found the pad. The pad I got is: 4D44 4147 5C5D 5652 5E28 5A52 5A59 (with possibly some extra characters at the end, because the lengths aren't exactly the same).

2 Number Theory & Hill Cipher

4. Is $2^{82589933} - 1$ prime? Yes, it is. [0.5]

   Why? It was discovered to be prime by GIMPS (Great Internet Mersenne Prime Search) in 2018. At that time, it was the largest known prime. Source:

   https://www.mersenne.org/primes/press/M82589933.html [0.5]

5. Use Euclid's Algorithm to find `gcd(422774, 1009).` [No Partial Marks] (1 Mark)

   $gcd(422774, 1009)$
   Use Euclid's algorithm:
   $422774 = 419 * 1009 + 3$
   $1009 = 336 * 3 + 1$

   Therefore, the GCD of 422774 and 1009 is 3.

6. Find the inverse of `1009 (mod 422774).` [No Partial Marks] (1 Mark)

   To find this, we can use the Extended Euclidean Algorithm and the results from Q5.

   $1 = 1009 - 336 * 3$
   $1 = 1009 - 336 * (422774 - 419 * 1009)$
   $1 = 1009 - 336 * 422774 + 336 * 419 * 1009$
   $1 = 1009 - 336 * 422774 + 140784 * 1009$
   $1 = 140785 * 1009 - 336 * 422774$
   $1 = 140785 * 1009(mod\ (422774))$

   Therefore, the inverse of 1009 (mod 422774) is 140785.

7. Find all solutions (between 1 & 265) to the equation $35x \equiv 15$ (mod 265). [1]

   $35x = 15(mod\ 265)$
   $7x = 3(mod\ 53)$
   $38 * 7x = 38 * 3(mod\ 53)$ 38 is the multiplicative inverse of 7
   $266x = 114(mod\ 53)$
   $x = 8(mod\ 53)$
   $x = 8, 61, 114, 167, 220, (mod\ 265)$

8. (Hill-Cipher) Bob sends Alice the following code, in which the Hill-Cipher has been used, modulo 31. The key matrix used is:

$$K = \begin{bmatrix} 5 & 30 & 23 \\ 6 & 30 & 20 \\ 26 & 1 & 9 \end{bmatrix} \quad \text{and The Ciphertext } A \text{ is:}$$

$$\begin{bmatrix} T & 1 & H & I & C & O & Z & F \\ F & W & B & T & S & P & B & J \\ M & R & 2 & A & J & X & K & U \end{bmatrix}$$

If Bob used the following decimal encoding:

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Code	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Letter	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	
Code	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	

(a) Compute the inverse of the matrix K (mod 31). [1]

(b) Find the plaintext M. (Remember to remove the gibberish & punctuate it correctly.) [1]

9. -113 (mod 10) = ____ [1]