CS-1306 - Monsoon 2024- Homework 1

Vedaa Anand

Question 1

Ciphertext: EVIRE

I began with assuming that the answer was ‘ARENA’, and worked backwards from there.
The first and last letter was ‘E’ of the cipher text, thus the corresponding letter should be ‘A’ if the answer is ‘ARENA’. This assumption meant that the cipher utilized shift 22: $A \to W$, $B \to X$, $C \to Y$ and so on. This proved to be correct for every consequent letter.

$$E \to A$$

$$V \to R$$

$$I \to E$$

$$R \to N$$

$$E \to A$$

Decrypted message: ARENA
Thus, Antony will meet Caesar at the Colosseum.

Question 2

We want to find a^{-1} such that:

$$1 \equiv a * a^{-1} \; mod \; m$$

Since $1 \equiv 27 \; mod \; 26$ and $a = 9$, we know that $a^{-1} = 3$.

Encrypted text: U C R
Encrypted value: 20 2 17
$3 * (x - 2) \; mod$ 26: 2 0 19

Decrypted text: CAT

Question 3

(a) In order to find the column length, we need to divide the length of the message by the length of the key.

$$\frac{\text{length of message}}{\text{length of key}} = \frac{49}{12} = 4 + \frac{1}{12}$$

Thus, each column will have a length of 5, but only the first column will have all 5 spaces filled. The other 11 columns will only have the first four spaces filled.

I wrote out the key, 'Cryptography', and labelled the columns based on the respective letter's place in the alphabet. For instance, 'A' is the first letter of the alphabet, and is labelled as column 1. In the case of repeated letters (R, Y), their numeric status was based on their position from left-to-right. For instance, the first 'R' was labelled 8, and the second was labelled 9. Once this was complete, I put in the encrypted text into the table column-wise, resulting in the following table:

C	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**Y**
2	8	11	6	10	5	3	9	1	7	4	12
p	e	o	p	l	e	s	a	y	n	o	t
h	i	n	g	i	s	i	m	p	o	s	s
i	b	l	e	b	u	t	i	d	o	n	o
t	h	i	n	g	e	v	e	r	y	d	a
y	-	-	-	-	-	-	-	-	-	-	-

Adding spaces and punctuation to the text for readability, the plaintext is:
People say nothing is impossible, but I do nothing every day.

Question 4

(a) Let

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We know that $BA \to HC$. This means:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} B \\ A \end{bmatrix} = \begin{bmatrix} H \\ C \end{bmatrix} (mod\ 26)$$

$$\implies \begin{bmatrix} Ba + Ab \\ Bc + Ad \end{bmatrix} = \begin{bmatrix} H \\ C \end{bmatrix} (mod\ 26)$$

We can break this down into two equations:

$$Ba + Ab = H$$

$$Bc + Ad = C$$

These equations can be simplified to:

$$(1 * a) + (0 * b) = H \implies a = H \implies a = 7$$

$$(1 * c) + (0 * d) = C \implies c = C \implies c = 2$$

We also know that $ZZ \to GT$. Thus:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} Z \\ Z \end{bmatrix} = \begin{bmatrix} G \\ T \end{bmatrix} (mod\ 26)$$

$$\implies \begin{bmatrix} Za + Zb \\ Zc + Zd \end{bmatrix} = \begin{bmatrix} G \\ T \end{bmatrix} (mod\ 26)$$

$$\implies \begin{bmatrix} 25a + 25b \\ 25c + 25d \end{bmatrix} = \begin{bmatrix} 6 \\ 19 \end{bmatrix} (mod\ 26)$$

Simplifying each equation:

$$25(a + b) = 6\ (mod\ 26)$$

$$25(c + d) = 19\ (mod\ 26)$$

Considering equation 1, we know that $25(mod\ 26) \equiv -1$, so:

$$-(a + b)\ (mod\ 26) = 6$$

$$\implies a + b = -6\ (mod\ 26)$$

$$\implies a + b = 20 \implies 7 + b = 20$$

$$\implies b = 13$$

Considering equation 2, once again we know that $25(mod\ 26) \equiv -1$, so:

$$-(c + d)\ (mod\ 26) = 19$$

$$\implies a + b = -19\ (mod\ 26)$$

$$\implies c + d = 7 \implies 2 + d = 7$$

$$\implies d = 5$$

Therefore, the key is:

$$M = \begin{bmatrix} 7 & 13 \\ 2 & 5 \end{bmatrix}$$

(b) For K to be a valid, the matrix needs to be invertible against modulus 26. This can be verified by checking if the determinant of the matrix is 0.

$$det(K) = (7 * 4) - (2 * 1) = 26$$

Since 26 *modulo* 26 is 0, this is not a valid matrix for encrypting a message.

Question 5

(a) Alice will not be able to find an encryption method under the given conditions that will allow her to reach perfect security. This is because **length of key** $<$ **length of message**.
Proof:

$$\mathcal{M} = \{5, 6, 7, 8, 9\}$$

$$\mathcal{K} = \{0, 1, 2\}$$

	0	**1**	**2**
5	$\frac{1}{9}$	$\frac{1}{9}$	$\frac{1}{9}$
6	$\frac{1}{9}$	$\frac{1}{9}$	$\frac{1}{9}$
7	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{18}$
8	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
9	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$

Let us calculate the sample space Ω:

	0	**1**	**2**
5	(5, 0, 5)	(5, 1, 6)	(5, 2, 7)
6	(6, 0, 6)	(6, 1, 7)	(6, 2, 8)
7	(7, 0, 7)	(7, 1, 8)	(7, 2, 9)
8	(8, 0, 8)	(8, 1, 9)	(8, 2, 5)
9	(9, 0, 9)	(9, 1, 5)	(9, 2, 6)

Testing if this is information-theoretically secure:

$$Pr(c = 5) = \frac{1}{9} + \frac{1}{36} + \frac{1}{36} = \frac{1}{6}$$

$$Pr(m = 8 \wedge c = 5) = \frac{1}{36}$$

$$Pr(m = 8 | c = 5) = \frac{Pr(m = 8 \wedge c = 5)}{Pr(c = 5)} = \frac{1}{6}$$

$$Pr(m = 8) = \frac{1}{36} + \frac{1}{36} + \frac{1}{36} = \frac{1}{12}$$

Since $Pr(m = 8|c = 5) \neq Pr(m = 8)$, it shows that c and m are *not* statistically independent, and thus she cannot reach perfect security.

(b) It *is* possible to create a system such that the newer cryptosystem is perfectly secure. For this to happen, the key needs to be modified:

$$\mathcal{K} = \{0, 1, 2, 3, 4\}$$

Now, $|\mathcal{M}| = |\mathcal{K}|$, so the system will be perfectly secure.

(c) Proof:

$$\mathcal{M} = \{5, 6, 7, 8, 9\}$$

$$\mathcal{K} = \{0, 1, 2, 3, 4\}$$

Each key, $k \in \mathcal{K}$, has probability $\frac{1}{5}$, and each message ,$m \in \mathcal{M}$, has probability $\frac{1}{5}$.

$m \backslash k$	**0**	**1**	**2**	**3**	**4**
5	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
6	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
7	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
8	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
9	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$

Let's calculate the sample space Ω:

$m \backslash k$	**0**	**1**	**2**	**3**	**4**
5	$(5, 0, 5)$	$(5, 1, 6)$	$(5, 2, 7)$	$(5, 3, 8)$	$(5, 4, 9)$
6	$(6, 0, 6)$	$(6, 1, 7)$	$(6, 2, 8)$	$(6, 3, 9)$	$(6, 4, 5)$
7	$(7, 0, 7)$	$(7, 1, 8)$	$(7, 2, 9)$	$(7, 3, 5)$	$(7, 4, 6)$
8	$(8, 0, 8)$	$(8, 1, 9)$	$(8, 2, 5)$	$(8, 3, 6)$	$(8, 4, 7)$
9	$(9, 0, 9)$	$(9, 1, 5)$	$(9, 2, 6)$	$(9, 3, 7)$	$(9, 4, 8)$

Testing if this is information-theoretically secure:

$$Pr(c = 5) = \frac{1}{25} + \frac{1}{25} + \frac{1}{25} + \frac{1}{25} + \frac{1}{25} = \frac{1}{5}$$

$$Pr(m = 8 \wedge c = 5) = \frac{1}{25}$$

$$Pr(m = 8 | c = 5) = \frac{Pr(m = 8 \wedge c = 5)}{Pr(c = 5)} = \frac{1}{5}$$

$$Pr(m = 8) = \frac{1}{25} + \frac{1}{25} + \frac{1}{25} + \frac{1}{25} + \frac{1}{25} = \frac{1}{5}$$

Since $Pr(m = 8) = Pr(m = 8 | c = 5)$, it shows that c and m are statistically independent, so c gives *no information* about m. As a result, this system is perfectly secure.

What do these exercises tell you about perfect security?
Can you draw some larger conclusions about this type of security from these exercises?
Perfect security ensures that an adversary's ability to decrypt a message is *not* dependent upon computational power. Instead, it works on the principle of 'equal chance'- it's equally likely to pick any message, ciphertext, and key from their respective supersets. Essentially, in order for perfect security to exist, for every $m \in \mathcal{M}$, and every $c \in \mathcal{C}$, there exists a unique key $k \in \mathcal{K}$, such that $E_k(m) \rightarrow c$. For this to exist, $|\mathcal{K}| \geq |\mathcal{M}|$.

Question 6

(a) Zark *will* recognize that it is only 1 repeated letter, but *will not* be able to deduce the letter, nor the key.
A shift cipher involves shifting letters of the alphabet by a fixed number of places. For instance, with a shift of 4, ‘A’ becomes ‘E’, ‘B’ becomes ‘F’, and so on. As a result, the cipher text will be 1 repeated letter, so Zark will recognize that. However, the lack of other letters present in the ciphertext means that there is no means of finding how large the shift is, and thus no means of knowing what the letter is.

(b) Zark *will* recognize that it is only 1 repeated letter, but *will not* be able to deduce the letter, nor the key.
An affine cipher is a substitution cipher, so each time a given letter occurs in the plaintext, it always is replaced by the same ciphertext letter. Affine encryption uses the encryption key (α, β) in $y \equiv \alpha x + \beta \ (mod\ 26)$, where α is coprime with 26.
Since $gcd(\alpha, 26) = 1$, α can take on the values $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$. β can take on any value $0 - 25$. As a result, there are $12 * 26 = 312$ possible encryption keys.
Technically, this can be brute-forced. However, the lack of other letters present in the ciphertext will prevent him from being able to test all possible encryption keys.

(c) Zark *will* recognize that it is only 1 repeated letter, and *will* know the letter, but *will not* be able to deduce the key.
Since ‘A’ takes the value 0, the numerical column matrix equivalent of the plaintext will be all 0s. As a result, the ciphertext and plaintext will be the same, and Zark will recognize the letter and the repetition. However, since everything is multiplied by 0, Zark has no way of knowing what the key is.

Question 7

(a) I knew that 'e' is the most common letter used in the English language, so I initially assumed $c \to e$. However, the text didn't make any sense. I then realized that there were more rs in the text, so I decided to try implementing $e \to r$, which is a shift of 13.
Plaintext: helpmeimtrappedinsideacaesarcipherandcantgetout

(b) Using the same strategy, I saw that 'v' was being used a lot in this ciphertext. I implemented $e \to v$, which is a shift of 17.
Plaintext: youmustbespeedoflightbecausetimestopswhenilookatyouhappyvalentinesday

(c) This time I was misled by the hs, but eventually figured out that it is $c \to b$, which is a shift of 25.
Plaintext: ihopeyouinterceptthissecrettransmissionwithoutanyerrorthistransmissionhastravelled--amillionlightyearstoinformyouthatwearecomingsoon

(d) I used the same strategy as (a) and (b): the key is $e \to a$, which is a shift of 22.
Plaintext: olddebayanisagoodoneexceptformelonmelonmelonmelonmelon

Question 9

Let's assume:

1. There are 26 letters in the alphabet.
2. There are 13 plugs.

Now, the problem becomes 'how many ways can 26 letters be divided into pairs of 13'?
First, select a set of 13 letters from the first set of the alphabet provided: $\binom{26}{13}$.
Next, assign the remaining 13 letters to the chosen 13. This can be done in 13! ways.
Lastly, divide by 2^{13}, because the order of the letters do not matter. This gives us:

$$\frac{\binom{26}{13} * 13!}{2^{13}}$$

$$= \frac{26!}{2^{13} * 13!}$$

$$= 7905853580625 \text{ ways}$$

This can be extended to the given problem:

1. There are 26 letters in the alphabet.
2. There are k plugs.

Select a set of k letters from the first set of the alphabet provided: $\binom{26}{k}$.
Then, assign the remaining $26 - k$ letters to the chosen k letters, where each pairing is distinct. This can be done in $\binom{26-k}{k} * k!$ ways.
Lastly, divide by 2^k, since the order of letters do not matter. This gives us:

$$\frac{\binom{26}{k} * k! * \binom{26-k}{k}}{2^k}$$

$$= \frac{26!}{k! * (26-2k)! * 2^k} \text{ ways}$$