CO21BTECH11002
Aayush Kumar
Assignment 1

1) Vigenere cipher is a classical symmetric key substitution cipher. It is a polyalphabetic cipher, meaning that it uses multiple substitution alphabets to encrypt the plaintext.

Sets:

(i) M (Message Space): The set of all possible plaintext messages.

(ii) C (Cipher Text Space): The set of all possible ciphertext messages, which corresponds to the characters used in M.

(iii) K (Key Space): The set of all possible encryption keys. It consists of strings of characters that determine how the substitution alphabets are generated.

Algorithms:-

(i) Gen: The key generation algorithm. It defines how encryption keys are generated or selected.

(ii) Enc:- It takes a plaintext message and an encryption key as input and produces the corresponding ciphertext.

Let $M = m_1 m_2 \ldots m_n$, $K = K_1 K_2 \ldots K_n$

then $C = C_1 C_2 \ldots C_n$

where $C_i = (m_i + K_i) \% L$

where L is the no. of possible characters for K_i.

(iii) Dec :- It takes a ciphertext message and a decryption key as input and produces the corresponding plaintext message.

Let $C = C_1 C_2 \cdots C_n$, $K = K_1 K_2 \cdots K_n$

Then $M = m_1 m_2 \cdots, m_n$

where $m_i = (C_i - K_i) \% L$

2) Consider that Adversary chooses two messages and sends them to Alice. Alice encrypts the messages and sends m_b randomly to A, where $b \in \{0,1\}$.

Then, $\Pr[\text{PrivK}^{eav}_{A,\Pi} = 1] = \Pr[\text{PrivK}^{eav}_{A\Pi} \mid b=0] \Pr[b=0]$
$+ \Pr[\text{PrivK}^{eav}_{A\Pi} \mid b=1] \Pr[b=1]$

$\Rightarrow \Pr[\text{PrivK}^{eav}_{A\Pi} = 1] = \frac{1}{2} \Pr[\text{PrivK}^{eav}_{A\Pi} \mid b=0]$
$+ \frac{1}{2} \Pr[\text{PrivK}^{eav}_{A\Pi} \mid b=1]$

Let C_m be the set of possible ciphertexts that can be obtained for any given $m \in M$.

$\Rightarrow \Pr[\text{PrivK}^{eav}_{A\Pi} \mid b=0] = \sum_{c \in C_{m_0}} \Pr[\text{Priv}^{eav}_{A,\Pi} = 1 \mid C=c] \Pr[C=c]$
$= \frac{1}{|K|} \sum_{c \in C_{m_0}} \Pr[\text{Priv}^{eav}_{A,\Pi} = 1 \mid C=c]$

For $c \in C_{m_0}$, let $M(c)$ be the message space that can be encrypted to c.

$\therefore\ Pr[PrivK^{eav}_{A,\Pi} = 1 \mid C = c] = 1 \cdot Pr[m_1 \notin M(c)] + \frac{1}{2} Pr[m_1 \in M(c)]$

For the best case, A would choose m_0, m_1 such that $|C_{m_0} \setminus C_{m_1}| = 2^l - |K|$

$\Rightarrow Pr[m_1 \notin M(c)] \leq \frac{2^l - |K|}{|C_{m_0}|} = \frac{\epsilon}{1-\epsilon}$

$\Rightarrow Pr[PrivK^{eav}_{A,\Pi} = 1 \mid C = c] = \frac{1}{2} + \frac{1}{2} Pr[m_1 \notin M(c)]$

$\leq \frac{1}{2} + \frac{\epsilon}{2(1-\epsilon)}$

$\Rightarrow Pr[PrivK^{eav}_{A,\Pi} \mid b = 0] \leq \frac{1}{2} + \frac{\epsilon}{2(1-\epsilon)}$

$\&\ Pr[PrivK^{eav}_{A,\Pi} \mid b = 1] \leq \frac{1}{2} + \frac{\epsilon}{2(1-\epsilon)}$

$\Rightarrow Pr[PrivK^{eav}_{A,\Pi}] \leq \frac{1}{2} + \frac{\epsilon}{2(1-\epsilon)}$

For $\epsilon \leq \frac{1}{2}$, $1 - \epsilon \geq \frac{1}{2}$

$\Rightarrow 2(1-\epsilon) \geq 1$

$\Rightarrow \frac{\epsilon}{2(1-\epsilon)} \leq \epsilon$

$\Rightarrow Pr[PrivK^{eav}_{A,\Pi}] \leq \frac{1}{2} + \epsilon$

3) $M = \{0,1\}^{n \times n}$

$F : M \times K \rightarrow M$, $F(m, K) = mK$

The adversary queries a null matrix $\{0\}^{n \times n}$.

Let $f(0^{n \times n}) = \begin{bmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ \vdots & \vdots & & \vdots \\ x_{1n} & x_{2n} & \cdots & x_{nn} \end{bmatrix}$ be the output returned by Alice, where f was chosen by

Alice randomly between f and a PRP.
For f, the probability that output is a null matrix is 1.

For a PRP, the probability that output is a null matrix is $1 - \frac{1}{2^{n^2}}$

Now, the Adversary outputs 0 (i.e., the function is f) if the output is null matrix and 1 otherwise.

Hence, the probability that the adversary is correct is $\frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{2^{n^2}}\right)$
which is significantly larger than $\frac{1}{2}$.
Hence, f is not a pseudorandom permutation.

5) $C_i = Enc(IV \oplus M_i \oplus (i-1), K)$
Consider the following situation. The Adversary A chooses 2 messages, m_0 & m_1.
$m_0 = M_{01} M_{02} \ldots M_{0L}$, $m_1 = M_{11} M_{12} \ldots M_{1L}$
In m_0, A sets $M_{01} = 0$ & $M_{02} = 1$
m_1 is chosen randomly
Hence, with the given encryption scheme we get $Enc(M_{01} \oplus IV \oplus 0, K) = Enc(IV, K)$
& $Enc(M_{02} \oplus IV \oplus 1, K) = Enc(IV, K)$
Hence for m_0 the first two blocks of cipher text would be same.

The adversary outputs 0 is the first two blocks are same and 1 otherwise.

In m_1, since it is chosen randomly, the probability that encryption of first two blocks are same given the blocks themselves are not same will be $1 - \frac{1}{2^{|M|}}$

where $|M| \rightarrow$ length of message block.

Hence the probability that the adversary is correct is $\frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{2^{|M|}}\right)$

which is significantly larger than $\frac{1}{2}$.

Hence, the encryption method is not secure.

4)

a) Voter 1 recieves value C_0 and adds V_1.

Voter 2 recieves value $(C_0 + V_1)\%n$ and adds V_2.

Voter 3 recieves value $(C_0 + V_1 + V_2)\%n$ and adds V_3

⋮

Voter n recieves value $\left(C_0 + \sum_{i=1}^{n-1} V_i\right)\%n$ and adds V_n.

Finally the center recieves the value $C_t =$

$$\left(C_0 + \sum_{i=1}^{n} V_i\right)\%n = (C_0 + S)\%n$$

$$\Rightarrow (C_t - C_0)\%n = (S + C_0)\%n - C_0\%n$$

$$= (S + C_0 - C_0)\%n$$

$$= S\%n = S$$

since $n > t \Rightarrow n > S \Rightarrow S\%n = S$

Hence, the center calculates the sum correctly.

(c) Let $i = x$, $j = x+2$, $K = x+1$

Then ith voter passes the value $c_i = (c + v_x) \% n$ to K.

Kth voter passes value $c_K = (c + v_x + v_{x+1}) \% n$ to jth voter.

jth voter knowing the value of v_x is ~~the~~ now able to calculate the value of $V_K = V_{x+1}$ by calculating $(C_K - (c_i + n)) \% n$

(f) $View_0 = (c_0, c_t)$ $\quad View_i = (S, c_{i-1})$

Given that c_0 is chosen randomly,

$$Pr[C = c_0 \mid S = s] = \frac{1}{n}$$

now, $Pr[C = c_1 \mid S = s] = Pr[C = c_0 \mid S = s] \, Pr[V_1 = 0]$

$$+ Pr[C = c_0 + 1 \mid S = s] \, Pr[V_1 = 1]$$

$$= \frac{1}{n} \times \left(1 - \frac{s}{t}\right) + \frac{1}{n} \times \frac{s}{t}$$

$$= \frac{1}{n}$$

Similarly for $Pr[C = c_2 \mid S = s] = Pr[C = c_3 \mid S = s]$

$$= \dots = Pr[C = c_i \mid S = s] = \dots = \frac{1}{n}$$

Hence, irrespective of the values of V_i, the distribution of $View_i$ remains the same.