Assignment-1 CS6160

Que1 Vigenere Cipher

Sol: Say we represent alphabets as numbers,

$a = 0, b = 1, \ldots, z = 25$.

- Gen (l):- Given length (period) of key Gen algorithm generates uniformly random key k of length l.

  $\Rightarrow$ For $i \in [0, l-1]$ choose uniform k_i form $\{0, 1, \ldots, 25\}$

  Output $k = k_0 k_1 \ldots, k_{l-1}$

- Enc (m, k):- Repeat the key until it has same length as message. Then ~~each~~ letter m_i in message is shifted k_i positions.

  $\Rightarrow$ Message $m = m_0 m_1 m_2 \ldots m_n$

  Key $k = k_0 k_1 \ldots k_l$

  Ciphertext $c = c_0 c_1 c_2 \ldots c_n$

  Then $c_i = [[m_i + k_{(i \% l)}] \bmod 26]$

  Output Ciphertext.

- Dec (c, k):- Repeat the key until it has same length as cipher text. Then letter c_i in cipher text is shifted earlier by k_i positions.

  $\rightarrow$ Cipher text $c = c_0 c_1 c_2 \ldots c_n$

  Key $k = k_0 k_1 \ldots k_l$

  Message $m = m_0 m_1 \ldots m_n$

  Then $m_i = [[c_i - k_{(i \% l)}] \bmod 26]$

  Output message

Que 2) $Pr[PrivK^{eav}_{A,\Pi} = 1] \leq \frac{1}{2} + \varepsilon, \forall \varepsilon > 0, |K| < |M|$

Sol: Using XOR- One time pad.

Consider the following experiment $PrivK^{eav}_{A,\Pi}$:

- Aderversary A outputs a pair of message $m_0, m_1 \in M$
- a uniform bit $b \in \{0,1\}$ is chosen & a key
  $c \rightarrow Enc_k(m_b)$ is given to A by Alice
- A output a bit b'.
- Adversary is succesful if $b' = b$.

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

$\Rightarrow Pr[PrivK^{eav}_{A,\Pi} | b=0] = \sum_{c \in C_{m_0}} Pr[Priv_{A,\Pi} = 1 | C=c] . Pr[C=c]$

By property of total probability & Bayes's Theorem

$Pr[C=c]$ is dependent the inverse of key size

Let $|K| = (1-\varepsilon)|M|$ $(|K| < |M|)$ — (2)

$Pr[C=c] = 1/|K|$

Also $C_{m_0} \rightarrow$ all set of ciphertext derived from message m_0.

$Pr[PrivK^{eav}_{A,\Pi} | b=0] = \frac{1}{|K|} \sum_{c \in C_{m_0}} Pr[Priv^{eav}_{A,\Pi} = 1 | C=c]$ (3)

If m_1 is not ~~one~~ messages that can be encrypted to c then A know no encrypted

$\hookrightarrow m_1 \notin M(c)$ → Messages that encrypt ~~key~~ to cipher text c

Else random guess by A.

So ③ becomes

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

$$= \Pr[m_1 \notin M(c)] + \frac{1}{2}[1 - \Pr[m_1 \notin M(c)]]$$

$$= \frac{1}{2} + \frac{1}{2}\Pr[m_1 \notin M(c)]. \quad (4)$$

$$\Pr[m_1 \notin M(c)] = \frac{|M| - |K|}{|K|}$$

$$\Rightarrow \frac{\varepsilon |M|}{|K|} \text{ from } ②$$

~~As $|K| \geq (1-\varepsilon)|M|$~~

So ④ becomes,

$$\Pr[\text{Priv}^{eav}_{A,\Pi} = 1 \mid C = c] = \frac{1}{2} + \frac{1}{2}\frac{\varepsilon |M|}{|K|} = \frac{1}{2} + \frac{1}{2}\frac{\varepsilon}{(1-\varepsilon)} \quad (8)$$

~~So by ⑧~~

Similar argument for $\Pr[\text{PrivK}^{eav}_{A,\Pi} \mid b = 1]$

∴ By ①, ③, ⑤,

$$\Pr[\text{PrivK}^{eav}_{A,\Pi}] \leq \frac{1}{2} + \frac{1}{2}\left(\frac{\varepsilon}{1-\varepsilon}\right)$$

Now As Probability less than 1

Given $\frac{1}{2} + \varepsilon \leq 1 \Rightarrow \varepsilon \leq 1/2$

$$\Rightarrow 2(1-\varepsilon) > 1$$

$$\Rightarrow \frac{\varepsilon}{2(1-\varepsilon)} < \varepsilon$$

$$\boxed{\Pr[\text{PrivK}^{eav}_{A,\Pi}] \leq \frac{1}{2} + \varepsilon}$$

D

Que 3 Consider the following experiment

Sol^n :- Adversaries queries Null Matrix to Alice.

Alice chose function f randomly from given F & a random permutation

$F(m,k) = mk$

returns random $n \times n$ matrix with $\{0,1\}$

bijection from $\{0,1\}^{n \times n}$ to itself.

If Output of F is null matrix, then Adversary outputs 0, else adversary outputs 1.

$\therefore$ Probability that Adversary is correct is

$$\frac{1}{2}(1) + \frac{1}{2}\left(1 - \frac{1}{2^{n^2}}\right)$$

when random permutation o/p matrix not null

As this probability is much larger than $1/2$

$\therefore$ $F(m,k) = mk$ is not a pseudo random permutation

$\square$.

Que 4

(a) Show that the protocol correctly computes the total sum

Sol^n

Proof by induction:—

~~Base Case~~ $S = (C_t - C_0) \bmod n$

Base Case $(t = 1)$

→ Counter generate C_0, for $t=0$.

then v_1 add voted, $\boxed{S_1 = V_1}$ → To prove

so $C_1 = (C_0 + v_1) \bmod n$

$S_1 = (C_1 - C_0) \bmod n$

Case I:- If $v_1 = 0$

then $\forall\, C_0 \in \{0, \dots, n-1\}$

$C_1 = C_0 \bmod n = C_0$

$\therefore\; S = (C_1 - C_0) \bmod n = (C_0 - C_0) \bmod n$

$S = 0$

$\therefore$ One voter vote → 0
$S = 0$. ✓

Case II If $v_1 = 1$

$\forall\, C_0 \in \{0, \dots, n-2\}$

↓

$C_1 = (C_0 + 1) \bmod n$

$C_1 = C_0 + 1 \quad [C_0 + 1 < n]$

$S = (C_0 + 1 - C_0) \bmod n$

$S = 1$

$C_0 = n-1$

↓

$C_0 = (n-1+1) \bmod n$

$C_0 = 0$.

↓

$S = (0 - (n-1)) \bmod n$

$S = 1$

$\therefore$ One voter vote → 1
$S = 1$

$\boxed{\text{True for } t = 1}$

Inductive step:- Assume for $t = k$,

$S_k = (C_k - C_0) \bmod n$ is correctly computed.

To show :- S_{k+1} is correctly computed.

$C_{k+1} = (C_k + V_{k+1}) \bmod n$

$S_{k+1} = (C_{k+1} - C_0) \bmod n$

$S_{k+1} = ((C_k + V_{k+1}) \bmod n - C_0) \bmod n$

Case 1 :- If $V_{k+1} = 0$

then $S_{k+1} = (C_k - C_0) \bmod n$

$= S_k$

As S_k computed correctly so S_{k+1} computed correctly.

Case 2 $v_{k+1} = 1$

S

$$S_{k+1} = S_k + v_{k+1}$$

$$\Rightarrow (c_{k+1} - c_0) \bmod n = (c_k - c_0) \bmod n + v_{k+1}$$

$c_k = n-1$

$(c_{k+1} - c_0) \bmod n$

$\Rightarrow ((n-1+1) \bmod n - c_0) \bmod n$

$\Rightarrow (-c_0) \bmod n$

$= n - c_0$

$\Rightarrow n - 1 - c_0 + 1$

$\Rightarrow (c_k - c_0) \bmod n + 1$

$\Rightarrow S_k + 1 \to v_i$

$\Rightarrow S_{k+1}$

$c_k < n-1$

$(c_{k+1} - c_0) \bmod n$

$\Rightarrow ((c_k + 1) \bmod n - c_0) \bmod n$

$\Rightarrow (c_k + 1 - c_0) \bmod n$

$\Rightarrow c_k - c_0 + 1$

$\Rightarrow S_{k+1} = S_k + 1 \to v_{k+1}$

S_{k+1} is computed correctly

Hence by principle of mathematical induction S is computed correctly

(b) Show that the protocol is perfectly secure in the following sense

.... as choice of votes varies & restriction that $v_i \in \{0,1\}$. & $\sum_{j=1}^{t} v_j = S$, the distribution of $View_i$ remains the same

Sol^n: $View_i := (S, c_{i-1})$, for $i \in \{1, \dots t\}$

$view_0 := (c_0, c_t)$.

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

where C is a random variable

$C \to \{0, 1, \dots, n-1\}$

For $i = 0$,

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

~~is choice of~~ as c_0 can take a value randomly from $\{0, \dots, n-1\}$

For $i = k$,

let $Pr[C = c_k \mid S = s] = 1/n$ true

for $i = k+1$

$$Pr[C = c_{k+1} \mid S = s] = Pr[C = c_k \mid S = s] \cdot Pr(v_{k+1} = 0) + Pr[C = c_k + 1 \mid S = s] \cdot Pr[v_{k+1} = 1]$$

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

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

$\therefore$ By principle of induction, distribution of $View_i$ remains the same.

(c) Show that if voters i, j collude, they can determine the vote of a third voter k. You are free to choose the indices i, j, k.

Sol^n

Choose $i = m$

$j = m+2$ & $k = m+1$

For $i \rightarrow$ v_m is known

Also $c_m = [c_{m-1} + v_m] \bmod n$ is known

For $j \rightarrow$ v_{m+2} is known

Also $c_{m+2} = [c_{m+1} + v_{m+2}] \bmod n$ is known

$\Rightarrow$ $c_{m+2} = [c_{m+1} + v_{m+2}] \bmod n$

$$c_{m+2} = [(c_m + v_{m+1}) \bmod n + v_{m+2}] \bmod n$$

Here c_{m+2}, c_m, v_{m+2} & n are known

So v_{m+1} i.e, the vote of k^{th} ~~voter~~ voter can be found.

$\therefore$ If i, j collude they can find vote of third voter k

Ans 5 Message block $M_1, M_2, \ldots, M_\ell$

$Enc(-, k) \rightarrow$ for each message block

First we pick $IV \in \{0,1\}^n$ then

$$C_i = Enc(IV \oplus M_i \oplus (i-1), k)$$

Sol^n:- Adversary queries M' message blocks M_1, M_2 such that

$$M_i \oplus (i-1) = 0$$

for first two block

$(i-1)$

i.e, $M_1 = m_0 m_1 \ldots m_n$
$= 0000000\ldots$ n times $\Rightarrow (1-1) = 0$

$M_2 = m_0 \ldots m_n$
$= 1111111$ n times $\Rightarrow 2-2 = 0$.

$\Rightarrow C_1 = Enc(IV \oplus M_1 \oplus (1-1), k)$
$= Enc(IV, k)$

$\Rightarrow C_2 = Enc(IV \oplus M_2 \oplus (2-1), k)$
$= Enc(IV, k)$

Alice choose a message randomly from M' and $M \rightarrow$ (randomly generated message)

If $C_1 = C_2$ then Adversary guess M' & output 0 else output 1

$\therefore$ Probability that Adversary is correct is

$$\frac{1}{2}(1) + \frac{1}{2}\left(1 - \frac{1}{2^n}\right)$$

$\rightarrow$ when M random message have all bits of message block M_1 & M_2 same

As this probability much larger than 1/2

$\boxed{\therefore \text{ This scheme is not secure for some pair of messages}}$