CS6160 Assignment 1

Gautam Singh
CS21BTECH11018

1) The Vigenere cipher is a cryptosystem with $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^+$, and algorithms as follows. Here, we assume

$$m = m_0 m_1 \dots m_{N-1} \quad (1)$$
$$k = k_0 k_1 \dots k_{M-1} \quad (2)$$
$$c = c_0 c_1 \dots c_{N-1} \quad (3)$$

where M and N are some positive integers.

   a) Gen is an algorithm that outputs a key from $\mathcal{K}$ uniformly at random.
   b) $\mathsf{Enc} : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ is defined as

$$\mathsf{Enc}(m,k) \triangleq c,\ c_i \triangleq m_i \oplus k_{i \pmod M},\ 0 \le i < N \quad (4)$$

   c) $\mathsf{Dec} : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ is defined as

$$\mathsf{Dec}(c,k) \triangleq m,\ m_i \triangleq c_i \oplus k_{i \pmod M},\ 0 \le i < N \quad (5)$$

2) Consider an encryption scheme over the binary alphabet $\Pi(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, where $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ and $\mathcal{K} = \mathcal{M} \setminus \{x\}$, and

$$\mathsf{Enc}(m,k) \triangleq m \oplus k \quad (6)$$
$$\mathsf{Dec}(c,k) \triangleq c \oplus k \quad (7)$$

Clearly, we have

$$\Pr(C = 0^n | M = x) = 0. \quad (8)$$

We use (8) to create an adversary $\mathcal{A}$ for the indistinguishability experiment. $\mathcal{A}$ sends message texts $m_0 = x, m_1 = y$ to Alice. If Alice outputs 0^n, then $\mathcal{A}$ outputs $b' = 1$, otherwise $\mathcal{A}$ outputs $b' = 0$. Here,

$$\begin{aligned}
&\Pr\left(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right) \\
&= \Pr(b' = 0 | b = 0) \Pr(b = 0) \\
&+ \Pr(b' = 1 | b = 1) \Pr(b = 1) && (9) \\
&= \Pr(C \neq 0^n | M = x) \Pr(b = 0) \\
&+ \Pr(C = 0^n | M = y) \Pr(b = 1) && (10) \\
&= \frac{1}{2} + \frac{1}{2|\mathcal{K}|} \le \frac{1}{2} + \epsilon && (11)
\end{aligned}$$

From (11), we see that for an ϵ-perfectly secure system, we have

$$\begin{aligned}
\frac{1}{2|\mathcal{K}|} &\le \epsilon && (12) \\
\implies |\mathcal{K}| &\ge \frac{1}{2\epsilon} && (13) \\
\implies 2^n - 1 &\ge \frac{1}{2\epsilon} && (14) \\
\implies n &\ge \log_2\left(1 + \frac{1}{2\epsilon}\right). && (15)
\end{aligned}$$

From (15), it is clear that we can obtain the required security by choosing n sufficiently large.

3) We describe an adversary $\mathcal{A}$ that can distinguish between F and a random permutation over $\{0,1\}^{n \times n}$. $\mathcal{A}$ makes the following queries and decisions.

   a) Send message $\mathbf{m}_1 = \mathbf{I}$, where $\mathbf{I}$ denotes the identity matrix. Let the received output be $\mathbf{c}_1$.
   b) If $\mathbf{c}_1$ is not invertible, output 1, else send message $\mathbf{m}_2 = \mathbf{c}_1^{-1}$. Let the received output be $\mathbf{c}_2$.
   c) If $\mathbf{c_2} = \mathbf{I}$, output 0, else output 1.

Then, we see that if a random string is used, the probability that $\mathbf{c}_2 = \mathbf{I}$ is negligible. If F is used, then it is clear that $\mathbf{c_2} = \mathbf{I}$. Thus,

$$\begin{aligned}
&\Pr(\mathsf{PRPExp}(\mathcal{A}, \Pi) = 1) \\
&= \frac{1}{2} + \frac{1}{2}(1 - \mathrm{negl}(n)) \approx 1. && (16)
\end{aligned}$$

Thus, $\mathcal{A}$ can distinguish between F and a random string with high probability. Thus, F is not a PRP.

4) a) We have, for $1 \le i \le t$,

$$c_i = v_i + c_{i-1} \bmod n. \quad (17)$$

Thus, inductively,

$$c_i = \sum_{j=1}^{i} v_j + c_0 \bmod n. \tag{18}$$

Note that, since $t < n$ and $v_i \in \{0, 1\}$,

$$0 \leq \sum_{i=1}^{t} v_i \leq t < n, \tag{19}$$

and therefore, using (19) and (18),

$$c_t = \sum_{i=1}^{t} v_i + c_0 \bmod n \tag{20}$$

$$\sum_{i=1}^{t} v_i = c_t - c_0 \bmod n = S \tag{21}$$

as required.

b) For $i = 0$, since $S = c_t - c_0 \bmod n$ and S is fixed, we must have $c_t = S + c_0 \bmod n$. Since c_0 is chosen uniformly at random, we have n uniformly random obtainable pairs (c_0, c_t). Thus,

$$\Pr\left(View_0 = (c_0, c_t)\right) = \frac{1}{n}. \tag{22}$$

Note that for $1 \leq i \leq t$,

$$c_i = \left(\sum_{j=1}^{i} v_j\right) + c_0 \bmod n. \tag{23}$$

We must also have $0 \leq c_i - c_0 \bmod n \leq i$. Hence,

$$\begin{aligned}
&\Pr\left(View_i = (S, c_{i-1})\right) \\
&= \sum_{c_0=0}^{n-1} \Pr\left(View_i = (S, c_{i-1}), c_0\right) && (24) \\
&= \frac{1}{n} \sum_{c_0=0}^{n-1} \Pr\left(View_i = (S, c_{i-1}) \mid c_0\right) && (25) \\
&= \frac{1}{n} \sum_{c_0=0}^{n-1} \Pr\left(c_{i-1} = \sum_{k=1}^{i-1} v_k + c_0 \bmod n \;\middle|\; S, c_0\right) && (26) \\
&= \frac{1}{n} \sum_{j=0}^{n-1} \frac{\binom{i-1}{j}\binom{t-i+1}{S-j}}{\binom{t}{S}} && (27)
\end{aligned}$$

where we define

$$j \triangleq \sum_{k=1}^{i-1} v_k = c_{i-1} - c_0 \bmod n. \tag{28}$$

Since $0 \leq c_0 \leq n-1$, we have $0 \leq j \leq n-1$. However, we know that for some $0 \leq k \leq n$,

$$\sum_{j=0}^{n} \binom{i}{j}\binom{n-i}{k-j} = \binom{n}{k}. \tag{29}$$

Since $\max(i-1, t-i+1) \leq t \leq n-1 < n$,

$$\begin{aligned}
&\Pr\left(View_i = (S, c_{i-1})\right) \\
&= \frac{1}{n\binom{t}{S}} \sum_{j=0}^{t} \binom{i-1}{j}\binom{t-i+1}{S-j} && (30) \\
&= \frac{1}{n}\frac{\binom{t}{S}}{\binom{t}{S}} = \frac{1}{n}. && (31)
\end{aligned}$$

Thus, the voting protocol is secure with respect to the given definiton.

c) Consider the voters $i, i+1, i+2$, where $1 \leq i \leq t-2$. Voter i conputes c_i and passes that on to voter $i+2$. Now, when voter $i+2$ computes c_{i+2}, we have,

$$c_{i+2} = c_i + v_{i+1} + v_{i+2} \bmod n \tag{32}$$

Since votes $i+2$ knows all the terms in (32) except the requried v_{i+1}, they can use the given information to determine it, and thus find the vote of voter $i+1$.

5) Consider the pair of messages M_1 and M_2, where for $1 \leq i \leq L$,

$$M_{1i} = (i-1), \; M_{2i} = m \tag{33}$$

where m is any message block. Then, for all i,

$$C_{1i} = \mathsf{Enc}(IV, k) \tag{34}$$

$$C_{2i} = \mathsf{Enc}(IV \oplus m \oplus (i-1), k). \tag{35}$$

Hence, all ciphertext blocks in C_1 are always equal. We use this as a test to distinguish the two messages. We output 1 if all ciphertext blocks are equal, and 0 otherwise. Since the probabilities of all ciphertext blocks of M_2 can be equal with negligible probability, it follows that we can distinguish between these two messages encrypted using this mode of operation with high probability.