CSE5014 · Cryptography and Network Security

# Assignment 1

Liu Leqi / 12011327

March 14, 2023

## 1 Q1

For shift cipher, there are only 26 possible keys. Here is the program to decrypt.

```python
c = 'gighsqv wg o dipzwq ibwjsfgwhm tcibrsr wb hvs zigv vwzzg ct bobgvob rwghfwqh gvsbnvsb wh wg kcfywbu hckofrg psqcawbu o kcfzr qzogg ibwjsfgwhm slqszzwbu wb wbhsfrwgqwdzwbofm fsgsofqv bifhifwbu wbbcjohwjs hozsbhg obr rszwjsfwbu bsk ybckzsrus hc hvs kcfzr'
for k in range(0, 27):
    m = f'{k} '
    for i in c:
        if i == ' ':
            m += i
            continue
        m += chr(ord('a') + (ord(i) - k) % 26)
    print(m)
```

With the key being **7**, the result is:
sustech is a public university founded in the lush hills of nanshan district shenzhen it is working towards becoming a world class university excelling in interdisciplinary research nurturing innovative talents and delivering new knowledge to the world

## 2 Q2

**Definition 1.6**
An encryption scheme $(Gen, Enc, Dec)$ with message space $\mathcal{M}$ and ciphertext space $C$ is perfectly secure if and only if for every two distinct plaintexts $\{x_0, x_1\} \in \mathcal{M}$, and for every strategy used by Eve, if we choose at random $b \in \{0,1\}$ and a random key $k \in \{0,1\}^n$, then the probability that Eve guesses $x_b$ after seeing the ciphertext $c = Enc_k(x_b)$ is at most $1/2$.
**Definition 1.7**
Two probability distributions $X, Y$ over $\{0,1\}^l$ are identical, denoted by $X \equiv Y$ , if for every $y \in \{0,1\}^l, Pr[X = y] = Pr[Y = y]$. An encryption scheme $(Gen, Enc, Dec)$ is perfectly secure if for every pair of plaintexts $x, x'$, we have $Enc_{U_n}(x) \equiv Enc_{U_n}(x')$.
The proof is as below.

- Definition 1.6 $\longrightarrow$ Definition 1.7
  Fix the plaintext space as $\mathcal{M} = \{x, x'\}$. For arbitrary $k \in \mathcal{K} = \{0,1\}^n$, let $c = Enc_k(x), c' = Enc_k(x')$. Suppose that

  $$\exists y \in C = \{0,1\}^l, Pr[c = y] \neq Pr[c' = y]$$

  Without loss of generality, assume $Pr[c = y] > Pr[c' = y]$. Since $Pr[c = y] + Pr[c' = y] = 1$, then $Pr[c = y] > \frac{1}{2}$.
  Construct an attacker Eve such that

  $$Eve(Enc_k(m)) = \begin{cases} x, & Pr[c = y] \\ x', & 1 - Pr[c = y] \end{cases}$$

  Since $Pr[Eve(Enc_k(m)) = x] = Pr[c = y] > \frac{1}{2}$, which contradicts the definition 1.6, then it must $Pr[c = y] = Pr[c' = y]$, i.e., $Enc_{U_n}(x) \equiv Enc_{U_n}(x')$.

- Definition 1.6 $\longrightarrow$ Definition 1.7
  Fix the plaintext space as $\mathcal{M} = \{x, x'\}$. For arbitrary $k \in \mathcal{K} = \{0,1\}^n$, let $c = Enc_k(x), c' = Enc_k(x')$. Suppose there exists an attacker Eve such that

$$Pr[Eve(Enc_k(x_b)) = x_b] > \frac{1}{2},\ x_b = x\ or\ x'$$

  Without loss of generality, let $Pr[Eve(Enc_k(x)) = x] > \frac{1}{2}$, then $Pr[Eve(Enc_k(x)) = x'] < \frac{1}{2}$ since $Pr[Eve(Enc_k(x)) = x] + Pr[Eve(Enc_k(x)) = x'] = 1$.
  Let

$$x'' = \begin{cases} x, & Eve(Enc_k(x)) = x \\ x', & Eve(Enc_k(x)) = x' \end{cases}$$

  Then without loss of generality, assume $Enc_k(x'') = c$. Since $Enc_k(x) = c, c \equiv c'$, then

$$Pr[Enc_k(c) = x''] = Pr[Enc_k(c) = x] > \frac{1}{2}$$

  However, since we have $Pr[Eve(Enc_k(x)) = x'] < \frac{1}{2}$ as assumption, contradicted.

Above all, definition 1.6 and 1.7 are equivalent.

# 3 Q3

1. It is NOT perfectly secure.
   Choose $k = 0$, then for every $m \in \mathbb{Z} = \{0, 1, \ldots, M-1\}$, the cipher text will be $c = (m+k) \mod M = m$, which leaks the message of plaintext.
2. It is NOT perfectly secure.
   Choose $k = 0$, then for every $m \in \mathbb{Z} = \{0, 1, \ldots, M-1\}$, the cipher text will be $c = (m+2k) \mod M = m$, which leaks the message of plaintext.

# 4 Q4

Suppose $Supp(X)$ is the support set of $Pr[X]$ over set $X$.

- "only if"
  For all $m \in Supp(M), c \in C$, we have

$$\begin{aligned} Pr[C = c|M = m] &= Pr[Enc_K(M) = c|M = m] \\ &= Pr[Enc_K(m) = c|M = m] \\ &= Pr[Enc_K(m) = c] \end{aligned}$$

  since $C = Enc_K(M)$ by definition (first equation), conditioning on $M = m$ (second equation), $K$ is independent of $M$ (third equation).
  By the Bayesian formula, we have

$$Pr[M = m|C = c]Pr[C = c] = Pr[C = c|M = m]Pr[M = m]$$

  If the scheme is perfectly secure, i.e., $Pr[M = m|C = c] = Pr[M = m]$, then $Pr[C = c|M = m] = Pr[C = c]$. Therefore, $\forall m, m' \in M, c \in C$, we have

$$\begin{aligned} Pr[End_K(m) = c] &= Pr[C = c|M = m] \\ &= Pr[C = c] \\ &= Pr[C = c|M = m'] \\ &= Pr[Enc_K(m') = c] \end{aligned}$$

- "if"
  Assume $Pr[M = m] = 0$, then we have $Pr[M = m|C = c] = Pr[M = m] = 0$.
  Assume $Pr[M = m] > 0$, then for $c \in C$, we have

$$\begin{aligned} Pr[C = c|M = m] &= Pr[Enc_K(M) = c|M = m] \\ &= Pr[Enc_K(m) = c|M = m] \\ &= Pr[Enc_K(m) = c] \\ &= Pr[Enc_K(m') = c] \\ &= Pr[C = c|M = m'] \end{aligned}$$

  Therefore, we have

$$\begin{aligned} Pr[C = c] &= \sum_{m' \in M} Pr[C = c|M = m']Pr[M = m'] \\ &= \sum_{m' \in M} Pr[Enc_K(m) = c]Pr[M = m'] \\ &= Pr[Enc_K(m) = c] \\ &= Pr[C = c|M = m] \end{aligned}$$

  Since $Pr[M = m] > 0$, by Bayesian formula, we have $Pr[M = m|C = c] = Pr[M = m]$.

# 5 Q5

- "only if":
  For a perfectly secure scheme $(Gen, Enc, Dec)$, we have

$$Pr[Eve(Enc_k(x)) = x] \leq \frac{1}{|M|}$$

  Choose a plaintext space $M$ with size $|M| = 3$, we have

$$Pr[Eve(Enc_k(x_i)) = x_i] \leq \frac{1}{3}$$

  where $i \in \{0, 1, 2\}$

- "if":
  To proof it, we can start from proving its contrapositive.

$$(Gen, Enc, Dec)\ is\ not\ perfectly\ secure \implies Pr[Eve(Enc_k(x_i)) = x_i] > \frac{1}{3}$$

  where $i \in \{0, 1, 2\}$. That is,

$$\exists M, Pr[Eve(Enc_k(x)) = x] > \frac{1}{|M|} \implies \exists M'\ with\ |M'| = 3, Pr[Eve(Enc_k(x_i)) = x_i] > \frac{1}{3}$$

  For $M' = \{x_0, x_1, x_2\}$, we can fix $x_0 = 0^l$, $x_1 = 1^m$ and $x_2 \leftarrow_R M'$. Then for random key $k \in \{0, 1\}^n$, we have

$$Pr[Eve(Enc_k(x_2) = x_2)] > \frac{1}{|M'|}$$

  Since $\forall k \in \{0, 1\}^n$, $x' = Eve(Enc_k(x_0))$ and $x'' = Eve(Enc_k(x_1))$ are fixed and independent with $x_2$. Then if we choose $x_2$ randomly from $M$, we have

$$Pr[Eve(Enc_k(x_0) = x_2)] \leq \frac{1}{|M'|}$$
$$Pr[Eve(Enc_k(x_1) = x_2)] \leq \frac{1}{|M'|}$$

Thus, $\exists x_2 \in M'$ such that

$$Pr[Eve(Enc_k(x_2) = x_2)] > Pr[Eve(Enc_k(x_0) = x_2)]$$
$$Pr[Eve(Enc_k(x_2) = x_2)] > Pr[Eve(Enc_k(x_1) = x_2)]$$

Denote that $p_{0,0} = Pr[Eve(Enc_k(x_0) = x_0)], p_{0,1} = Pr[Eve(Enc_k(x_0) = x_1)], p_{0,2} = Pr[Eve(Enc_k(x_0) = x_2)], p_{1,0} = Pr[Eve(Enc_k(x_1) = x_0)], p_{1,1} = Pr[Eve(Enc_k(x_1) = x_1)], p_{1,2} = Pr[Eve(Enc_k(x_1) = x_2)], p_{2,0} = Pr[Eve(Enc_k(x_2) = x_0)], p_{2,1} = Pr[Eve(Enc_k(x_2) = x_1)], p_{2,2} = Pr[Eve(Enc_k(x_2) = x_2)]$. Then for eavesdropper,

$$\begin{aligned} p_{0,0} + p_{0,1} + p_{0,2} &= 1 \qquad & p_{0,0} + p_{1,0} + p_{2,0} &= 1 \\ p_{1,0} + p_{1,1} + p_{1,2} &= 1 \qquad & p_{0,1} + p_{1,1} + p_{2,1} &= 1 \\ p_{2,0} + p_{2,1} + p_{2,2} &= 1 \qquad & p_{0,2} + p_{1,2} + p_{2,2} &= 1 \end{aligned}$$

With $p_{2,2} > p_{0,2}$ and $p_{2,2} > p_{1,2}$, we have $p_{2,2} > \frac{1}{3}, p_{0,2} < \frac{1}{3}, p_{1,2} < \frac{1}{3}$.
Construct a new eavesdropper Eve' as

$$Eve'(c) = \begin{cases} x_2 & if\ Eve(c) = x_2 \\ x_i, i \in \{0,1,2\}\ at\ random & otherwise \end{cases}$$

Since

$$\begin{aligned} Pr[Eve'(Enc_k(x_0)) = x_0] &= \frac{1}{3} \\ Pr[Eve'(Enc_k(x_1)) = x_1] &= \frac{1}{3} \\ Pr[Eve'(Enc_k(x_2)) = x_2] &\begin{cases} > \frac{1}{3} & if\ Eve(Enc_k(x_2)) = x_2 \\ = \frac{1}{3} & if\ Eve(Enc_k(x_2)) = x_0 \\ = \frac{1}{3} & if\ Eve(Enc_k(x_2)) = x_1 \end{cases} \end{aligned}$$

The expectation of $Pr[Eve'(Enc_k(x_i)) = x_i] > \frac{1}{3}, i \in \{0,1,2\}$.

# 6 Q6

The proof is as following:

- $\Delta(X,X) = 0, \forall X$
  By definition, we have

$$\Delta(X,X) = \max_{T \subseteq \{0,1\}^n} |Pr[X \in T] - Pr[X \in T]| = 0$$

- $\Delta(X,Y) = \Delta(Y,X), \forall X, Y$
  By definition, we have

$$\Delta(X,Y) = \max_{T \subseteq \{0,1\}^n} |Pr[X \in T] - Pr[Y \in T]| = \max_{T \subseteq \{0,1\}^n} |Pr[Y \in T] - Pr[X \in T]| = \Delta(Y,X)$$

- $\Delta(X,Z) \leq \Delta(X,Y) + \Delta(Y,Z), \forall X, Y, Z$
  By definition, we have

$$\begin{aligned} \Delta(X,Z) &= \max_{T \subseteq \{0,1\}^n} |Pr[X \in T] - Pr[Z \in T]| \\ &= \max_{T \subseteq \{0,1\}^n} |Pr[X \in T] - Pr[Y \in T] + Pr[Y \in T] - Pr[Z \in T]| \\ &\leq \max_{T \subseteq \{0,1\}^n} |Pr[X \in T] - Pr[Y \in T]| + \max_{T \subseteq \{0,1\}^n} |Pr[Y \in T] - Pr[Z \in T]| \\ &= \Delta(X,Y) + \Delta(Y,Z) \end{aligned}$$

# 7 Q7

To prove the computational indistinguishability is an equivalence relation, we need to show that it satisfies reflexivity, symmetry, transitivity.

- reflexivity:
  For every polynomial-time algorithm $A$, there is a negligible function $\epsilon$ such that

  $$|Pr[A(X_n) = 1] - Pr[A(X_n) = 1]| = 0 \leq \epsilon(n)$$

  Therefore, $X_n \approx X_n$.

- symmetry:
  If $X_n \approx Y_n$, then for every polynomial-time algorithm $A$, there is a negligible function $\epsilon$ such that

  $$\begin{aligned}&|Pr[A(X_n) = 1] - Pr[A(Y_n) = 1]| \\ &= |-Pr[A(Y_n) = 1] + Pr[A(X_n) = 1]| \\ &= |Pr[A(Y_n) = 1] - Pr[A(X_n) = 1]| \leq \epsilon(n)\end{aligned}$$

  Since $X_n \approx Y_n$ implies $|Pr[A(Y_n) = 1] - Pr[A(X_n) = 1]| \leq \epsilon(n)$, i.e., $Y_n \approx X_n$, it satisfies symmetry.

- transitivity:
  If $X_n \approx Y_n$ and $Y_n \approx Z_n$, then for every polynomial-time algorithm $A$, there is a negligible function $\epsilon$ such that

  $$\begin{aligned}&|Pr[A(X_n) = 1] - Pr[A(Z_n) = 1]| \\ &= |Pr[A(X_n) = 1] - Pr[A(Y_n) = 1] + Pr[A(Y_n) = 1] - Pr[A(Z_n) = 1]| \\ &\leq |Pr[A(X_n) = 1] - Pr[A(Y_n) = 1]| + |Pr[A(Y_n) = 1] - Pr[A(Z_n) = 1]| \\ &\leq \epsilon'(n) + \epsilon''(n)\end{aligned}$$

  Let $\epsilon(n) = \epsilon'(n) + \epsilon''(n)$, then we have $|Pr[A(X_n) = 1] - Pr[A(Z_n) = 1]| \leq \epsilon(n)$, i.e., $X_n \approx Z_n$.

Above all, the computational indistinguishability is an equivalence relation.