CS403 · Cryptography and Network Security

Assignment 1

Yubin Hu / 11712121

October 12, 2020

Q.1

Due to the shift-cipher's key is from 0 to 25, so we try all 26 keys. When the $key = 13$, we decrypt the cihertext:

"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."

Q.2

We prove that for every pair of plaintexts x, x', the probability that Eve guesses x_b after seeing the ciphertext $c = Enc_k(x_b)$ is at most $1/2$, if and only if we have $E_{U_n}(x) \equiv E_{U_n}(x')$.

"if" part

if $E_{U_n}(x) \equiv E_{U_n}(x')$, the Eve can not get any information and the probability is at most.

"only if" part

We prove by contrapositive. Suppose $\exists x_1, x_2$ such that $E_{U_n}(x_1) \not\equiv E_{U_n}(x_2)$ which means that there has a y_0 satisfied that $Pr[Y_{x_1} = y_0] > Pr[Y_{x_2} = y_0]$. So that Eve guesses x_1 if the ciphertext $y = y_0$, otherwise Eve guesses randomly. Then the probability is larger than $1/2$.

Q.3

"if" part

Suppose that $Pr[E_{nc_k}(m) = c] = Pr[E_{nc_k}(m') = c]$, we should prove that (Gen,Enc,Dec) with message space M is perfectly secure, which means:

$$Pr[M = m|C = c] = \frac{Pr[C = c|M = m] * Pr[M = m]}{\sum_{m' \in M} Pr[C = c|M = m'] * Pr[M = m']} = Pr[M = m]$$

$$Pr[C = c|M = m] * Pr[M = m] = \sum_{m' \in M} Pr[C = c|M = m'] * Pr[M = m']$$

Since $\forall m, m' \in M$, we have $Pr[C = c|M = m] = Pr[C = c|M = m']$, so that

$$\sum_{m' \in M} Pr[C = c|M = m'] * Pr[M = m'] = Pr[C = c|M = m'] * \sum_{m' \in M} Pr[M = m'] = Pr[C = c|M = m]$$

Above all, we complete the proof.

"only if" part

Suppose that (Gen,Enc,Dec) with message space M is perfectly secure. Fix arbitrary messages m, m' and ciphertext c, since it is perfectly secure,

$$\forall m \in M,\ Pr[M = m|C = c] = Pr[M = m]$$

So we have

$$Pr[E_{nc_k}(m) = c] = \frac{Pr[M = m|C = c] * Pr[C = c]}{Pr[M = m]} = Pr[C = c]$$

$$Pr[E_{nc_k}(m') = c] = \frac{Pr[M = m'|C = c] * Pr[C = c]}{Pr[M = m']} = Pr[C = c]$$

The resuly is nothing to do with m, $Pr[E_{nc_k}(m) = c] = Pr[E_{nc_k}(m') = c]$

Q.4

(1)

Yes. For every $m \in Z_M$, we have $Pr[E_k(m) = c] = \frac{|k \in Z_M : k + m \ mod \ M = c|}{|Z_M|} = \frac{1}{6}$. Due to an encryption scheme (Gen,Enc,Dec) with message space M is perfectly secure if and only if $Pr[E_{nc_k}(m) = c] = Pr[E_{nc_k}(m') = c]$, this encryption scheme is *perfectly secure*.

(2)

No. Let $m_1 = 1$, $m_2 = 0$, $c = 4$, $Pr[E_{nc_k}(m_1) = c] = 0$, $Pr[E_{nc_k}(m_2) = c] = \frac{1}{3}$, they go against *an encryption scheme (Gen,Enc,Dec) with message space M is perfectly secure if and only if* $Pr[E_{nc_k}(m) = c] = Pr[E_{nc_k}(m') = c]$, so this encryption scheme is not perfectly secure.

Q.5

for any two messages m_0, m_1, m_0 and m_1 agree on at least $l/2$ bits.. Suppose there is a new message m_2, m_2 and m_1 also agree on at least $l/2$ bits.

m_2 could be composed of the first half of m_0 and the second half of m_1. So that we have $E_{U_n}(m_0) \equiv E_{U_n}(m_1) \equiv E_{U_n}(m_2)$ which prove that any encryption scheme that is half-message perfectly secure must in fact also be perfectly secure.

Q.6

To prove that the statistical distance $\triangle(X, Y)$ defined in Definition 2.1 of Lecture 3 is a metric. We should prove:

(1) $\triangle(X, Y) = 0 \Leftrightarrow (X, Y)$

since

$$\triangle(X, Y) = max_{T \subseteq 0,1^n}$$

$$|Pr[X \in T] - Pr[Y|inT]| = 0$$

which means $t \in 0, 1^n$ and $Pr[X \in T] = Pr[Y|inT]$. Suppose $\forall t \in 0, 1^n$

$$Pr[X = t] = Pr[X \in t] = Pr[X \in t] = Pr[Y \in t] = Pr[Y = t]$$

So that $X = Y$

(2) $\triangle(X, Y) = \triangle(Y, X)$

since

$$\triangle(X, Y) = max_{T \subseteq 0,1^n}$$

so that

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

$$|Pr[Y \in T] - Pr[X|inT]| = \triangle(Y, X)$$

(3) $\triangle(X, Y) \leq \triangle(X, Z) + \triangle(Z, Y)$

$\triangle(X,Y) = \frac{1}{2}\sum_{w\in Supp(X)\cup Supp(Y)} |Pr[X=w]-Pr[Y=w]|$ So that:

$$\begin{aligned}
&\triangle(X,Z)+\triangle(Z,Y) \\
&\quad = \frac{1}{2}\sum_{w\in Supp(X)\cup Supp(Y)} |Pr[X=w]-Pr[Z=w]| + \frac{1}{2}\sum_{w\in Supp(X)\cup Supp(Y)} |Pr[Z=w]-Pr[Y=w]| \\
&\quad = \frac{1}{2}\sum_{w\in Supp(X)\cup Supp(Y)} (|Pr[X=w]-Pr[Z=w]| + |Pr[Z=w]-Pr[Y=w]|) \\
&\quad \geq \frac{1}{2}\sum_{w\in Supp(X)\cup Supp(Y)} (|Pr[X=w]-Pr[Z=w] + Pr[Z=w]-Pr[Y=w]|) \\
&\quad = \frac{1}{2}\sum_{w\in Supp(X)\cup Supp(Y)} (|Pr[X=w]-Pr[Y=w]|) \\
&\quad = \triangle(X,Y)
\end{aligned}$$

So the statistical distance $\triangle(X,Y)$ defined in Definition 2.1 of Lecture 3 is a metric.

Q.7

To prove that the computational indistinguishability $\approx$ defined above is an equivalence relation, we need to prove that $\approx$ is relexive, symmetric and transitive.

reflexive

$X_n \approx Y_n$ for any ϵ, $Pr[A(X_n)=1]-Pr[A(Y_n)=1] \leq \epsilon(n)$, whith means $X_n \approx X_n$

symmetric

If $X_n \approx Y_n$, $|Pr[A(X_n)=1]-Pr[A(Y_n)=1]| = |Pr[A(Y_n)=1]-Pr[A(X_n)=1]|$, whith means $X_n \approx X_n$

transitive

If $X_n \approx Y_n$ and $Y_n \approx Z_n$, for any ϵ, $Pr[A(X_n)=1]-Pr[A(Y_n)=1] \leq \epsilon(n)$, $Pr[A(Y_n)=1]-Pr[A(Z_n)=1] \leq \epsilon(n)$

$$\begin{aligned}
&Pr[A(X_n)=1]-Pr[A(Y_n)=1] \\
&\quad = Pr[A(X_n)=1]-Pr[A(Y_n)=1]+Pr[A(Y_n)=1]-Pr[A(Z_n)=1] \\
&\quad \leq |Pr[A(X_n)=1]-Pr[A(Y_n)=1]| + |Pr[A(Y_n)=1]-Pr[A(Z_n)=1]| \\
&\quad \leq 2\epsilon(n)
\end{aligned}$$