20161190 이민재

Q1. We already know that finding a collision on H can be done with $O(|T|^{\frac{1}{2}})$ by birthday paradox.

↳ Select two samples at M -> $O(n^2)$

hash collision => $O(\frac{1}{|T|})$

$H(x) = H(y) = H(z)$ mean $(H(x) = H(y)$ && $H(y) = H(z))$

So, this probability is $O\left(\frac{1}{|T|} \times \frac{1}{|T|}\right) = O\left(\frac{1}{|T|^2}\right)$

↳ select three samples at M -> $O(n^3)$

=> $O\left(\frac{n^3}{|T|^2}\right)$, we want this probability 1.

So the bound on n -> $O(|T|^{\frac{2}{3}})$

Q2.

a) $E_1(pk, m) = (E(pk, m), 0^{128})$

$$D_1(sk, (c_1, c_2)) = \begin{cases} D(sk, c_1) & \text{if } c_2 = 0^{128} \\ \perp & \text{otherwise} \end{cases}$$

This is chosen chipher text secure.

Because at this system,

$Adv_{cca}[AE] = |Pr[exp(0)=1] - Pr[exp(1)=1]|$

is negligible

-> back page continue

b) $E_2(pk, m) = (c_1, c_2)$ for $c_1, c_2 \leftarrow E(pk, m)$

$D_2(sk, (c_1, c_2)) = D(sk, c_1)$

$\Rightarrow$ This is not chosen - ciphertext secure.

attacker use $m_1 = 0^{128}$, $m_2 = 1^{128}$ and can get

get (C_1, C_2). and ask the value of decreption

$(C_1, E(pk, 0^{128}))$ and be given in respone m_0 or m_1.

Then the attacker win (not secure)

c) $E_3(pk, m) = (E(pk, m), E(pk, 0^{128}))$

$D_3(sk, (C_1, C_2)) = \begin{cases} D(sk, c_1) & \text{if } D(sk, c_2) = 0^{128} \\ \perp & \text{otherwise} \end{cases}$

$\Rightarrow$ This is not chosen - chiphertext secure.

attacker use $m_0 = 0^{128}$, $m_1 = 1^{128}$ and can get (C_1, C_2).

attacker ask the value of decretion $(C_1, E(pk, 0^{128}))$

and be given in respone m_0 or m_1

Then the attacker win (not secure)

$\therefore$ Anser is a

3, Let's assume A and B want to know S.
They have relatively prime r_1, r_2.
(The theorem Given $a, b \in \mathbb{Z}$, at least one of them non zero $\exists$ x and $b \in \mathbb{Z}$, such that $\gcd(a, b) = ax + bb$)

So we can say $ar_1 + br_2 = 1$ there are $\exists a, b \in \mathbb{Z}$,
and they can also compute a, b by Extend Euclid Algorithm

$$S_1^a \cdot S_2^b \equiv S^{ar_1} \times S^{br_2} \equiv S^{ar_1 + br_2} \equiv S \mod N$$

$\therefore$ A, B can get S, so this system is terribly insecure

4) Summerize situation
$pk = (g, g^x = h)$, $SK = (g, x)$
$Enc(sk, m) = g^r, m \times h^r$
$$Dec(pk, (c_0, c_1)) = \frac{c_1}{c_0^x} = \frac{m \times h^r}{g^{rx}} = \frac{m \times h^r}{(g^x)^r} = \frac{m \times h^r}{h^r} = m$$

CCS $\Rightarrow$ using $\begin{cases} m_1 \Rightarrow \text{can get } c_1, c_2 \ (g^{r_1}, m_1 h^{r_1}) \\ m_2 \Rightarrow \text{can get } c_3, c_4 \ (g^{r_2}, m_2 h^{r_2}) \end{cases}$

$C_1 \times C_3 = g^{r_1 + r_2}$, $C_2 \times C_4 = m_1 m_2 h^{r_1 + r_2}$
$Enc(sk, m_1 m_2) = (g^r, m_1 m_2 h^r) = (C_1 C_3, C_2 C_4)$

So, this is not chosen chipher secure

5)

If the value of ($K == W \oplus T$), then they have same key

$$W \oplus T = U \oplus R \oplus T = S \oplus T \oplus R \oplus T$$

$$= K \oplus \cancel{R} \oplus \cancel{T} \oplus \cancel{R} \oplus \cancel{T} = K$$

$\therefore$ $W \oplus T = K$, so they have the same key.

But this is not secure. Adversary can intercept (S, U, W) while Alice and Bob are exchange (S, U, W)

And Adversery can compute

$$S \oplus U \oplus W = K \oplus \cancel{r} \oplus \cancel{K} \oplus \cancel{r} \oplus \cancel{t} \oplus \cancel{K} \oplus \cancel{r} \oplus \cancel{t} \oplus \cancel{r}$$

$$= K$$

At the security game, adversary has $S \oplus U \oplus W$.

If get K from challenger and $K = (S \oplus U \oplus W)$

then adversary say $b = 0$. otherwise say $b = 1$.

This system, adversary win the game except $b = 1$ and uniform random key same with real key

So adversary win probability

$= 1 - Pr(\text{lose}) = 1 - (b=1 \text{ and match key with real key})$

$= 1 - \frac{1}{2} \times \frac{1}{2^n} = 1 - \frac{1}{2^{n+1}}$ our case is $n = 256$

(also 2^{n+1} is exponent so this is negligible)

So, this crypto system is insecure !