2016 11월 01일 21시

Problem 1

"If for any efficient stat. test A, $Adv_{PRG_n}[A,G]$ is negligible", then $G: K = \{0,1\}^s \rightarrow \{0,1\}^n$ is a secure PRG

- $G_1(k) = G(k) \oplus 1^n$ is Secure PRG

$\Rightarrow Adv_{PRG}[A,G] = \left| \Pr_{k \xleftarrow{R} \{0,1\}^s}[A(G(k))=1] - \Pr_{r \xleftarrow{R} \{0,1\}^n}[A(r)=1] \right|$

$= \left| \frac{1}{2} - \frac{1}{2} \right| = 0$ (negligible)

- $G_2(k) = G(k_1) \| G(k_2)$ is Secure PRG

$\Rightarrow Adv_{PRG}[A, G_2] \Rightarrow$ negligible

- $G_3(k) = G(k) \| G(k)$ is not Secure PRG

$\Rightarrow Adv_{PRG}[A, G_3] \Rightarrow$ not negligible

- $G_4(k) = G(k) \| 0$ is not Secure PRG

$\Rightarrow Adv_{PRG}[A, G_4] \Rightarrow$ not negligible

- $G_5(k) = rev(G(k))$ is Secure PRG

$\Rightarrow Adv_{PRG}[A, G_5] \Rightarrow$ negligible

Problem 2

Def (E,D) is semantically secure if for all efficient adversary A, $Adv_{ss}[A,E]$ is negligible.

$$Adv_{ss}[A,E] = \left| Pr[A(E(k,m_0))=1] - Pr[A(E(k,m_1))=1] \right|$$

=> E_2 => by asking for the encryption of 0^n and $0^{n-1}1$ attacker can distinguish and get hint.

=> E_3 => attacker know the secret key because ciphertext inform the s-key

=> E_4 => by asking for the encryption of 0^n and 1^n, attacker can know the secret key 0^n

∴ E_1 is semantically secure

($Adv_{ss}[A,E_1]$ is negligible)

Problem 3

Fix an int $\ell > 0$. $\mathcal{M}, \mathcal{K}, \mathcal{C}$ space are equal to $\{0,1\}^{\ell}$

- Gen : choose a key from $\mathcal{K} = \{0,1\}^{\ell}$
  (chosen as the key with probability exactly $\frac{1}{2^{\ell}}$)
- Enc : $k, m \in \{0,1\}^{\ell}$, $c := k \oplus m$
- Dec : $k, c \in \{0,1\}^{\ell}$, $m := k \oplus c$

(Enc(k, m) = c satisfy k value is only one.)

At the one-time pad

$$\Pr[C=c \mid M=m] = \Pr[k \oplus m = c \mid M=m]$$
$$= \Pr[K = m \oplus c \mid M=m] = \frac{1}{2^{\ell}}$$

We can see that for any $c \in \mathcal{C}$,

$$\Pr[C=c] = \sum_{m \in \mathcal{M}} \Pr[C=c \mid M=m] \times \Pr[M=m]$$
$$= 2^{-\ell} \times \sum_{m \in \mathcal{M}} \Pr[M=m] = 2^{-\ell}$$

where the sum is over $m \in \mathcal{M}$ with $\Pr[M=m] \neq 0$.

by the Bayes theorem,

$$\Pr[M=m \mid C=c] = \frac{\Pr[C=c \mid M=m] \cdot \Pr[M=m]}{\Pr[C=c]}$$
$$= \frac{\frac{1}{2^{\ell}} \times \Pr[M=m]}{\frac{1}{2^{\ell}}} = \Pr[M=m]$$

If attacker get C, and he doesn't know this C Come from m_1 or m_2. Probability is same

⇒ OTP is perfect secrety (Ciphertext only attack is useless)

Problem 4

$$Adv_{PRG}[A, H] = \left| Pr[A(H(k)) = 1] - Pr[A(r) = 1] \right|$$

a	b	a ∨ b
0	0	0
0	1	1
1	0	1
1	1	1

$$Pr[A(a \vee b) = 1] = \frac{3}{4}$$

$$\therefore \text{Advantage} = \left| \frac{3}{4} - \frac{1}{2} \right| = \frac{1}{4}$$

Problem 5

PRF is secure if a random function in Funs[X,Y] is indistinguishable from a random function in S_F.

if $Adv_{PRF}(A,F) = \left| \Pr_{k \leftarrow K}[A(F(k,x))=1] - \Pr_{f \leftarrow Funs[X,Y]}[A(f(x))=1] \right|$

is negligible => Indistinguishable

not negligible => distinguishable

- $F_1(k,x) = F(k,x)[0,\dots,n-2]$ => Secure PRF

=> advantage is negligible (indistinguishable)

- $F_2(k,x) = F(k,x) \| 0$ => not secure

=> advantage is not negligible (distinguishable)

the last bit is always 0, the string has not same probability

$\Pr[A(f(x))=1]$

- $F_3((k_1,k_2),x) = F(k_1,x) \| F(k_2,x)$ => Secure PRF

=> advantage is negligible (indistinguishable)

(string1 + string2)'s bits are also random that mean

($\Pr[A(F(k,x))=1 = \Pr[A(f(x))=1]$)

- $F_4(k,x) = \begin{cases} F(k,x) & \text{if } x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$ => not secure

=> advantage is not negligible (distinguishable)

attacker can send 0^n so the value

$\Pr[A(F(k,x))=1 \neq \Pr[A(f(x))=1]$

Problem 6

Yes! G is a secure PRG.

$F: K \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF.

$G(k) = \underbrace{F(k,0)}_{n} \| \underbrace{F(k,1)}_{n} \| \cdots \| \underbrace{F(k,t)}_{n} \Rightarrow \{0,1\}^{nt}$

$G(k) = F(0) \| F(1) \| \cdots \| F(k)$ (→ random, → independent random) ⇒ output is truly random

[paused random $G(k) = F(k,0) \| F(k,1) \| \cdots \| F(k,t)$

⇒ Output is random

that mean $F(k,\cdot)$ is indistinguishable from truly random function $f(\cdot)$.

∴ G is a secure PRG

Problem 7

64 bit 56 bit 64 bit

$$DES\text{-}X(m) := K_2 \oplus Enc(K, m \oplus K_1)$$

$\therefore$ DES key size $56 + (64 \times 2) = 184$ bits

$$DES\text{-}X : \{0,1\}^{184} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$$

$$\Rightarrow (DES\text{-}X)^{-1}(K, K_1, K_2, C) = K_1 \oplus DES^{-1}(K, K_2 \oplus C)$$

* meet in the middle attack (broke 2 DES)

$C_1 = DES(K_2, DES(K_1, M_1)) \Rightarrow DES^{-1}(K_2, C_1) = DES(K_1, M_1)$

This mean $C = E(K_1, (E(K_2, m)))$ is equivalent to

$D(K_1, C) = E(K_2, m)$

There is a meet in the middle attack on DES-X. It finds a 184-bit DES-X key using 2^{120} DES and DES^{-1} computations. So the effective key length of DES-X seems to be 120, which is large enough for security.