TD 1

Wednesday, September 24, 2025 15:52

Problem 1 ***PRGs with Non-Uniform Seeds***

Consider a secure PRG $\mathbf{G}: \{0,1\}^\lambda \to \{0,1\}^n$.

1. Starting from $\mathbf{G}$ and splitting $k = (k_1, k_2) \in \{0,1\}^\lambda \times \{0,1\}^m$, construct the new PRG $\mathbf{G}'$: $\{0,1\}^{\lambda+m} \to \{0,1\}^{n+m}$ as

$$\mathbf{G}'(k = (k_1, k_2)) = \mathbf{G}(k_1) || k_2,$$

where $||$ denotes concatenation. Show that the new PRG $\mathbf{G}'$ is also secure.

2. Define yet another PRG $\mathbf{G}''$: $\{0,1\}^\lambda \to \{0,1\}^m$ for $m > n$:

$$\mathbf{G}''(k) = \mathbf{G}(k) || 0^{m-n}.$$

Is this PRG secure?

3. Is the PRG $\mathbf{G}'$ secure if the key k is chosen uniformly at random over all length-λ bit-strings with last bit 0?

1) $Adv_A(G') = | P(A(G'(k_1, k_2)) = 1) - P(A(B_1 || B_2) = 1) |$

$= | \sum_{k_2} P(K_2 = k_2) \cdot P(A(G(K_1) || k_2)) = 1 - \sum_{k_2} P(K_2 = k_2) \cdot P(A(B_1 || k_2) = 1) |$

△ ineq. $\leq \sum_{k_2} P(K_2 = k_2) \, | P(A(G(K_1) || k_2) = 1) - P(A(B_1 || k_2) = 1) |$

$= \sum P(K_2 = k_2) \, Adv_{A_{k_2}}(G)$ ← k_2 is constant here

$\leq \varepsilon(\lambda)$

2) let the adversary A decides

1 if last m-n bits are 0

0 otherwise

$Adv(A, G'') = |1 - \frac{1}{2^{m-n}}|$ not negligible

3)

Problem 2 **Encryption Chain**

Problem 2 *Encryption Chain*

Consider the perfectly secure cipher $(\mathbf{E}, \mathbf{D})$ and construct the new cipher $(\mathbf{E}', \mathbf{D}')$ where

$$\mathbf{E}'(k = (k_1, k_2), m) = (\mathbf{E}(k_1, k_2), \mathbf{E}(k_2, m)).$$

Show that this new cipher is perfectly secure. (See Shannon's definition of perfect secrecy.)

We would like $m \perp\!\!\!\perp C$

$$I(M; (E(K_1,K_2), E(K_2,m)))$$

$$= I(M; E(K_2,m)) + I(m; E(K_1,K_2) \mid E(K_2,m))$$

$= 0$ since E perfect

$$= H(E(K_1,K_2) \mid E(K_2,m)) - H(E(K_1,K_2) \mid E(K_2,m), m)$$

$$\leq H(E(K_1,K_2)) - H(E(K_1,K_2) \mid E(K_2,m), m)$$

$$= I(E(K_1,K_2); E(K_2,m), m)$$

$$\leq I(E(K_1,K_2); m, K_2)$$ Data processing Inequality

$= 0$ since perfect

$$= I(E(K_1,K_2); K_2) + I(E(K_1,K_2); m \mid K_2)$$

$= 0$

$K_1 \perp\!\!\!\perp m$, $K_2 \perp\!\!\!\perp m$ $\Rightarrow E(K_1,K_2) \perp\!\!\!\perp m$

Problem 3 *A Secure PRG from a Secure PRF*

Consider a secure PRF $\mathbf{F}: \mathcal{K} \times \{1, \ldots, t\} \to \{0,1\}^n$ and construct the PRG $\mathbf{G}: \mathcal{K} \to \{0,1\}^{nt}$ as

$$\mathbf{G}(k) = \mathbf{F}(k,1) \,||\, \mathbf{F}(k,2) \,||\, \mathbf{F}(k,3) \,||\, \cdots \,||\, \mathbf{F}(k,t).$$

Show that the PRG $\mathbf{G}$ is secure.

Assume the adversary against G

A with advantage as follows

$$Adv(A, G) = |Pr(A(F(K,1)||\ldots||F(K,t)) = 1) - Pr(A(B^{nt}) = 1)|$$

Suppose an adversary B against F

that takes 1...t for the query and get F(K,1)... F(K,t)

—

Since F is secure,

$$Adv(B,F) = \left| Pr(B(F(k,1)\| \cdots \|F(k,t)) = 1) - Pr(B(u^{nt}) = 1) \right| \leq \varepsilon \text{ negligible}$$

trivially $Adv(A,G) = Adv(B,F) \leq \varepsilon$

∎

Problem 4 ***Fragments of Keys***

1. Consider a situation where two users A_1 and A_2 should be able to decrypt a OTP ciphertext, but no single user on its own can learn any information about the key or the plaintext. How would you distribute the key k among the two users?
2. Consider now a situation with three users A_1, A_2 and A_3. We would like that any pair of users can decrypt the ciphertext but no single user can learn any information about the key or the plaintext. How do you distribute the key now?
3. Consider finally a situation with τ users $A_1, \ldots, A_\tau$. As before, we would like that any pair of users can decrypt the ciphertext, but no single user on its own can learn any information about the plaintext or the key. How do you distribute the key among the users?

1) Let $K = k_1 \oplus k_2$ be the decryption key
assign k_i to A_i respectively

2) Let $K = k_1 \oplus k_2 \oplus k_3$ be the key
assign all k_i to A_j where $i \neq j$
any two users should have
4 sub-keys with one being duplicate
XOR the non-duplicates gives the K

3) similar to 2) but $K = \sum_{i=1}^{\tau} k_i$
where Σ denotes the bitwise summation
(XOR essentially)

Problem 5 ***Security of RC4***

Consider the PRG of the RC4 stream cipher introduced by Ron Rivest in 1987. It is based on a 256 bytes array S and two single-byte pointers i and j. The seed (key) k is used to initialize the array S by means of a given Pseudo-Random Permutation on the set $\{0, 1, \ldots, 255\}$. The outputs of the RC4 PRG are obtained as described in the following algorithm:

Algorithm 1 Outputs of RC4 PRG

```
i ← 0; j ← 0
repeat
  i ← (i + 1) mod 256
  j ← (j + S[i]) mod 256
  swap( S[i] ; S[j] )
  output S( (S[i] + S[j]) mod 256 )
until forever
```

1. What key size (seed length) would be required to start the array S with a truly random permutation of the numbers $\{0, 1, \ldots, 255\}$? (The actual key size of RC4 is typically $40 - 128$ bits.)
2. Assume that after the initialization the second entry of array S, called $S(2)$, equals 0. Calculate

2. Assume that after the initialization the second entry of array S, called $S(2)$ equals 0. Calculate the first and the second output bytes, z_1 and z_2, of the RC4 PRG.

3. Answer the following questions assuming that the initialization of the array S has been performed by means of a truly random permutation.

   (a) What is the joint probability that $S(2) = 0$ after the initialization and $z_2 = 0$.

   (b) You can assume that when $S(2) \neq 0$ after the initialization, then the RC4 PRG produces $z_2 = 0$ with a probability $\approx \frac{1}{n}$. Use this result, to approximate the probability $\Pr[z_2 = 0]$.

   (c) Is the RC4 PRG secure assuming that the initial permutation is truly random? If the PRG is not secure, describe an adversary and its (approximated) nonnegligible advantage.

1) Truly random permutation 256!

$\Rightarrow \log_2 256! \approx 256 \lg_2 256$

$= 256 \times 8 = 2048$

2) first iteration

$i=0 \quad j=0$

$i=1, j = S^0[1] \bmod 256 \triangleq a$

denote $S^0[a] = b$ then

$S^1[1] = b \quad S^1[a] = a$

output $S^1(b+a \bmod 256)$

$= \begin{cases} a & \text{if } (a+b) \bmod 256 = a \\ b & \text{if } (a+b) \bmod 256 = 1 \\ S^0((a+b) \bmod 256) & \text{else} \end{cases}$

S^k denotes the array at k-th iteration

if $a \neq 2$, then $S^1[2]$ remains unchanged

if $S^0[1] = a = 2$ then

$b = S^0[2] = 0, \quad S^1[2] = 2$

second iteration

$i=2 \quad j = (a + S^1[2]) \bmod 256 = \begin{cases} a & \text{if } a \neq 2 \\ 4 & \text{if } a = 2 \end{cases}$

if $a \neq 2$

$S^2[2] = S^1[a] = a$

$S^2[a] = S^1[2] = 0$

output $S^2(a \bmod 256) = 0$

if $a = 2$

$S[2] = S[4] = S[4]$ (since $i+j \bmod 256 \neq 4$, $S'[4]$ cannot be modified)

$S^2[4] = S'[2] = 2$

Output $S^2((2+S^0[4]) \bmod 256)$

3). $\mathbb{P}(S^0[2]=0 \wedge Z_2=0) = \underbrace{\mathbb{P}(S^0[2]=0)}_{=\frac{1}{256}} \cdot \mathbb{P}(Z_2=0 \mid S^0[2]=0)$

$\mathbb{P}(Z_2=0 \mid S^0[2]=0)$ can be evaluated w.l 2)

if $a \neq 2$, with probability $\mathbb{P}(a \neq 2) = \frac{254}{255}$

$P(Z_2=0 \mid a \neq 2 \wedge S^0[2]=0) = 1$

if $a = 2$. w.l prob. $\mathbb{P}(a=2) = \frac{1}{255}$

$Z_2 = 0$ iff $S^2(c) = 0$

in the second iteration, only $S(2)$ & $S(4)$ are changed and both of them are not 0

$\Rightarrow S^2(c) = 0 \iff S^1(c) = 0 \Rightarrow c = 1$

$\Rightarrow 2 + S^0[4] \equiv 1 \bmod 256 \Rightarrow S^0[4] = 255$

$\Rightarrow \mathbb{P}(Z_2=0 \mid a=2 \wedge S^0[2]=0)$

$= \mathbb{P}(S^0[4] \mid a=2 \wedge S^0[2]=0) = \frac{1}{254}$

with the law of total probability

$P(Z_2=2 \mid S^0[2]=0) = \frac{254}{255} \times 1 + \frac{1}{255} \times \frac{1}{254}$

$$\Rightarrow \mathbb{P}(Z_2 = 2 \wedge S^0[2] = 0) = \frac{1}{256} \cdot \frac{254}{255} + \frac{253!}{256!}$$

b) $\mathbb{P}(Z_2 = 0 \mid S^0[2] = 0) = \frac{(n-2)^2+1}{(n-1)(n-2)}$ from above

$$\mathbb{P}(S^0[2] = 0) = \frac{1}{n} \quad \mathbb{P}(S^0[2] \neq 0) = \frac{n-1}{n}$$

$$\mathbb{P}(Z_2 = 0 \mid S^0[2] \neq 0) \approx \frac{1}{n}$$

$$\mathbb{P}(Z_2 = 0) = \mathbb{P}[Z_2 = 0 \mid S(2) = 0) \cdot \mathbb{P}(S(2) = 0)$$
$$+ \mathbb{P}(Z_2 = 0 \mid S(2) \neq 0) \cdot \mathbb{P}(S(2) \neq 0)$$
$$\approx \frac{(n-2)^2+1}{n(n-1)(n-2)} + \frac{n-1}{n^2}$$
$$= \frac{n((n-2)^2+1) + (n-1)^2(n-2)}{n^2(n-1)(n-2)} - \frac{1}{n}$$
$$(<) \approx \frac{n(n-2) + (n-1)^2}{n^2(n-1)}$$
$$(<) \approx \frac{2n-1}{n^2} \approx \frac{2}{n}$$

c) No. consider the adversary

$$A(g) = \begin{cases} 1 & \text{if } z_2 = 0 \\ 0 & \text{else} \end{cases}$$

$$Adv(A) = |\mathbb{P}(A(G_{RC4}) = 1) - \mathbb{P}(A(B_R) = 1)|$$
$$\approx \left| \frac{2n-1}{n^2} - \frac{1}{n} \right| = \left| \frac{n-1}{n^2} \right| \approx \frac{1}{n}$$

not negligible unless n is very large