Shan Yitian

2021180022

Assignment 2

Submission Deadline: 2021.9.29, 12:00pm

1. Let $G: \{0,1\}^s \rightarrow \{0,1\}^n$ be a secure PRG. Which of the following is a secure PRG (could be more than one), and give your explanation.

✓ $G'(k_1, k_2) = G(k_1)||G(k_2)$ Because random|| random still random

$G'(k) = G(0)$ Because "0" is certain that is not random

✓ $G'(k) = G(k)$ Because $G(k)$ is a secure PRG.

$G'(k) = G(k)||0$ The attacker knows the LSB is either 1 or 0, which is not secure.

✓ $G'(k) = G(k \oplus 1^s)$ $\because k \xleftarrow{\$} K$ $\therefore k \oplus 1^s$ is Random $\therefore G(k \oplus 1^s)$ is secure

✓ $G'(k) = reserver(G(k))$, where reverse(x) reverses the string x so that the first bit of x is the last bit of reverse(x) and so on.

Obviously, if $G(k)$ is random, the reverse$(G(k))$ is random.

2. Let $G: K \rightarrow \{0,1\}^n$ be a secure PRG. Define $G'(k_1, k_2) = G(k_1) \wedge G(k_2)$ where $\wedge$ is the **bit-wise AND function**. Consider the following statistical test A on $\{0,1\}^n$. A(x) outputs LSB(x), the least significant bit of x. What is the Adv_{PRG}[A, G']? You may assume that LSB(G(k)) is 0 for exactly half the seeds k in K.

We can know $Pr[LSB(G(k))=0] = 0.5 = Pr[LSB(G(k))=1]$

So, $Pr[LSB(G'(k_1,k_2))=1] = 0.5 \times 0.5 = 0.25$

Then $Adv_{ss}[A, G'] = |Pr[Exp(0)=1] - Pr[Exp(1)=1]| = 0.25 - 0 = 0.25$

3. Let (E, D) be a one-time semantically secure cipher where the message and ciphertext space is $\{0,1\}^n$. Which of the following encryption scheme are semantically secure? Give your explanation for each of the options.

✓ 1) $E'((k, k'), m) = E(k, m)||E(k', m)$

2) $E'(k, m) = E(0^n, m)$

✓ 3) $E'(k, m) = E(k, m)||k$

4) $E'(k, m) = E(k, m)||LSB(m)$

The attrack can distinguish Exp(0) from Exp(1) in (2) and (4), but they can't.

4. Suppose you are told that the one time pad encryption of the message "attack at dawn" is 6c73d5240a948c86981bc294814d (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key?

attack at dawn

⊕ 6c73d5240a948c86981bc294814d

⊕ attack at dusk

6c73d5240a948c86981bc2808548l