COMPUTATIONAL SECURITY, PSEUDORANDOM GENERATORS

ABHAY SHANKAR K: CS21BTECH11001

1. Computational Security

Computational Security: A scheme $\Pi = (Gen, Enc, Dec)$ is (t, ϵ) secure if an adversary can find information about m from c using time t (not really time, think big-O) with prob. of correctness $\geq \epsilon$

A maxim:

$$(1-\epsilon)^{\frac{3}{\epsilon}} \approx \exp -3 < 0.1$$

Thus, adversary can guess the key with probability 0.9 in time $\frac{3}{\epsilon}$

Probabilistic Polynomial time: An algorithm A is said to run in PPT if its runtime $\leq p(n)$ for some polynomial p, with input size n.

Security, again: Indistinguishability expt with 2 choices:

- Adversary is efficient
- Probability of success (as defined before) $\leq 0.5 + negl()$

Indistinguishability: AKA Semantic Security

Π is indistinguishable if an efficient adversary cannot predict a message, given the ciphertext, non-negligibly better than random, i.e. above defn.

2. Pseudo-RNG

Seed: $s \in \{0,1\}^n$ where n is smol

Generating function: $G : \{0,1\}^n \to \{0,1\}$

where G is deterministic.

Unpredictable PRG: Upon observing $\{x_1, \ldots, x_n\}$, we cannot predict x_{n+1} (with probability > 0.5)

Common PRG:

- *LFSR*: $x_i = x_{i-1} \oplus x_{i-4}$

  Generalising, with the LFSR sequence $l = \{l_1, \ldots, l_k\}$, $x_i = \bigoplus_{q \in l} x_{i-q}$

3. Problems

(1) $M = C = \{0,1\}^2$

$K = \{01, 10, 11\}$

Let the adversarial messages be $m_0 = 00, m_1 = 11$. Then,

- $Enc(m_0, 01) = 01$: Guess
- $Enc(m_0, 10) = 10$: Guess
- $Enc(m_0, 11) = 11$: Predict m_0
- $Enc(m_1, 01) = 10$: Guess
- $Enc(m_1, 10) = 01$: Guess
- $Enc(m_1, 11) = 00$: Predict m_1

Clearly, the probability of guessing correctly would be $\frac{2}{3}$

Negligible function: $f(n)$ is negligible if

$$\lim_{n\to\infty} f(n) \leq \frac{1}{g(n)} \forall \text{ polynomials } g$$

We would aim to make ϵ - the probability of guessing the key - a negligible function.