PERFECT SECURITY, ONE-TIME PAD, ETC.

ABHAY SHANKAR K: CS21BTECH11001

1. Recap

Perfect Security: We say that given $\Pi = (Gen, Enc, Dec)$, $\forall c \in C$, $\forall m \in M$, with X as a random variable over M and Y over C,

$$P(X = m|Y = c) = P(X = m)$$

Def 2: $\forall m_0, m_1 \in M$, $c \in C$,

$$P(Enc(m_0, k) = c) = P(Enc(m_1, k) = c)$$

Def 3: Perfect Adversarial Indistinguishability:

- Adversary picks message randomly from $\{m_0, m_1\}$, sends to Alice.
- Alice encrypts, sends it back.
- Adversary guesses.

With $b \in \{0, 1\}$, $c = Enc(m_b, k)$, and the adversary guesses $b' \in \{0, 1\}$,

$$P(b = b') = 0.5$$

One-Time Pad: K = M = C = $\{0, 1\}^n$

$$c = m \oplus k$$

Issues:

- len(k) = len(m)
- The key cannot be reused.

2. Today

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 $\geq \epsilon$

3. Problems

(1) Prove OTP is PS with Def 2 To prove: $P(Enc(m_0, k) = c) = P(Enc(m_1, k) = c)$ where C = M = K = $\{0, 1\}^n$

$$\begin{aligned} &P(Enc(m_0, k) = c) \\ &= P(m_0 \oplus k = c) \\ &= P(k = c \oplus m_0) \\ &= \frac{1}{2^n} \end{aligned}$$

(2) Prove OTP is PS with Def 3