Lecture 05 ()

1. Students will be given chits
2. Need to write about what is not clear
3. Summarize the lecture

1 Solution for Q04.02

Solve using contrapositive. Let us assume that there is an adversary A that can break E'. We now construct B that breaks E.

Algorithm:

1. B forwards m_0, m_1 received from A
2. B then sends (ct, ct) to A
3. B returns output of b received from A

Above approach won't work (think why)

1.1 Hint

Construct two worlds:

1. World 0 - challenger encrypts m_0
2. World 1 - challenger encrypts m_1

Claim: Adversary won't behave differently in the two worlds

2 Construction for Secure Encryption Schemes - Examples

$$K = \{0,1\}^n, M = \{0,1\}^l, l > n$$

$$enc(m,k) = m \oplus G(k)$$

G is a public function which is efficiently computable

2.1 Examples of G

1. $G(s) = ss$

2. $G(s)$: xor of bits of $G(s) = 0$

Both can be broken with $m_0 = 0 \dots 0, m_1 = 0 \dots 01$. Therefore, if output of G is sufficiently different from random, then encryption breaks.

2.2 Formulating 'Looks Random' using Game

1. Challenger chooses a bit b, s, $u_0 = G(s)$, $u_1 = U$
2. Adversary guesses b

2.3 What are some Attacks on E_G

1. Malleability
2. Using the key multiple times

3 Issues with using Time in the Key

The keys are not independent, therefore, can be broken