CS:6160 CRYPTOLOGY

PRACTICE QUESTIONS
LECTURE 2

Instructions

- Try these questions before class. Do not submit!
- We will discuss the solutions on Thursday August 26, 2021

(1) Consider an encryption scheme (Gen, Enc, Dec) where for any two messages $m, m^{'} \in \mathcal{M}$ the distribution of the ciphertext when m is encrypted is identical to the distribution of the ciphertext when $m^{'}$ is encrypted. i.e.

$$Pr[Enc_K(m) = c] = Pr[Enc_K(m^{'}) = c], \forall c \in \mathcal{C}$$

The encryption scheme is said to have *perfect indistinguishability.*
Q: Show that an encryption scheme has perfect indistinguishability if and only if an encryption scheme is perfectly secret.

(2) Is the One Time Pad secure against chosen ciphertext attack?

(3) You have a randomly chosen key k of length n and a message m of length $n-2$ to be encrypted. You come up with the following encryption scheme:

$$Enc_k(m) = k \oplus (01 \circ m), m \in \{0,1\}^{n-2}, k \in \{0,1\}^n,$$

where $\circ$ is the concatenation operator. That is, 01 is appended to m in the beginning to get a string of length n. Does this scheme provide perfect secrecy?

(4) You have a mechanism to generate random keys of length k and l s.t. $k + l = n - 1$. The message you want to encrypt is of length n. To encrypt this message you come with the following scheme:

$Enc_{k_1,k_2}(m) = (k_1 \circ 1 \circ k_2) \oplus m, m \in \{0,1\}^n, k_1 \in \{0,1\}^k, k_2 \in \{0,1\}^l.$

Does this scheme provide perfect secrecy?

AUGUST 26, 2021 ; DEPT OF CSE, IIT HYDERABAD