

Assignment II: Symmetric Key Encryption

Deadline: **24/09/2022**

IAI, TCG CREST

1. Let F be a secure PRF defined over $(\{0, 1\}^n, \{0, 1\}^n, \{0, 1\}^n)$.
 - (a) Prove that $G_k(x) := F_k(x) \oplus x$ is a secure PRF.
 - (b) Prove that $G_{(k,k')}(x) := F_k(x) \oplus F_{k'}(x)$ is a secure PRF.
 - (c) Show that $G_k(x) := F_k(x) \| F_k(F_k(x))$ is insecure.
2. Prove that if F is a pseudorandom function defined over $(\{0, 1\}^n, \{0, 1\}^n, \{0, 1\}^n)$, then

$$G(s) := F_s(1) \| F_s(2) \| \cdots \| F_s(\ell)$$

is a pseudorandom generator with expansion factor $n\ell$.

3. Let F be a pseudorandom function from n -bits to n -bits and G be a pseudorandom generator with expansion factor $n + 1$. For each of the following encryption schemes, state whether the scheme (i) has indistinguishable encryptions in the presence of an eavesdropper and whether (ii) it is IND-CPA secure.
 - (a) $Enc_k(m) := \langle r, G(r) \oplus m \rangle$, where $m \in \{0, 1\}^{n+1}$, $r \leftarrow_{\$} \{0, 1\}^n$.
 - (b) $Enc_k(m) := m \oplus F_k(0^n)$.
 - (c) $Enc_k(m) := \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r + 1) \rangle$, where $r \leftarrow_{\$} \{0, 1\}^n$, where $m = m_1 \| m_2$, $|m_1| = |m_2| = n$.
4. Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $r \leftarrow_{\$} \{0, 1\}^n$ is chosen, and the i -th ciphertext block c_i is computed as

$$c_i := F_k(r \oplus i \oplus m_i).$$

Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

5. Consider a ciphertext corresponding to a message encrypted using CBC mode. Suppose a single bit error has occurred in one of the ciphertext block. Which plaintext blocks will it affect during the decryption? What is the effect of such single-bit error in the ciphertext in case of Counter (CTR) mode?