CS6111 (2025): Assignment 2

Instructor: John Augustine

Due: Sept. 14, 2025 (Noon 12:00 PM IST).

- Use LaTeX to typeset your answer. You must submit both the LaTeX file as well as the PDF file. A Turnitin submission link will be provided.
- You can use theorems/lemmas from the textbook (Katz and Lindell, Edition 3 only) without proving them. However, you should mention the theorem/lemma number from the textbook and paraphrase the statement of the theorem/lemma to make your solution self-contained.
- The deadline is Sept. 14, 2025 (Noon 12:00 PM Indian Standard Time).
- Please follow the academic honesty policy for assignments. If you are stuck and need a hint, please post a question on Moodle.
- The assignment is 24 marks. It will be later scaled down to 6 marks.

1. (1 mark) Read Chapter 3 of Katz and Lindell, Edition 3, except starred subsections.

Solution: Yes, I have read the chapter.

2. (3 marks) The Electronic Code Book (ECB) mode of operation encrypts a message M by partitioning it into n-bit blocks $M_1, M_2, \ldots, M_L$ and computing $C_i = F_k(M_i)$ for each block. Is the ECB mode of operation CPA-secure? If yes, provide proof. If not, describe a concrete chosen-plaintext attack.

Solution: No, the ECB model is not CPA secure.

Let us assume the adversary chooses two messages $M, M^{'}$ both of length 2n bits such that ,

$$M = aa$$

$$M^{'} = ab$$

The ECB Code book gives the following cipher texts,

$$C = (F_k(a), F_k(a)) \quad C' = (F_k(a), F_k(b))$$

The adversary can attack the system effectively by checking if the **first half and second half bits** of the ciphertext are equal.

$$Pr[PrivK^{eav}_{A,\pi} = 1] = \frac{1}{2}Pr[A\ Outputs\ 0|M] + \frac{1}{2}Pr[A\ Outputs\ 1|M']$$

Since the adversary can attack the system effectively, using the strategy mentioned above,

$$Pr[PrivK^{eav}_{A,\pi} = 1] = \frac{1}{2} * 1 + \frac{1}{2} * 1 = 1$$

The CPA attack can be defined as below :

1. Adversary $\mathcal{A}$ chooses two messages of 2n bits M, M' such that $M = aa\ \ , M' = ab$
2. System chosses Key k, $k \leftarrow Gen(.)$ and also a random bit b, $b \leftarrow \{0, 1\}$
3. the challenge ciphertext is sent to $\mathcal{A}$,

   $$\mathcal{A} \leftarrow (F_k(M_{b0}), F_k(M_{b1})) = (C_0, C_1)$$

   where,

   $$M_{b0} = M, \quad M_{b1} = M'$$

4. Adversary outputs as follows,

$$Output\ of\ \mathcal{A} = \begin{cases} 0\ \ , if & C_0 = C_1 \\ 1\ \ , if & C_0 \neq C_1 \end{cases}$$

3. (3 marks) Can we achieve "perfect" CPA-security? If so, how would you define it? Otherwise, explain why not.

Solution:

- **Definition:** Perfect CPA-security requires that even an unbounded adversary with access to an encryption oracle cannot distinguish between the encryptions

of two chosen messages with probability better than $\frac{1}{2}$:

$$\Pr[A \text{ succeeds}] = \frac{1}{2}.$$

- This is achievable in settings like the *One-Time Pad*, where:
  - $|K| \geq |M|$ (key space is at least as large as the message space),
  - keys are chosen uniformly at random,
  - ciphertext distribution is uniform and independent of the plaintext.
- **Problem under CPA:** the same key is reused for multiple encryption queries.
  - An unbounded adversary can query all possible plaintexts.
  - This allows the adversary to recover the key.
- **Conclusion:** Perfect CPA-security is impossible.

4. (5 marks) Let F be a pseudorandom function. Comment whether the following constructions of functions from F are also pseudorandom, with proof.

   (a) $F'_k(x) = F_k(x)||F_k(F_k(x))$

Solution: No the function is not Pseudorandom,
Let us define a distinguisher D as follows:

1. Sample $x \leftarrow \{0,1\}^n$
2. Query the oracle F' and obtain the first n bits $a = F_k(x)$ and second n bits $b = F_k(F_k(x))$
3. Query the oracle F' again with a to obtain

$$F'_k(F_k(x)) = F_k(F_k(x))||F_k(F_k(F_k(x))) = a'||b'$$

4. Distinguisher outputs 1 if $a' = b$

Let us compute the success probability,

$$|Pr[D(F'_k(x)) = 1] - Pr[D(r) = 1]| = |1 - Pr[D(r) = 1]|$$

$$Pr[D(F'_k(x)) = 1] = 1$$

$$Pr[D(r) = 1] = Pr[a' = b \; for \; a \; purely \; random \; function] = \frac{1}{2^n}$$

Since, we want all the n bits to be equal.

$$\implies |Pr[D(F'_k(x)) = 1] - Pr[D(r) = 1]| = 1 - 2^{-n} = 1 - negl(n)$$

Hence, a distinguisher can succeed with a significant probablity , therefore $F'(x)$ is not pseudorandom.

(b) $F'_k(x) = F_k(x \oplus c_0)||F_k(x \oplus c_1)$, where c_0 and c_1 are arbitrary but fixed bit strings that the distinguisher knows.

Solution: No, the function is not pseudorandom,
Let us define a distinguisher D as follows:

1. Query the oracle F' with x = 0 and obtain the first n bits, $a = F_k(c_0)$ and second n bits $b = F_k(c_1)$
2. Query the oracle F' with $x = c_1 \oplus c_2$ to obtain the first n bits $a' = F_k(c_0 \oplus c_1 \oplus c_o) = F_k(c_1)$ and second n bits $b' = F_k(c_0 \oplus c_1 \oplus c_1) = F_k(c_0)$
3. Distinguisher outputs 1 if $a' = b$ and $b' = a$

Let us compute the success probability,

$$|Pr[D(F'_k(x)) = 1] - Pr[D(r) = 1]| = |1 - Pr[D(r) = 1]|$$

$$Pr[D(F'_k(x)) = 1] = 1$$

$$Pr[D(r) = 1] = Pr[a' = b \ \& \ b' = a \ for \ a \ purely \ random \ function] = \frac{1}{2^{2n}}$$

Since, we want all the n bits to be equal.

$$\implies |Pr[D(F'_k(x)) = 1] - Pr[D(r) = 1]| = 1 - 2^{-2n} = 1 - negl(n)$$

Hence, a distinguisher can succeed with a significant probablity , therefore $F'(x)$ is not pseudorandom.

5. (7 marks) Let F be a strong pseudorandom permutation. For each of the following schemes, the shared key is a uniformly random $k \in \{0,1\}^n$. State how decryption is done in each scheme and whether the scheme has:

   (i) indistinguishable encryptions in the presence of an eavesdropper (EAV-security),

   (ii) CPA-security (chosen-plaintext attack security),

   Support your answer with an attack or a proof of security.

(a) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \parallel m_2$ with $|m_1| = |m_2|$. Then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r)\rangle$.

Solution:
Decryption Scheme -

- Query the oracle F_k to obtain $F_k(r)$
- XOR $F_k(r)$ to obtain m_1 *and* m_2,

$$m_1 \oplus F_k(r) \oplus F_k(r) = m_1 \text{ and } m_2 \oplus F_k(r) \oplus F_k(r) = m_2$$

- Concatenate m_1 and m_2 to obtain the original message m as $m_1||m_2$

(i) The encryption scheme is not EAV secure since an adversary can compute $m_1 \oplus F_k(r) \oplus m_2 \oplus F_k(r) = m_1 \oplus m_2$ to retrieve some information about m_1 *and* m_2

(ii) The encryption is not CPA secure since an adversary can choose two plain texts as

$$m = m_1||m_1 \ \ and \ \ m' = m_1||m_2$$

to obtain the ciphertext as $\langle r, c_1, c_2\rangle$. The adversary outputs 0 if $c_1 = c_2$ and 1 otherwise.

(b) To encrypt $m \in \{0,1\}^{n/2}$, choose uniformly random bit strings r_1 and r_2 of length $n/2$ each and send the ciphertext $\langle F_k((r_1 \oplus r_2) \parallel m)\rangle$.

Solution:
Decryption Scheme -

- Since we have access to the inverse bijective map, we can obtain the input to the bijection

$$(r_1 \oplus r_2) \parallel m$$

- Obtain the last $\frac{n}{2}$ bits of the input to get m

(i) The encryption scheme is EAV secure since the adversary doesn't have access to the bijection F_k (because it does not have access to key k) and hence the ciphers appear random to the eaves dropper. Inverse bijection cannot be found and eav cannot decrypt the message correctly.

(ii) The encryption is CPA secure since for any choice of messages m_0, m_1, the output cipher texts appear random due to the choice of r_1, r_2 and pseudorandomness of the function.

6. (5 marks) Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Consider a function $H : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ that takes $2n$-bit inputs $L_0 \parallel R_0$ and $2n$-bit keys $k_1 \parallel k_2$ (where L_0, R_0, k_1, k_2 are all n-bit strings). For $i = 1, 2$, define L_i and R_i as

$$L_i = R_{i-1} \ ; \ R_i = L_{i-1} \oplus F_{k_i}(R_{i-1})$$

and output the $2n$-bit string $L_2 \parallel R_2$. So, $H_{k_1 \parallel k_2}(L_0 \parallel R_0) = L_2 \parallel R_2$. Is H a pseudorandom function? Specify a distinguisher or a proof that it is indeed pseudorandom.

Solution:

Let us expand the computation of H as follows:

- $L_1 = R_0$ *and* $R_1 = L_0 \oplus F_{k_1}(R_0)$
- $L_2 = R_1 = L_0 \oplus F_{k_1}(R_0)$ *and* $R_2 = L_1 \oplus F_{k_2}(R_1) = R_0 \oplus F_{k_2}(L_0 \oplus F_{k_1}(R_0))$

Let us define the distinguisher as follows :

1. Query the oracle H with $L_0 || R_0$

$$a = L_2 = L_0 \oplus F_{k_1}(R_0)$$

$$b = R_2 = L_1 \oplus F_{k_2}(R_1) = R_0 \oplus F_{k_2}(L_0 \oplus F_{k_1}(R_0))$$

2. Query the oracle again with $L_0' || R_0$, that is a different left string

$$a' = L_2 = L_0' \oplus F_{k_1}(R_0)$$

3. XOR a and a' to check if it is equal to $L_0 \oplus L_0'$

4.

$$Output = \begin{cases} 1 \ , & a \oplus a' = L_0 \oplus L_0' \\ 0, & otherwise \end{cases}$$

Let us compute the success probability of the distinguisher,

$$|Pr[D(H(x)) = 1] - Pr[D(r) = 1]| = |1 - Pr[D(r) = 1]|$$

$$Pr[D(r) = 1] = 1$$

$$Pr[D(r) = 1] = Pr[a \oplus a' = L_0 \oplus L_0' \ for \ a \ purely \ random \ function] = \frac{1}{2^n}$$

Since, we want all the n bits to be equal.

$$\implies |Pr[D(H(x)) = 1] - Pr[D(r) = 1]| = 1 - 2^{-n} = 1 - negl(n)$$

Hence, a distinguisher can succeed with a significant probablity , therefore $H(x)$ is not pseudorandom.

Acknowledgment

I would like to thank Shri prathaa and Pranay for their useful discussion on solving the problems. Recall that your marks will not be affected by this acknowledgment.