Week 4 **CS6160: Cryptology**

CPA Security and Block Cipher Modes

1 CPA Security: Semantic Security against Chosen Plaintext Attack

In a Chosen Plaintext Attack (abbreviated as CPA), we assume that the adversary can make queries to the Encryption function $Enc(\_, k)$ and thus obtain the ciphertexts corresponding to plaintexts of their choice. Notice that this is more powerful than a Known Plaintext Attack, where some (plaintext, ciphertext) pairs are given to the adversary but the adversary cannot choose the plaintexts or the ciphertexts.

When someone (in this case the adversary) does not know a function f (in this case $Enc(\_, k)$) but can query the values of the function on various inputs, they are said to have **oracle access** to f.

We now formally define CPA security by means of the following.

CPA Indistinguishability Experiment $PrivK^{CPA}_{A,\Pi}(n)$**:**

1. Alice generates a key $k \in \{0,1\}^n$ uniformly at random.
2. The adversary A is given the value n (in unary) and oracle access to $Enc(\_, k)$ throughout the experiment.
3. The adversary A chooses two messages m_0, m_1 and sends them to Alice.
4. Alice picks $b \in \{0,1\}$ uniformly at random and sends $c = Enc(m_b, k)$ to A.
5. The adversary A outputs a value $b' \in \{0,1\}$.
6. The output or value of the experiment is 1 if $b' = b$ and 0 otherwise.

Clarification: The adversary may also query $Enc(\_, k)$ only on messages m_0, m_1. In particular, this implies that for a deterministic cryptosystem (i.e. one which always outputs the same ciphertext for a given plaintext), an adversary can win the above experiment with probability 1.

We can now define CPA security for an encryption system.

Definition 1. *We say that a private-key encryption scheme* $\Pi = (Gen, Enc, Dec)$ *is CPA-secure if for all PPT adversaries* A*, there is a negligible function* $negl()$ *such that:*

$$Pr[Priv_{A,\Pi}^{CPA}(n) = 1] \leq \frac{1}{2} + negl(n).$$

2 Block Cipher Modes

Recall that in a block cipher, we divide a message into blocks of fixed size and also that an encryption algorithm such as DES or AES can encrypt one block.

We now discuss the important issue of how to encrypt a message with several blocks using an encryption algorithm.

2.1 ECB Mode:

The most obvious way is to encrypt each block separately and then concatenate all the corresponding ciphertexts and is called the Electronic Cook Book (ECB) mode. However, the ECB mode is insecure in at least two ways.

- Firstly, ECB encryption is deterministic and hence cannot be CPA-secure.
- Secondly, partial information is always leaked when two message blocks are identical. For example, if the ciphertext looks like $C_1C_2C_1C_3$, then an eavesdropper can see that the first and third blocks are the same, and even this is information that should not be leaked. This also opens up the possibility of tampering for an active adversary, as they may be able to modify just some blocks and send a valid and different ciphertext to the receiver.

The main conclusion is that ECB mode should never be used for block cipher encryption.

2.2 CBC Mode:

We now describe the first solution that addresses the drawbacks of ECB mode. The Cipher Block Chaining (CBC) mode works as follows. Suppose that the message is $M = M_1 M_2 \ldots M_L$, where each M_i is a n-bit block.

1. A random initialization vector (IV) is generated from $\{0,1\}^n$.
2. The first cipherblock is computed as $C_1 = Enc(M_1 \oplus IV, k)$.
3. Each successive block is computed as $C_i = Enc(M_i \oplus C_{i-1}, k)$.
4. The final ciphertext is $IV||C_1|| \ldots ||C_L$.

It turns out that CBC Mode when used with a PRP as the encryption function, is CPA-secure. We do not formally prove this though, and instead give a proof for the CTR mode (net section).

We mention a couple of drawbacks of CBC mode:

- It cannot be parallelized.
- When the last message block is shorter than the block size, it needs to be padded and this can lead to padding attacks (discussed later).

2.3 CTR Mode:

The Counter Mode (also sometimes called Randomized Counter Mode) works as follows. As before, let $M = M_1 \ldots M_L$ be the message.

- As in CBC mode, a random IV is chosen from $\{0,1\}^n$.
- The ith cipherblock is generated as $C_i = M_i \oplus Enc(IV + i - 1, k)$.

The IV used in CTR mode is usually called a counter (as it is incremented for each block), hence the name of the mode.

The advantages of this mode over CBC mode are that it can be parallelized (as each cipherblock can be generated independently of any other given the IV) and it does not use padding.

In the next section, we show that a block cipher used in CTR mode is CPA-secure if the encryption algorithm is a PRP.

3 Block Ciphers in CTR Mode are CPA-secure

Theorem 1. *Let $Enc : M \times \{0,1\}^n \to C$ be a PRP (where $C = M$). Consider a block cipher encryption system Π that uses $Enc()$ in CTR mode. If A is a PPT-adversary, then $Pr[PrivK^{CPA}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$, where $negl(n)$ is some negligible function.*

Proof. Consider the following modified experiment $PrivK^{CPA}_{A,\Pi'}(n)$, where the function Enc is replaced by a random permutation $\pi : M \to C$.

We show two things:

- For every PPT adversary A, it must be the case that:

$$|PrivK^{CPA}_{A,\Pi}(n) - PrivK^{CPA}_{A,\Pi'}(n)| \leq negl(n) \tag{1}$$

  for some negligible function $negl()$.

- Let A be an adversary A that can make at most $q(n)$ queries, with each query message having at most $q(n)$ blocks, where $q()$ is some polynomial. Then

$$PrivK^{CPA}_{A,\Pi'}(n) \leq \frac{1}{2} + \frac{2q(n)^2}{2^n} \tag{2}$$

To prove (1), suppose for contradiction that there is a PPT adversary A such that $PrivK^{CPA}_{A,\Pi}(n) = p_1(n)$, $PrivK^{CPA}_{A,\Pi'}(n) = p_2(n)$, $p_1(n) > p_2(n)$ and $r(n) = p_1(n) - p_2(n)$ is non-negligible.

Then we can build a PPT algorithm D which can distinguish Enc from a random permutation as follows:

- D receives oracle access to a function f that is either $f_0 = Enc$ or f_1, a random permutation and D's goal is to make queries to f to determine whether $f = f_0$ or $f = f_1$.
- D picks a random key $k \in K$.
- D simulates A for $PrivK^{CPA}_{A,\Pi}(n)$ and chooses two messages m_0, m_1.
- D picks $b \in \{0,1\}$ at random and simulates A on $f(m_b, k)$ to obtain A's guess b'.

- If $b' = b$, D guesses that $f = f_0$ otherwise D guesses that $f = f_1$.

The probability that D is correct equals:

$$\frac{1}{2}p_1(n) + \frac{1}{2}\left(1 - p_2(n)\right) = \frac{1}{2} + \frac{r(n)}{2}$$

which is non-negligible if $r(n)$ is non-negligible. This contradicts the fact that *Enc* is a PRP, therefore it must be the case that (1) is true.

We now prove (2). Let $q = q(n)$. Let $M_1 = M_{1,1}|| \dots ||M_{1,q}$ and $M_2 = M_{2,1}|| \dots ||M_{2,q}$ be the two messages chosen by the adversary, where each $M_{i,j}$ is a block. Let $C = IV||C_{i,1}|| \dots C_{i,q}$ be the ciphertext corresponding to M_i, where $i \in \{1, 2\}$. C is the ciphertext received by the adversary.

Let $M_i = M_{i,1}|| \dots ||M_{i,q}$ for $i = 3, \dots, q + 2$ be the messages queried by the adversary and let $C_i = IV_i||C_{i,1}|| \dots ||C_{i,q}$ be the corresponding ciphertexts.

We have for $i \geq 3$:

$$C_{i,j} = M_{i,j} \oplus \pi(IV_i + j - 1, k). \tag{3}$$

Since π is a random permutation, each individual ciphertext block is a random element of M; thus the only way that the adversary can distinguish M_1 from M_2 is if an event such as the following happens:

For some j_1, j_2, j_3 such that $M_{1,j_1} = M_{i,j_2} \neq M_{2,j_1}$ it is the case that

$$IV + j_1 - 1 = IV_i + j_2 - 1 \tag{4}$$

If the above happens, then the adversary checks whether the C_{i,j_2} cipherblock is equal to C_{i,j_1}. If yes, the adversary concludes that the message was M_1, otherwise that the message was M_2.

The probability that some relation of the form (4) happens is at most $\dfrac{2q(n)^2}{2^n}$. If a relation of the form (4) does not exist among the IVs of the query ciphertexts, then the adversary can only guess with probability 1/2. Combining the above two observations, we obtain the bound in (2).

□