1 Last Lecture

An encryption scheme, with algorithms Enc and Dec must satisfy correctness and security. For (perfect) correctness, we require that for all keys k and messages m,

$$\mathsf{Dec}(\mathsf{Enc}(m,k),k) = m.$$

Last lecture, we saw a few intuitive definitions of a secure encryption scheme. We were only considering *eavesdropping adversaries* – adversaries that see the ciphertext, and try to learn some information about the underlying message. In particular, an eavesdropping adversary does not try to tamper the ciphertext (we will see such attacks later in the course).

Listed below are a few intuitive definitions for an encryption scheme to be secure against eavesdropping adversaries:

- An encryption scheme is secure if no adversary can recover the message, given an encryption of a random message using a random key.
- An encryption scheme is secure if no adversary can recover any information about the message, given an encryption of a random message using a random key.
- An encryption scheme is secure if the probability distribution of messages doesn't change, even if conditioned on receiving a ciphertext.

In this note, we will only focus on the third one, and then will present another equivalent, simpler-to-work-with definition. [1]

2 Probability distribution based definition

Suppose there is an eavesdropping adversary who is monitoring the encrypted communication between Alice and Bob. Alice wants to send an encrypted movie to Bob, and both don't want the adversary to know which movie was sent. The adversary has some prior information about Alice's movie preferences. Let us assume the worst case scenario: the adversary knows the exact probability distribution corresponding to Alice's movie preferences. For example,

- "Movie1" is the most likely movie that Alice will send. The adversary knows that with probability 1/2, Alice will send this movie.
- "Movie2" is the second most likely movie, it has a probability of 1/4.
- "Movie3" also has probability 1/4.

Now suppose Alice picks a movie and sends its encryption to Bob. Then, *even before seeing the ciphertext*, the adversary knows that "Movie1" will be sent with probability 1/2. Given the ciphertext, does the adversary know some extra information now? Or does the adversary still think that it is "Movie1" with probability 1/2 and the other two with probability 1/4? We want our encryption scheme to be so secure that even after seeing the ciphertext, the adversary still thinks that "Movie1" has probability 1/2, "Movie2" has probability 1/4 and "Movie3" has probability 1/4.

To build our confidence in this 'intuitive definition', let us see a few example encryption schemes that are clearly broken, and do not satisfy the above 'intuitive definition'.

Example 1: Let $\mathcal{M}$ (the message space), and $\mathcal{K}$ (the key space) be $\{0,1\}^n$. Consider the scenario where encryption of a message $m = (m_1, \ldots, m_n)$ with key k is $(m \oplus k, m_1)$ (note that $\oplus$ denotes bitwise XOR). Clearly, this encryption scheme reveals the first bit of the message, and therefore it should not be secure.

[1] The OneNote file contains formalisation of the first two intuitive definitions, but this is not part of the course syllabus.

Indeed there is a simple attack. Consider a distribution $\mathcal{D}$ defined as follows:

$$\Pr_{m \leftarrow \mathcal{D}}\Big[m = x\Big] = \begin{cases} 1/2 \text{ if } x = 00\ldots0 \\ 1/2 \text{ if } x = 11\ldots1 \\ 0 \text{ otherwise} \end{cases}$$

If the adversary sees that the last bit of the ciphertext is 0, then the adversary knows that the message underlying the ciphertext is the all zeroes string. As a result, the probability of the message being all zeroes string (which was 1/2 before seeing the ciphertext) becomes 1 after seeing a ciphertext whose last bit is 0.

Example 2: Consider the scenario where the message space $\mathcal{M}$ and key space $\mathcal{K}$ comprises of integers in range 0 to 99 (inclusive). The encryption of m with key k consists of two numbers: $m + k \mod 100$ and $m * k \mod 5$.

Again, we want to show that this scheme is not secure. For this, we need to demonstrate a distribution such that the likelihood of a message increases after seeing a ciphertext. Consider the following distribution: $m = 0$ with probability 1/2 and $m = 1$ with probability 1/2. This is the adversary's information about the message distribution before seeing the ciphertext. Suppose the adversary sees a ciphertext $\mathsf{ct} = (a, b)$ where b is nonzero. Then, given this ciphertext, the adversary knows for sure that the underlying message m was not 0.

We now formally state the above discussed intuitive definition.

Definition 02.03. An encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ with key space $\mathcal{K}$ and message space $\mathcal{M}$ satisfies *'perfect secrecy'* (or *'perfect security'*) if the following holds for any distribution $\mathcal{D}$ over $\mathcal{M}$, any message x and ciphertext c,

$$\Pr_{m \leftarrow \mathcal{D}}\Big[m = x\Big] = \Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}\Big[m = x \mid \mathsf{Enc}(m, k) = c\Big]$$

Note that the key's distribution is fixed to be uniform (as you can see on the RHS, the probability is over the choice of a random key $k \leftarrow \mathcal{K}$), but we want security for any distribution of messages (that is, $m \leftarrow \mathcal{D}$ in both LHS and RHS expressions). Fixing the key's distribution to be uniform is a popular design choice. This choice is available at the time of designing the encryption scheme. The message distribution, however, is allowed to be arbitrary. This is because we want our encryption scheme to offer security in all real-world settings. For instance, the security of the encryption scheme should not deteriorate based on the language of communication between Alice and Bob, or Alice's movie preferences.

3 Indistinguishability based definition

Sometimes, it is a bit difficult to use Definition 02.03. Therefore, we present another (seemingly different) definition that is simpler to work with, and at the same time, is equivalent to Definition 02.03.

This new definition does not talk about any distribution of messages. Instead, it requires that for all messages m_0, m_1 and all ciphertexts c, the probability that m_0 is mapped to c (using a random key) is equal to the probability of m_1 being mapped to c (again, using a random key). If this condition is satisfied, then we say that the scheme satisfies perfect indistinguishability.

Definition 02.04. An encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$, key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$ satisfies *'perfect indistinguishability'* if for all $m_0, m_1 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$,

$$\Pr_{k \leftarrow \mathcal{K}}\Big[\mathsf{Enc}(m_0, k) = c\Big] = \Pr_{k \leftarrow \mathcal{K}}\Big[\mathsf{Enc}(m_1, k) = c\Big].$$

It is easy to check that the insecure encryption schemes in Examples 1 and 2 would be insecure as per this definition as well. The next section shows that any encryption scheme is secure as per Definition 02.03 if and only if it is secure as per Definition 02.04.

4 Equivalence of the above definitions

Theorem 02.01. An encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ satisfies Definition 02.03 if and only if it satisfies Definition 02.04.

Proof Sketch: The formal proof can be found in the textbook. Here, we provide a sketch.

Part (a): Definition 02.03 implies Definition 02.04
Proof by contradiction. Suppose Definition 02.04 is not satisfied. Then there exist messages m_0, m_1 and ciphertext c^* such that $\Pr_k\left[\mathsf{Enc}(m_0, k) = c^*\right] \neq \Pr_k\left[(m_1, k) = c^*\right]$. Then define distribution $\mathcal{D}$ as follows: $\Pr_{m \leftarrow \mathcal{D}}\left[m = m_0\right] = \Pr_{m \leftarrow \mathcal{D}}\left[m = m_1\right] = 1/2$. Let $x = m_0$ and $c = c^*$.

We need to show that $\Pr_{m,k}\left[m = x \mid \mathsf{Enc}(m, k) = c\right] \neq 1/2$.

Since $\Pr_k\left[\mathsf{Enc}(m_0, k) = c^*\right] \neq \Pr_k\left[(m_1, k) = c^*\right]$, this means

$$\Pr_{m,k}\left[m = m_0 \mid \mathsf{Enc}(m, k) = c\right] \neq \Pr_{m,k}\left[m = m_1 \mid \mathsf{Enc}(m, k) = c\right].$$

Now since $\sum_{i=0}^{1} \Pr_{m,k}\left[m = m_i \mid \mathsf{Enc}(m, k) = c\right] = 1$, this means

$$\Pr_{m,k}\left[m = x \mid \mathsf{Enc}(m, k) = c\right] \neq 1/2$$

This concludes the proof of Part (a).

Part (b): Definition 02.04 implies Definition 02.03
For any distribution $\mathcal{D}$, message x and ciphertext c,

$$\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}\left[m = x \mid \mathsf{Enc}(m, k) = c\right] \tag{1}$$

$$= \frac{\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}\left[m = x \wedge \mathsf{Enc}(x, k) = c\right]}{\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}\left[\mathsf{Enc}(m, k) = c\right]} \quad \text{(Bayes' rule)} \tag{2}$$

$$= \frac{\Pr_{m \leftarrow \mathcal{D}}\left[m = x\right] \cdot \Pr_{k \leftarrow \mathcal{K}}\left[\mathsf{Enc}(x, k) = c\right]}{\Pr_{\substack{m \leftarrow \mathcal{D} \\ k \leftarrow \mathcal{K}}}\left[\mathsf{Enc}(m, k) = c\right]} \quad \text{(key and message indep. sampled)} \tag{3}$$

To finish the proof, we need the following observation. This is the part where we use the fact that our scheme $(\mathsf{Enc}, \mathsf{Dec})$ satisfies Definition 02.04.

Observation: For any $x \in \mathcal{M}$ and $c \in \mathcal{C}$, $\Pr_k\left[\mathsf{Enc}(x, k) = c\right] = \Pr_{k,m}\left[\mathsf{Enc}(m, k) = c\right]$.

Note, the probability in LHS is over the choice of key k (message x and ciphertext c are fixed), and the RHS is over choice of $m \leftarrow \mathcal{D}$ and key k (the ciphertext c is fixed).

The RHS can be expressed as follows:

$$
\begin{aligned}
&\sum_{z \in \mathcal{M}} \Pr_{k,m}\Big[m = z \ \wedge \ \mathsf{Enc}(m,k) = c\Big] \\
= &\sum_{z \in \mathcal{M}} \Pr_{k,m}\Big[m = z \ \wedge \mathsf{Enc}(z,k) = c\Big] \\
= &\sum_{z \in \mathcal{M}} \Pr_{m}\Big[m = z\Big] \cdot \Pr_{k}\Big[\mathsf{Enc}(z,k) = c\Big]
\end{aligned}
$$

The last step follows from the fact that k and m are chosen independently.

Finally, we use Definition 02.04 : $\Pr_k[\mathsf{Enc}(x,k) = c] = \Pr_k[\mathsf{Enc}(z,k) = c]$ for all $x, z \in \mathcal{M}$ and $c \in \mathcal{C}$. This completes the proof. □

5 Shannon's One Time Pad

Shannon's One Time Pad is an encryption scheme that achieves Definition 02.04 (and Definition 02.03). The message space, key space and ciphertext space are all $\{0,1\}^n$. The encryption and decryption algorithms are as follows.

- $\mathsf{Enc}(m,k) = m \oplus k$
- $\mathsf{Dec}(c,k) = c \oplus k$

The one time pad satisfies perfect security (i.e. Definition 02.03), and it is easier to use Definition 02.04 for showing this. Take any $m_0, m_1, c \in \{0,1\}^n$. Then,

$$\Pr_{k \leftarrow \mathcal{K}}[m_0 \oplus k = c] \ = \ \Pr_{k \leftarrow \mathcal{K}}[k = c \oplus m_0] \ = \ \frac{1}{|\mathcal{K}|} \ = \ \Pr_{k \leftarrow \mathcal{K}}[m_1 \oplus k = c].$$

Additional References

Relevant sections of the textbook [Boneh-Shoup]: Sections 2.1.1 and 2.1.2.