CSA E0 235: Cryptography January 19, 2016

[Lecture 3]

Instructor: Arpita Patra *Submitted by: Pratik Sarkar*

1 Recap

In our previous lecture we saw the definition of perfect security, analysed the construction of One Time Pad (OTP) and proved how it satisfies the property of perfect security. Furthermore we discussed the drawbacks of OTP, that the key size must be as large as the message and keys cannot be reused.

2 Topics to be Covered

We will show that the problems faced by OTP are inherent to any perfect secure schemes and they cannot be avoided at any cost. We will also discuss more definitions of perfect security and their equivalences with the previous definitions and then conclude perfect security, giving rise to the world of computational security, which will overcome the problems faced by perfect security, by relaxing some assumptions on the power of the adversary and the amount of break allowed to happen.

3 Drawbacks of Perfect Security

Any perfect security scheme faces two drawbacks:

1. Keyspace must be as large as possible

2. Keys should not be reused

Let's prove the first statement.

Theorem 1 *Keyspace K must be as large as message space M for perfect security*

Proof Assume the size of keyspace is less than message space, i.e. $|K| < |M|$. Let c be a ciphertext which occurs with non-zero probability, $Pr(C = c) > 0$. Let $M(c)$ denote the set of all messages that can be decrypted from c by some key k.
$M(c) = \{m | m = Dec_k(c) \ for \ some \ k\}$ Since $|K| < |M|$, the number of messages that can be decrypted from c is less than the size of message space. So $M(c) \leq |K| < |M|$ and $\exists m \in M, \ s.t. \ m \notin M(c)$.
$Pr[M = m | C = c] = 0 \neq Pr[M = m]$

Thus the apriori and posteriori probabilities are different for m, contradicting perfect security. For perfect security to hold $|K| \geq |M|$. For OTP, $|K| = |M|$ and it is optimal key-length wise and key-usability wise. ■

4 Definitions of Perfect Security

In this section we discuss various definitions of Perfect Security and show equivalence among them. Each definition is tailored for usage in different scenarios.

Definition 1 An encryption scheme (Gen, Enc, Dec) over a message space M is perfectly secure iff for every probability distribution over M, every message $m \in M$ and every ciphertext $c \in C$:
$Pr[M = m|C = c] = Pr[M = m]$ $\diamondsuit$

It says that the probability of knowing a ciphertext before and after seeing the plaintext remains the same.

Definition 2 An encryption scheme (Gen, Enc, Dec) over a message space M is perfectly secure iff for every probability distribution over M, and every two messages $m_0, m_1 \in M$ and every ciphertext $c \in C$:
$Pr[C = c|M = m_0] = Pr[C = c|M = m_1]$ $\diamondsuit$

It says that the probability distribution of the ciphertext remains independent of the message space.

Theorem 2 *Shannon's Theorem: A scheme (Gen, Enc, Dec) with $|K| = |M| = |C|$ is perfectly secure iff:*

1. *Every key k is chosen with probability $\frac{1}{K}$ by Gen.*
2. *For every message $m \in M$ and $c \in C$, there is an unique key k s.t, $Enc_k(m) = c$.*

For any perfectly secure scheme, $|C| \geq |M|$ has to hold. Let us assume it doesn't and $|C| < |M|$. Then for a particular key k, the ciphertext must be decryptable to 2 messages m_i and m_j. This violates correctness and so $|C| \geq |M|$. The optimal is $|C| = |M|$.

To prove $Pr[M = m|C = c] = Pr[M = m]$, we use bayes theorem as follows:
$Pr[M = m|C = c] = \frac{Pr[C=c|M=m].Pr[M=m]}{Pr[C=c]}$
For any arbitrary c and m and $c \leftarrow Enc_k(m)$,
$Pr[C = c|M = m] = Pr[K = k] = \frac{1}{|K|}$
$Pr[C = c] = \sum_{m \in M} Pr[C = c|M = m].Pr[M = m] = \frac{1}{|K|} \sum Pr[M = m] = \frac{1}{|K|}$
$Pr[M = m|C = c] = \frac{1}{|K|} \times |K| \times Pr[M = m] = Pr[M = m]$
Hence Definition 1 is proved.

Let $m = m_0, m_1, \ldots$ and c is a ciphertext that occurs with non zero probability for some message. Let K_i be the set of all the keys that map m_i to c, i.e.
$Enc_k(m_i) = c, k \in K_i$.
We claim the following two statements:

1. $K_i \neq \emptyset, \forall i$
2. $K_i \cap K_j = \emptyset, \forall i, j$

These $K_1, K_2, \ldots$ sets a partition on the keyspace. We assume that $Pr[C = c|M = m] > 0$, for some m/ For arbitrary $c, m_i \; and \; m_j$,

$Pr[C = c|M = m_i] = Pr[C = c|M = m_j]$.

This denotes that c is decryptable to every message, and thus $K_i \neq \emptyset$.

Assume the same k maps both m_i and m_j to c, then $Dec_k(c) = m_i \; and \; Dec_k(c) = m_j$, this violates correctness as the same ciphertext maps to two different messages for same key. Thus we prove that $K_i \cap K_j = \emptyset$.

For $|K| = |M|$, so each K_i will have only 1 key in it. Thus every message is encryptable to a particular cipher c with just 1 key, $Enc_k(m) = c$. We get the following:

$Pr[K = k_i] = Pr[C = c|M = m_i] = Pr[C = c|m = m_j] = Pr[K = k] = \frac{1}{|K|}$

Hence we prove the two statements of Shannon's theorem and definition 2. Note that using Shannon's theorem we can easily prove perfect security without computing the probability distributions on $Pr[C = c|M = m]$ and $Pr[M = m]$ for all possible m, c. But this will hold only for $|K| = |M| = |C|$.

We can observe that OTP is optimal as it samples keys uniformly random from the keyspace and it holds the shannon's theorem with minimal keysize possible for perfect security.

5 Perfect Security as an indistinguishable game

It is carried out in the form of a game between an unbounded adversary and a hypothetical honest challenger. Here the attacker is assumed to carry out a cipher text only attack (coa), where he sees the ciphertexts and tries to guess the message. The experiment $Priv^{coa}_{A,\pi}$ is played as following:

1. The adversary A outputs a pair of message m_0 and $m_1 \in M$.
2. The challenger generates a random key k by running the Gen algorithm and obtains a random bit b by tossing a coin. Then he encrypts the message m_b as $c \leftarrow Enc_k(m_b)$ and sends it to A.
3. A outputs a bit b'.
4. The output of the experiment is 1 if $b' = b$ else the output is 0.

An encryption scheme (Gen, Enc, Dec) over a message space M is perfectly secure if for every adversary A it holds that:

$Pr[Priv^{coa}_{A,\pi} = 1] = \frac{1}{2}$

The adversary cannot distinguish between the encryptions of m_0 and m_1 with any advantage. Even after seeing the ciphertext c and having complete knowledge of the messages, his probability of guessing b' correctly is equivalent to the probability of guessing b' without seeing c. Thus the apriori probability is same as the posteriori probability. Hence this game based definition is equivalent to the defintion 1 of perfect security.

6 Concluding Perfect Secrecy

Perfect security schemes gave us very simple and fast schemes with 0 advantage to the adversary. We gave unbounded computing power to the adversary and allowed no break to occur, which is unrealistic for practical purposes. For the simplest kind of attack, Ciphertext Only Attack, by the adversary, we had to incur 2 major drawbacks that the key cannot be reused and the keysize must be as large as message size. For stronger attacks like Chosen Ciphertext Attack (CCA) and Chosen Plaintext Attack (CPA), we will have even stronger limitations. So this calls for some relaxations on the power of the adversary and the amount of break allowed to happen. This leads us to the world of statistical and computational security. In statistical security model, the adversary is given unbounded power but the break is allowed to happen with negligible probability. Furthermore, if we bound the adversary to a polynomial time turing machine, then we obtain computational/cryptographic security. Here the keys can be reused and the key size is smaller than the message size. We will explore the world of computational security in the next lecture.

References

[1] Arpita Patra, *http://drona.csa.iisc.ernet.in/ arpita/Cryptography16.html* Lecture notes.

[2] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*.