CSC 591 Cryptography 8/29/2018

One-Time Pad

Lecturer: Alessandra Scafuro *Scribe: Courtney Weglar*

Perfectly Secure Encryption Scheme

In this class we formally defined an encryption scheme and introduced the notion of perfect security for an encryption scheme. Intuitively, an encryption scheme is perfectly secure if the ciphertexts generated by the encryption algorithm do not provide any *additional* information to an adversary with respect to the message that was actually encrypted. To formally define what it means to not learn any *additional* information, we have to define the information that the adversary already knows. We assume that the adversary knows:

- The distribution of the *plaintexts*; that is, the messages that will be encrypted, and their probability of being encrypted.
- The encryption algorithm.
- The decryption algorithm.

At this point, we also assume that the adversary is unbounded; that is, they have no computational/storage restriction.

Definition

Intuitive Definition of Perfect Security: an encryption scheme has perfectly secure ciphertexts if by looking at a cipher c, the adversary does not learn any additional information about message m. In other words, given c, the adversary's *a posteriori* knowledge (what the adversary knows after obtaining c) is equivalent to the adversary's *a priori* knowledge (what the adversary knew before obtaining c). The *a priori* knowledge of the adversary is knowledge of the message space and knowledge of the encryption scheme being used. The adversary knows the probability distribution over $\mathcal{M}$, or likelihood that different messages will be sent (for more information, see textbook chapter 2 page 29). If the encryption scheme is perfectly secure, the adversary's *a posteriori* knowledge is the exact same as the adversary's *a priori* knowledge.

An encryption scheme is defined by three algorithms: key generation algorithm Gen, encryption algorithm Enc, and decryption algorithm Dec, along with a specification of a finite message space $\mathcal{M}$. The Gen algorithm outputs a key k, chosen according to some distribution. $\mathcal{K}$ denotes the finite key space that is the set of all possible keys that can be output by the Gen algorithm. The Enc algorithm takes as input a key $k \epsilon \mathcal{K}$ and a message $m \epsilon \mathcal{M}$ and outputs a ciphertext c. $\mathcal{C}$ denotes the set of all possible ciphertexts that can be output by the encryption algorithm Enc for all possible choices of k $\epsilon \mathcal{K}$ and m $\epsilon \mathcal{M}$. The Dec algorithm takes as input a ciphertext $c \epsilon \mathcal{C}$ and a key $k \epsilon \mathcal{K}$ and outputs a plaintext message $m \epsilon \mathcal{M}$.

Definition 1 *An encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is perfectly secure for message space* $\mathcal{M}$ *if*

$$Pr[M = m|C = c] = Pr[M = m]$$

Assumptions

None

Scheme: One-Time-Pad

Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$ be the plaintext space, the key space and the ciphertext space, respectively, The one-time-pad encryption scheme is described as follows:

Key Generation: Gen: Output $k \xleftarrow{\$} \mathcal{K}$.

Encryption: $\mathsf{Enc}(m, k)$: Output $c = m \oplus k$.

Decryption: $\mathsf{Dec}(c, k)$: Output $m = c \oplus k$.

Security Proof

The scheme is secure because Pr[M=m'|C=c']=Pr[M=m']. This means that the probability that the adversary can guess the correct message after seeing the encrypted ciphertext is the same as the probability that the adversary can guess the correct message without seeing the ciphertext at all. In other words, the adversary is equally sure that the guessed decryption of the message is correct before and after having seen the ciphertext.

Theorem: One-Time Pad is perfectly secure

Proof:

$Fix\ c,\ m'$

$Pr[M = m'|C = c] = \frac{Pr[C=c|M=m']*Pr[M=m']}{Pr[C=c]}$

$Pr[C = c|M = m'] = Pr[C = Enc_k(m')] = Pr[c = k \oplus m'] = Pr[k = c \oplus m'] = \frac{1}{2^l}$

$Pr[C = c] = \sum_{m' \in M} Pr[C = c|M = m'] * Pr[M = m'] = \frac{1}{2^l} \sum_{m' \in M} Pr[M = m'] = \frac{1}{2^l} * 1 = \frac{1}{2^l}$

$\therefore \frac{Pr[C=c|M=m']*Pr[M=m']}{Pr[C=c]} = \frac{\frac{1}{2^l} Pr[M=m']}{\frac{1}{2^l}} = Pr[M = m']$

$\therefore Pr[M = m'|C = c] = Pr[M = m']$

One limitation of perfect security is that the key space $\mathcal{K}$ must be $\geq$ the message space $\mathcal{M}$. In other words, if all keys are the same length, and the message space contains only strings of some fixed length, the key must be at least as long as the message. Specifically, the

key length of the One-Time Pad scheme is actually the optimal length for a given perfectly secure algorithm. Another limitation is that each key can be used only once. So, in order to send some message m, you must use a unique key for that message, which requires a lot of computational power and is not very efficient.