EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 3 — January 12, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Perfectly Secret Encryption

- Let us look at encryption schemes that are provably secure even against an adversary with unbounded computational power. Such schemes are called *perfectly secret*. The existence of such schemes is not obvious because we are allowing the adversary to launch brute-force attacks (for e.g., try all possible keys for any key length).
- This work was done by Shannon in the 1940s, so not exactly modern cryptography which is post 1970s. But Shannon was way ahead of his time.
- Recall the syntax of encryption: $m \in \mathcal{M}, k \in \mathcal{K}, k = \texttt{Gen}, c = \texttt{Enc}_k(m), m = \texttt{Dec}_k(c)$
- $c \leftarrow \texttt{Enc}_k(m)$ may be probabilistic but $\texttt{Dec}_k(c) = m$ with probability 1. This is called perfect correctness.
- Let M be a random variable denoting the message (plaintext) being encrypted.
- Let K be a random variable denoting the value of the key output by $\texttt{Gen}$. Almost always a uniform random variable on $\mathcal{K}$.
- K and M are assumed to be independent.
- Let C be a random variable denoting the ciphertext.
- Fixing an encryption scheme and a distribution over $\mathcal{M}$ determines a distribution over $\mathcal{C}$ given by choosing a key $k \in \mathcal{K}$.
- Example: Consider the shift cipher with message set $\mathcal{M} = \{\texttt{kim}, \texttt{ann}, \texttt{boo}\}$ with probabilities 0.5, 0.2, 0.3 respectively. What is $\Pr[C = \texttt{dqq}]$? What is $\Pr[M = \texttt{ann} \mid C = \texttt{dqq}]$?

1.1 Perfect Secrecy

- Assume that adversary knows
  - Probability distribution over $\mathcal{M}$
  - Encryption scheme
  - Ciphertext transmitted
- Ciphertext text should reveal nothing about the plaintext.

Definition (KL page 29)**.** *An encryption scheme (*$\mathtt{Gen}$*,* $\mathtt{Enc}$*,* $\mathtt{Dec}$*) with message space* $\mathcal{M}$ *is* ***perfectly secret*** *if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$*, and every ciphertext* $c \in \mathcal{C}$ *for which* $\Pr[C = c] > 0$*:*

$$\Pr[M = m \mid C = c] = \Pr[M = m].$$

In other words, the *a posteriori* probability that some message $m \in \mathcal{M}$ was sent, conditioned on the ciphertext that was observed, should be the same as the *a priori* probability that m was sent.

Lemma. *An encryption scheme (*$\mathtt{Gen}$*,* $\mathtt{Enc}$*,* $\mathtt{Dec}$*) with message space* $\mathcal{M}$ *is* ***perfectly secret*** *if and only if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$ *for which* $\Pr[M = m] > 0$ *and every ciphertext* $c \in \mathcal{C}$*:*

$$\Pr[C = c \mid M = m] = \Pr[C = c].$$

Equivalent formulation of perfect secrecy: The probability distribution of the ciphertext does not depend on the plaintext, i.e.

$$\Pr[\mathtt{Enc}_K(m) = c] = \Pr\left[\mathtt{Enc}_K(m') = c\right]$$

This implies that the ciphertext contains no information about the plaintext.

Lemma. *An encryption scheme (*$\mathtt{Gen}$*,* $\mathtt{Enc}$*,* $\mathtt{Dec}$*) with message space* $\mathcal{M}$ *is perfectly secret if and only if* $\Pr[\mathtt{Enc}_K(m) = c] = \Pr[\mathtt{Enc}_K(m') = c]$ *holds for every* $m, m' \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*.*

Proof. ($\Rightarrow$) If a scheme is perfectly secure, $\Pr[C = c \mid M = m] = \Pr[C = c] = \Pr[C = c \mid M = m']$.

($\Leftarrow$) The case of $\Pr[M = m] = 0$ is trivial. For $\Pr[M = m] > 0$, note that $\Pr[C = c \mid M = m] = \Pr[\mathtt{Enc}_K(m) = c]$. Use Bayes' theorem to show that $\Pr[M = m \mid C = c] = \Pr[M = m]$. □

2 One-Time Pad

- Patented by Vernam in 1917. At that time, he did not know that it was a perfectly secret encryption scheme.
- Shannon introduced the notion of perfect secrecy in the 1940s and proved that the one-time pad achieves it.
- Construction

3 References and Additional Reading

- Sections 2.1,2.2 from Katz/Lindell