15:853: Algorithms in the Real World
Fall 2019

Lecture 17

October 31 2019

Lecturer: Francisco Maturana *Scribe: Tianjun Ma*

17.1 Recap From Last Class

This is the first lecture on cryotography.

17.2 Overview

Introduction

- Definitions
- One-time pad
- Security

Private-Key Algorithms

- Overview
- Block Ciphers
- Feistel Networks
- Permutation Network
- Rijindael

Number Theory

- Groups

17.3 Introduction

17.3.1 Definitions

Cryptography

The general term describing the techniques for secure communication with the presence of malicious third party.

Cryptology

The theory behind cryptography.

Encryption

The encoding of messages.

Cryptanalysis

The study of breaking cryptographic systems.

Cipher

A method or algorithm used for encrypting or decrypting.

Private Key

Also known as Symmetric Key, when $key_1 = key_2$. This is because all parties share the same private keys used for decoding.

Public Key

Also known as Asymmetric Key, when $key_1 \neq key_2$. This is because there is a public key and a private key for the cryptographic system. It is hard for malicious third party to obtain the private key but the public key is available to everyone.

17.3.2 One-time pad

Procedure

1. Generate the key $k \in \{0,1\}^n$(in unary) given length n as input
2. Encrypt k using $m \in \{0,1\}^n$ by calculating $c = m \oplus k$
3. Dycrypt c by calculating $m = c \oplus k$

Properties

One-time pad is perfectly secret. That is, Let M, C be random variables representing the message and ciphertext, respectively. Then for every message m and ciphertext c with $P(C = c) > 0$, we have

$$P(M = m|C = c) = P(M = m)$$

which means taht the ciphertext contains no information about the message.

Proof:

$$\begin{aligned}
P(C = c|M = m) &= P(m \oplus K = c) \\
&= P(K = m \oplus c) \\
&= \frac{1}{2^n} \\
P(C = c) &= \sum_m P(C = c|M = m)P(M = m) \\
&= \frac{1}{2^n} \sum_m P(M = m) \\
&= \frac{1}{2^n} \\
P(M = m|C = c) &= P(C = c|M = m)\frac{P(M = m)}{P(C = c)} \\
&= P(M = m)
\end{aligned}$$

□

Problems

As its name suggests, we cannot reuse a one-time pad, otherwise the adversary will be able to deduce $m_1 \oplus m_2$ given c_1, c_2 while $c_1 = k \oplus m_1$ and $c_2 = k \oplus m_2$. This is very undesirable as too much information about the original message will be exposed.

17.3.3 Security

Importance of Randomness

To make one-time pad perfectly secret, the key needs to be truly uniformly random, as an adversary can exploit biases in randomness.

Computational Secrecy

Perfect secrecy requires the key to be at least as long as the message, but this will become impractical if the message is long. To find a more cost effective way of achieving good secrecy, we need to settle for a weaker definition, that is:

Any efficient adversary suceeds in breaking the sceheme with at most negligible probability.

- Efficient: the adversary runs in probabilistic polynomial time.
- Negligible: goes to zero faster than any inverse polynomial:

- A positive function f is negligible if for every positive integer c, there exists N_c such that $\forall n > N_c, f(n) < \frac{1}{n^c}$
- We denote this relationship as $f = negl(n)$.

Cryptanalytic Attacks

Represent ciphertext messages as c and plaintext messages as m,

- Ciphertext Only: the attacker has multiple cs but does not know the corresponding ms.
- Known Plaintext: the attacker knows multiple cs with their corresponding ms.
- Chosen Plaintext: the attacker gets to choose ms and generate their corresponding cs.
- Chosen Ciphertext: the attacker gets to choose cs and generate their corresponding ms.

17.4 Private-Key Cryptosystems

17.4.1 Overview

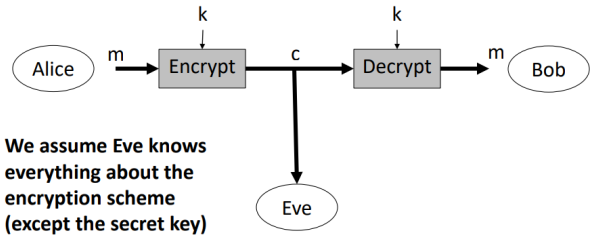

Figure 17.1. Procedure of Private Key Encryption, adopted from lecture slides

Question: what does it mean to be secure?

Regardless of any information that Eve has, c should not leak any additional information about m.

17.4.2 Block Ciphers

A block cipher C is a function with:

- Input: a key $k \in \{0,1\}^{|k|}$, block $x \in \{0,1\}^n$ with $|k| \leq n$
- Output: a block $y \in \{0,1\}^n$

such that it is hard to distinguish this function from a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$.

Counter Mode

We basically chop long messages into blocks. However, equal messages will then have equal encryptions. We can resolve this problem using the counter design which encrypts messages with an increasing counter.

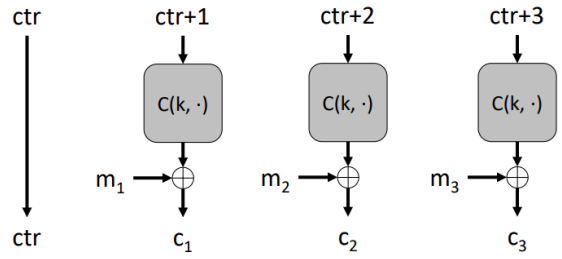

Figure 17.2. Generating new one-time pad for each block, adopted from lecture slides

Iterated Block Ciphers

Both the encryption and the decryption contains n rounds, where we have a key for each round. Denote the round function using R, the state after round i as s_i, and the key for round i as k_i, our encrypting and dycrypting procedure looks like:

17.4.3 Feistel Networks

This is a iterated block ciphers design used by DES(Data Encryption Standard) where the round function doesn't need to have an inverse. To decrypt, we simply run with round keys in reverse order.

17.4.4 Permutation Network

This design nicely introduces the avalanche effect, where changing one bit of input m bit will affect all of c.

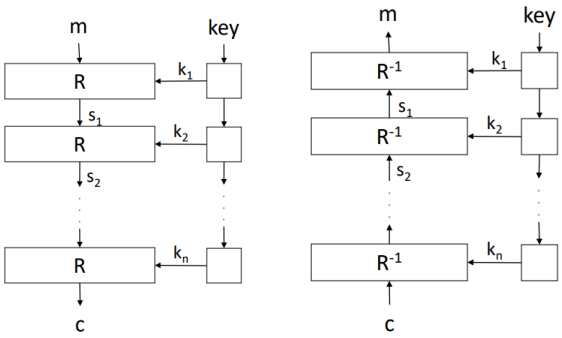

Figure 17.3. Iterated Block Ciphers Encryption and Decryption, adopted from lecture slides

17.4.5 Rijindael

Goals

- Resistance against known Attacks
- Speed and Memory Efficiency across Platforms
- Design Simplity
- Clarity of Security Goals

Overview

Rijindael is an iterated block cipher that is mathematically resonably sophisticated. It consist of

- 10-14 rounds
- 128-256 bit blocks
- 128-256 bit keys

and it is selected by AES(Advanced Encryption Standard) as the new private-key encryption standard.

17.4.6 Performance Comparison

Algorithm	Bits/key	Mbits/sec
DES-cbc	56	399
Blowfish-cbc	128	703
Rijindael-cbc	128	917

17.5 Groups Theory Review

Details available in section **3.5** of the scribe note of Lecture 3.