Week 2: Intro to symmetric key

David Thomson
dthomson@math.carleton.ca

Carleton University

September 15, 2013

Symmetric key cryptography

Cryptosystems today are broken into two major classes: symmetric key and public key.

Today (and in this class), we will mostly focus on symmetric key, whereas MATH 4809 focuses on public-key cryptography. We'll pick up RSA and perhaps some DLOG stuff later.

Claude Shannon

Just about all of the technology we use today was essentially determined by Shannon.

Shannon conceived one of the basic postulates of information theory: that information can be treated as a measurable quantity. For example, we have bounds (called the Shannon capacity) on the amount of information (i.e., number of bits) that can be transmitted through various media (channels).

He also has a landmark paper "Communications theory of secrecy systems" (1949), which outlines the priciples of modern cryptography.

Some of Shannon's definitions

Definition. A (true) secrecy system is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms).... The transformations are supposed reversible so that unique deciphering is possible when the key is known. The choice of a key determines a particular transformation in the set forming the system.

The method of confusion is to make the relation between the simple statistics of (the intercepted cryptogram) E and the simple description of (the key) K a very complex and involved one.

In the method of diffusion the statistical structure of the message which leads to redundancy is "dissipated" into long range statistics–i.e., into statistical structure involving long combinations of letters in the cryptogram.

Symmetric key cryptosystems

Shannon's principles are based upon the "hard problem" of determining complex transformations knowing only

- the system being employed (the set of all transformations),
- some encrypted information.

The principles of confusion and diffusion are universal, but were developed before public key crytography was discovered.

Symmetric key cryptosystems

Shannon's principles are based upon the "hard problem" of determining complex transformations knowing only

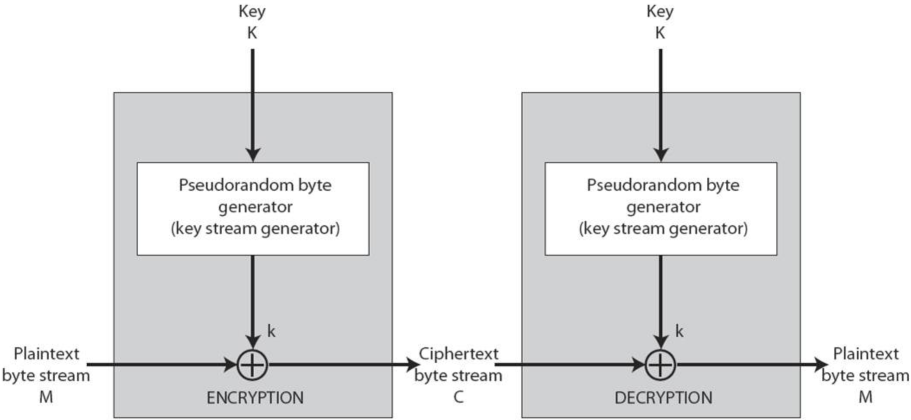
- the system being employed (the set of all transformations),
- some encrypted information.

The principles of confusion and diffusion are universal, but were developed before public key crytography was discovered.

Definition. A symmetric key cryptosystem is a system where the sender and the intended receiver share a secret key. In Shannon's terms, the sender and receiver *a priori* decide upon a transformation.

This is called symmetric key because the receiver uses the inverse of the same transformation as the sender. Mechanically, this is equivalent to feeding the message through the cipher backwards.

Stream ciphers


Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

What properties do we need?

Stream ciphers can be looked at as an approximation of the one-time pad.

To be considered secure, a stream cipher needs:

1. A large period,
2. "good randomness properties".

Moreover, stream ciphers are usually preferred in resource-constrained devices. They should be implemented very quickly and cheaply in hardware, though they are also used in software, e.g., WEP for 802.11.

A perfect application of stream ciphers is for wireless sensor networks.