Message confidentiality

Pieter van den Hombergh

Fontys Hogeschool voor Techniek en Logistiek

June 6, 2016

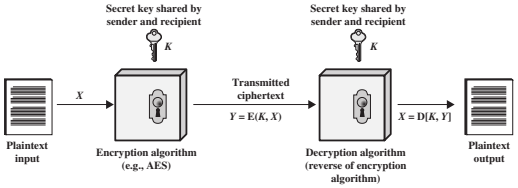
Purpose of Encryption

- Maintain confidentiality
- Best way to keep something secret is not to share it.
  Effective against gossip,
  but not very useful sharing the information is essential.
  Think bank information, account, pin but also business plans or strategi
- Thinking military is a good starting point: Paranoid.

Terminology

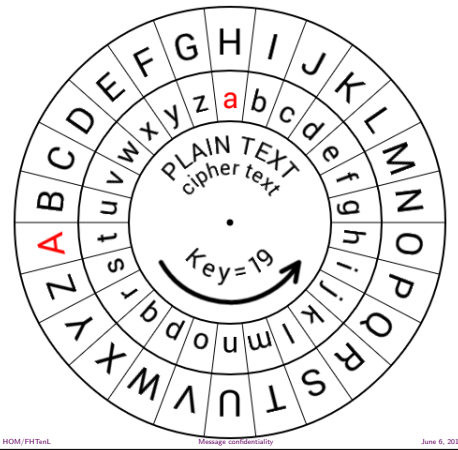
- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering ciphertext from plaintext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (code breaking) - study of principles/methods of deciphering ciphertext without knowing key
- Cryptology - field of both cryptography and cryptanalysis

Simplified diagram symmetric encryption



Same keys use at both transmitting and receiving end. Both key must be kept secret, making sharing the keys risky.
source: Network Security Essentials. W. Stallings

Old Cipher



Message confidentiality
HOM
Purpose
Terminology
block
Using Mathematical Operations
stream
study

Caesar cipher explained

- Based on substitution of characters of characters over fixed distance or rotation. (See picture on previous page).
- Used by Julius for private correspondence.
- Easily broken, no communication security.
- Is application of modulo arithmetic.
  - Encryption $E_n(x) = (x + n) \mod 26$.
  - Decryption: $D_n(x) = (x + 26 - n) \mod 26$.

source
`https://en.wikipedia.org/wiki/Caesar_cipher`

Message confidentiality
HOM
Purpose
Terminology
block
Using Mathematical Operations
stream
study

Enigma

see NumberPhile on Enigma

The military version of the enigma had some important modifications over the original, mainly the patch panel (plug board).
The encryption was actually quite strong. It was mainly the flaws in the procedures, predictability of the plain text, and the availability of key tables and the hardware that helped crack the code.

Message confidentiality
HOM
Purpose
Terminology
block
Using Mathematical Operations
stream
study

Advantages and disadvantages of Symmetric Encryption

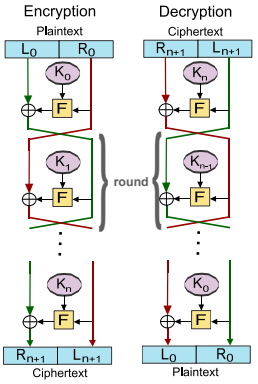
- ✓ Can be used for broadcast (multiple receivers for one encryption.)
- ✗ Distributing keys can be complex.
- ✓ Typically cheaper (faster)

Message confidentiality
HOM
Purpose
Terminology
block
Using Mathematical Operations
stream
study

Mathematical operations

- ✗ Bit wise OR and AND loose information.
- Addition (also subtraction) increase the amount of information.
- (integer) division looses information.
- Multiplication increases the amount of information.
- ✓ Bit wise XOR does **not**. It is in fact modulo 2 addition.

Feistel Circuit, block cipher



- The stream run from top to bottom in both cases.
- The keys in decryption are in reversed order w.r.t. the encryption.
- In every round, half of the block is encrypted with K_i and xor-ed with the other half then swaps places with the other half for the next round.
- The "key" is a/the combination of all K_i.

`source Feistel Cipher`

AES /Rijndael

Developed by Dr. Joan Daemen and Dr. Vincent Rijmen of Belgium, and selected as the winner of the NIST competition for finding a replacement of DES and 3DES.
AES is a slight modification of Rijndael.
AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.
Unlike its predecessor DES, AES does not use a Feistel network
source `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

Crypto strength

Key size (bits)	Cipher	Key space	Time at $10^9/s$	Time at $10^{13}/s$
56	DES	$2^{56} \approx 7.2E16$	2^{55} ns $= 1.125yr$	1 hr
128	AES	$2^{128} \approx 73.4E38$	2^{127} ns $= 5.3E21yr$	5.3E17 yr
168	3DES	$2^{168} \approx 3.7E50$	2^{167} ns $= 5.8E33$	5.8E29 yr
192	AES	$2^{192} \approx 6.3E57$	2^{191} ns $= 9.8E40$	9.8E36 yr
256	AES	$2^{256} \approx 1.2E77$	2^{255} ns $= 1.8E60$	1.8E56 yr

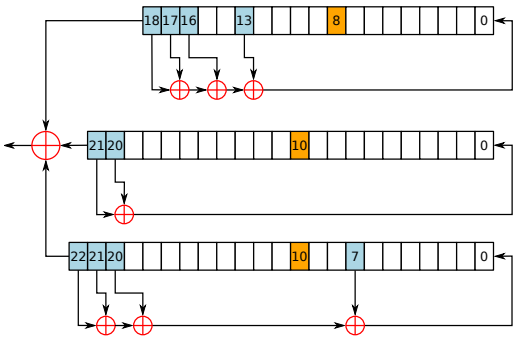
The importance of Random numbers

The generation of **random numbers** is essential to cryptography.
One of the most difficult aspect of cryptographic algorithms is in depending on or generating, true random information. This is problematic, since there is no known way to produce true random data, and most especially no way to do so on a finite state machine such as a computer.

Stream Cipher

- Encrypt the data as they pass by, not in blocks but typically as bits (real serial stream) or bytes (which are tiny blocks).
- Bit streams are easily done in hardware, but unnatural for modern byte or word oriented general purpose CPU's.
- Application: streaming data, audio, video.
- Use of Linear Feedback Shift Registers (LFSR) is common, again in combination with XOR.
- Combined with a one time pad (of the same length as the message) makes it unbreakable (proof by CE Shannon, 1949)
  - This one time pad needs to be transported using another route, making this approach unworkable, but for most critical applications.

A5/1, GSM cipher



The GSM A5/1 cipher, now considered insecure. From wikipedia.
`https://en.wikipedia.org/wiki/Stream_cipher`

Study for this week

Study the mentioned wikipedia pages

- `https://en.wikipedia.org/wiki/Cryptographic_primitive`
- `https://en.wikipedia.org/wiki/Stream_cipher`
- `https://en.wikipedia.org/wiki/Caesar_cipher`
- `https://en.wikipedia.org/wiki/Feistel_cipher`
- `https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`

Watch the videos at youtube (Numberphile and Computerphile):

- `https://www.youtube.com/watch?v=8ZtInClXe1Q`
- `https://www.youtube.com/watch?v=G2_Q9FoD-oQ`
- `https://www.youtube.com/watch?v=V4V2bpZlqx8`