Elements of Cryptography. Symmetric Encryption.

NSE, sections 2.1-2.2
WSPC, chapter 3

Cryptography

- Cryptography is a collection of mathematical techniques for protecting information;
- Most important technique is *encryption/decryption;*
- We have discussed already an importance of encryption/decryption in several contexts, for example:
  - Protection of message content from disclosure;
  - Providing anonymity in Mix-networks;
  - Providing anonymity in DC-networks;
  - etc

Cryptography for information protection

Level	What to protect	Method
3	Existence of message	Steganography
2	Metadata of message	Privacy-enhancing technologies
1	Content of message	Encryption
0	Nothing	None

Table by I.A. Goldberg

Cryptography is used
- Directly at the level 1
- As an important ingredient at the levels 2 and 3

Two categories of encryption algorithms

- Symmetric encryption (or symmetric key encryption):
  - to encrypt and decrypt a message the *same key* (a piece of information; sequence of bits) is used
- Asymmetric encryption (or asymmetric key encryption):
  - One key is used for encryption (usually publicly known, *public key*);
  - Another key is used for decryption (usually *private*, or *secret* key)

Symmetric (conventional) encryption

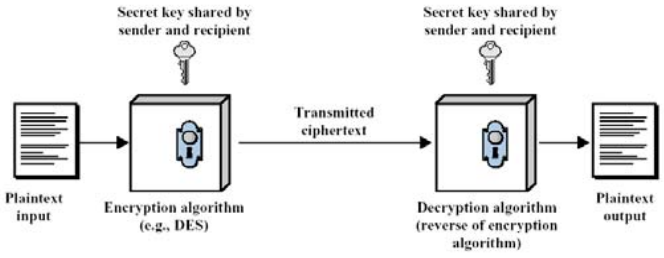

Figure 2.1 Simplified Model of Symmetric Encryption

Components of Symmetric Encryption

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext (encrypted text)
- Decryption algorithm

Security of symmetric encryption

Important principle:

security of symmetric encryption depends on

- the secrecy of the key,
- Not the secrecy of the algorithm

Why?

- It is difficult to *invent* new algorithms and *keep* them in a secret;
- Producing keys is much easier;

Requirements for symmetric encryption

- *Strong* encryption algorithm:
  - The adversary (opponent) should be unable to decrypt encrypted text, even if he/she knows several pairs (plaintext, encrypted plaintext)
- Sender and receiver must have obtained copies of the secret key in a secure way and *must keep the key secure*

Two more classifications of cryptosystems

- **Type of operations used**
  - Substitutions;
  - Transpositions;
- **The way in which plaintext is processed**
  - Block cipher: input block of elements (e.g. characters) is transformed to the output block at once;
  - Stream cipher: processes the input elements continuously, one element at a time.

Classics: substitutions

Each element of the plaintext (bit, letter, group of bits) is mapped to another element

Example:

A -> B
B -> C
C -> D
….
Z -> A

Plaintext **"Knowledge is power"**
is transformed into
"Lopxmfehf jt rpxfs"

Classics: transposition

Elements of the plaintext are re-arranged.

Example: "Knowledge is power"

K n o w l
e d g e
i s p o
w e r

Is transformed into
"Keiwndseog weprl o "

Two remarks

- Most modern algorithms include multiple stages of *interleaving* substitutions and transpositions;
- The encryption uses a *key* (unlike simple examples on the previous slides)

Cryptanalysis and computationally secure schemes

- **Cryptanalysis:** The process of attempting to discover the plaintext or key;
- Depends very much on the information available;
- An encryption scheme is *computationally secure* if
  - The cost of breaking the scheme exceeds the value of the encrypted information;
  - The time required to break the scheme is more than lifetime of the information;

Types of Attacks (Cryptanalysis)

Table 2.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Brute-Force Approach in Cryptanalysis

- If nothing else helps and there is no weakness in the encryption algorithms, brute-force approach may be applied;
- Try every possible key until correct translation of the encrypted text into plaintext is obtained;
- **Possible issue**: how does cryptanalyst recognize correct plaintext? Imagine it has been compressed before encryption;
- **Main issue:** time !!!

Time required for brute-force search

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years