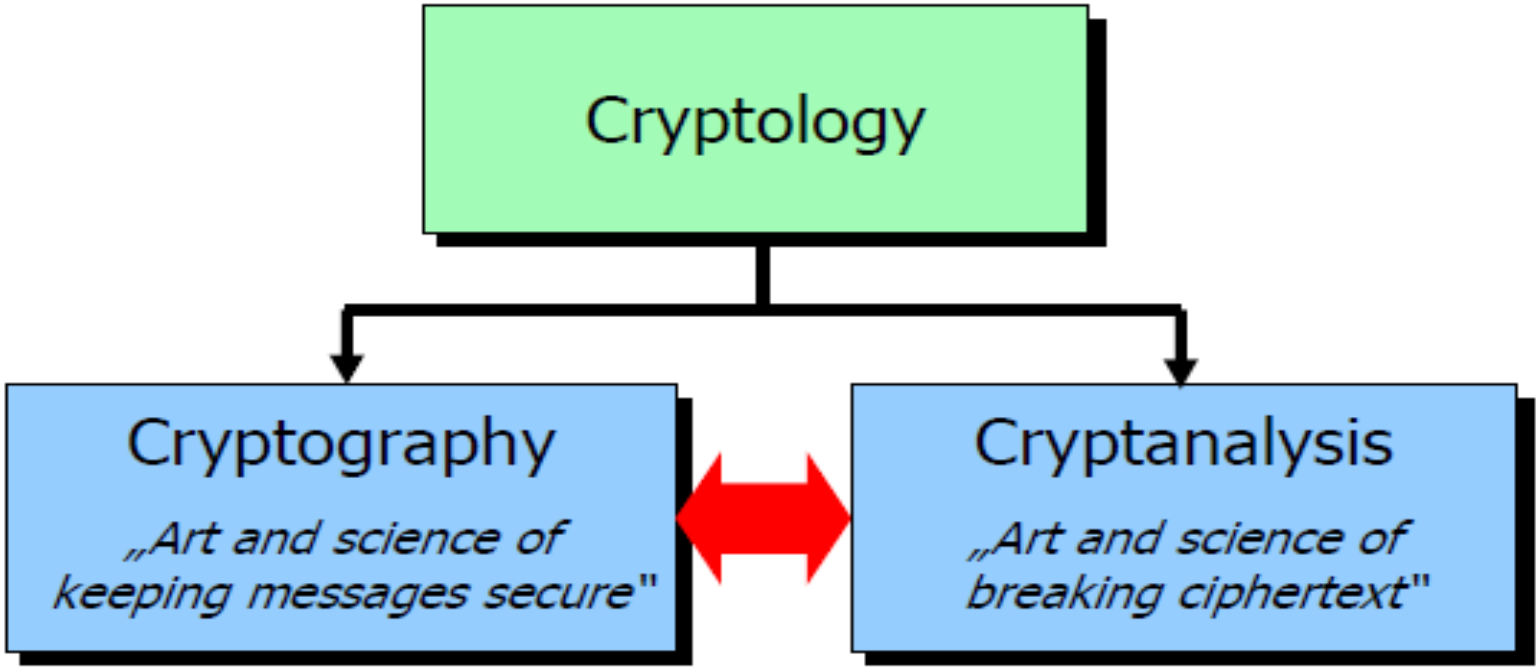
Terminology and classical Cryptology

By

Hafez Barghouthi

What is Cryptology?



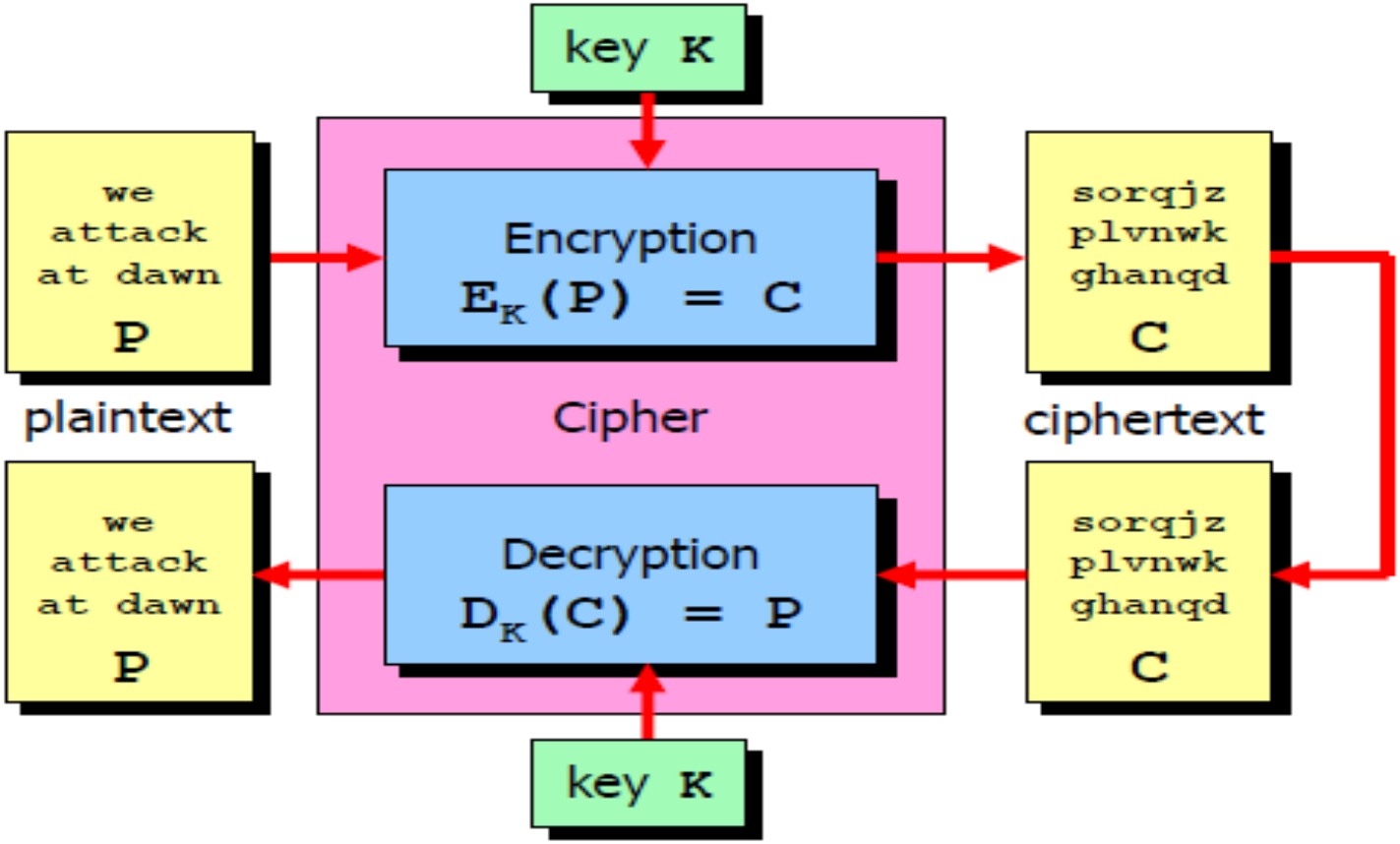
Cryptology is a branch of mathematics !!

Terminology

- The art and science of keeping messages secure is ***cryptography,*** and it is practiced by ***cryptographers.***
- ***Cryptanalysts*** are practitioners of ***cryptanalysis***, the art and science of breaking cipher text.
- The branch of mathematics encompassing both cryptography and cryptanalysis is ***cryptology*** an its practitioners are ***cryptologists***.
- Modern cryptologists are generally trained in ***theoretical mathematics*** (they have to be ☺).

Source: Bruce Schneier, „Applied Cryptography", Second Edition, p. 1,John Wiley & Sons, 1996

Terminology-2



Terminology-3

- A message is **plaintext** (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is called **encryption.**
- An encrypted message is **ciphertext.** The process of turning ciphertext back into plaintext is called **decryption.**
- A **cryptographic algorithm**, also called a **cipher,** is the mathematical function used for encryption and decryption.
- The security of a modern cryptographic algorithm is based on a **secret key.**
- This key might be any one of a large number of values. The range of possible
- key values is called the **keyspace.**
- Both encryption and decryption operations are dependent on the key K and this is denoted by the K subscript in the functions **$E_K(P) = C$ and $D_K(C) = P$.**

Fundamental Assumptions

The security of a cipher should rely on the secrecy of the key only!

Auguste Kerckhoffs, „La Cryptographie militaire", 1883

Fundamental Assumptions-2

- Attacker knows every detail of the crypto-graphical algorithm
- Attacker has an encryption / decryption equipment (HW machine or SW implementation)
- •Attacker has access to an arbitrary number of plaintext /ciphertext pairs generated with the same (unknown) key.
- Strong cipher: Best attack should be brute force key search!

Types of Attacks (cryptanalysis)

- **Ciphertext-Only Attack**
  - Attacker knows cipher text of several messages encrypted with the same key and/or several keys.
  - Recover the plaintext of as many messages as possible or even better deduce the key (or keys).
- **Known-Plaintext Attack**
  - Known cipher text / plaintext pair of several messages.
  - Deduce the key or an algorithm to decrypt further messages.
- **Chosen-Plaintext Attack**
  - Attacker can choose the plaintext that gets encrypted thereby potentially getting more information about the key
- **Adaptive Chosen-Plaintext Attack**
  - Attacker can choose a series of plaintexts, basing the choice on the result of previous encryption → differential cryptanalysis!

History evidence

Mary Stuart
Queen of Scotland

Elizabeth I
Queen of England

Codes have decided the fates of empires throughout recorded history

• Mary Stuart, Queen of Scotland was put to death by her cousin Queen Elizabeth of England, for the high crime of treason after spymaster Sir Francis Walsingham cracked the secret code she used to communicate with her conspirators.

Source: Simon Singh, „The Code Book“, Doubleday, 1999

Cryptanalysis is not just for fun ☺.

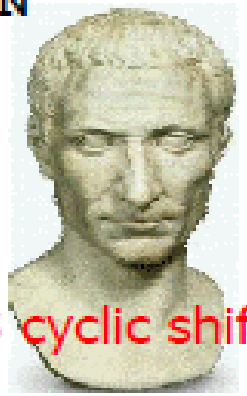
Caesar Monoalphabetic Substitution Cipher

MESSAGE FROM MARY STUART KILL THE QUEEN

Substitution Table - Caesar's Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC ← key = 3 cyclic shifts



PHVVD JHIUR PPDUB VWXDU WNLOO WKHTX HHQ

General Substitution Table

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EYUOBMDXVTHIJPRCNAKQLSGZFW ← 26! possible keys

JBKKE DBMAR JJEAF KQLEA QHVII QXBNL BBP

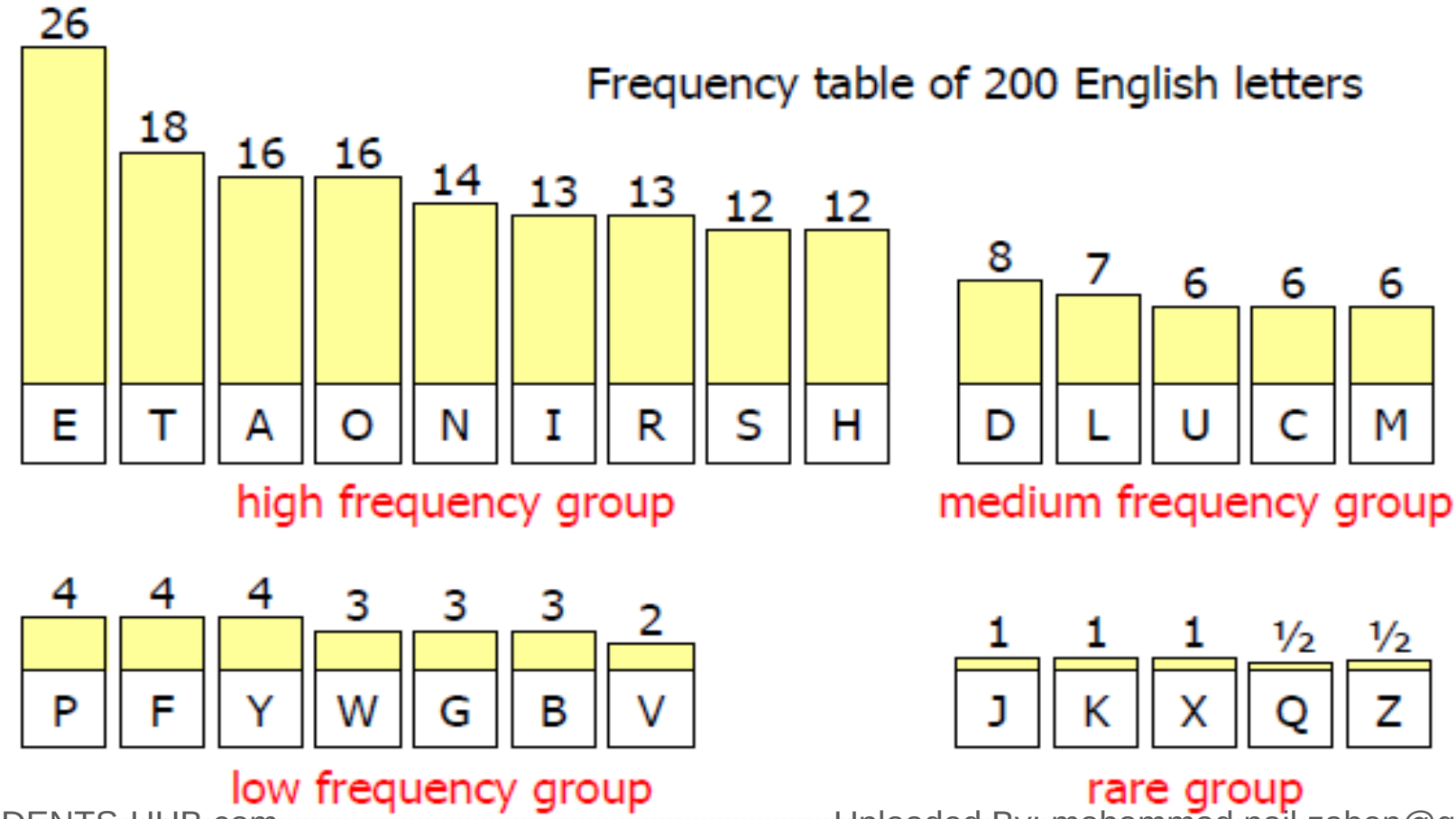
Monoalphabetic Substitution (old and weak but not bad)

- Each character in an alphabet is replaced by another character in the same alphabet or sometimes even by a symbol of a different alphabet.
- 26! Different keys it seem to be secure.
- Each occurrence of a specific plaintext character is always mapped to the same cipher text character.
- Weak against count statistics of natural language plaintexts.
- Not bad coz great Idea
- **Substitution using S-Boxes**

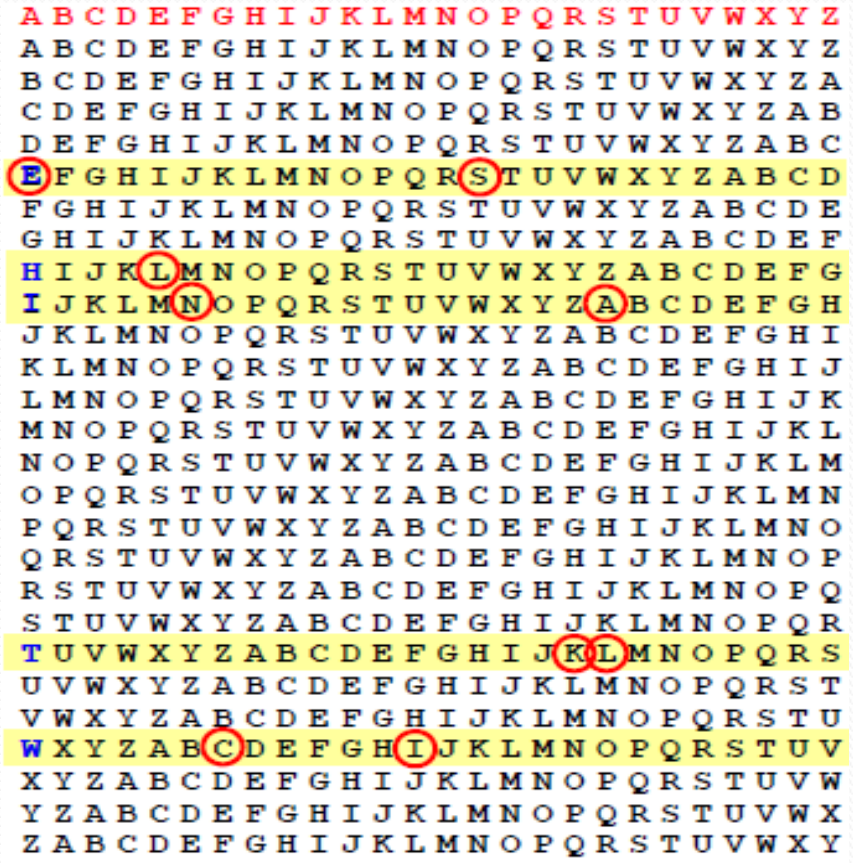
  • In modern ciphers a fixed number of plaintext bits are grouped together and are substituted by a different bit combination according to a fixed lookup table.

  • A software or hardware module which implements this substitution operation is called an **S-Box.**

Redundancy of Natural Language Texts



Vigenère Polyalphabetic Substitution Cipher



plaintext alphabet

Vigenère square

Keyword: **WHITE**

MESSAGE FROM ...

WHITEWH ITEW

ILALECL NKSI

Poly alphabetic substitution

- Effectively smears the characteristic statistics of natural language text.
- For a long time was thought to be unbreakable.
- Problem of long period using the key.
- A frequency analysis can be effected on each individual alphabet.

How to construct a Secure Cipher?

World War II German Enigma Machine

1 0 1 0 0 1 1 1 0 1 . . .

Thomas Jefferson's Cipher Wheel

Thomas Jefferson‘s Cipher Wheel

- Protect communications from England and France to the U.S
- Device consisted of an iron spindle and a screw used to keep 36 distinct wooden wheels fixed in place.
- On each of the numbered wheels the 26 letters of the alphabet were engraved on the circumference in arbitrary order, so that no two cylinder had the same order.
- In order to encrypt a plain text, the letters were arranged on a single line by aligning the individual wheels accordingly.
- The cipher text could then be read off by selecting any other line of the cylinder.

The German Enigma

- The Enigma was an electromechanical rotor machine implementing a poly alphabetic substitution cipher.
- It was used by the German Wehrmacht and Kriegsmarine to encrypt most of its communications.
- Due to several weaknesses both in the implementation and the usage of the machine, the cipher could be broken by the British.

Claude Shannon 1916 - 2001

- The Father of Information Theory
- Model of a secrecy system.
- Definition of perfect secrecy.
- Basic principles of „confusion“ and „diffusion“.

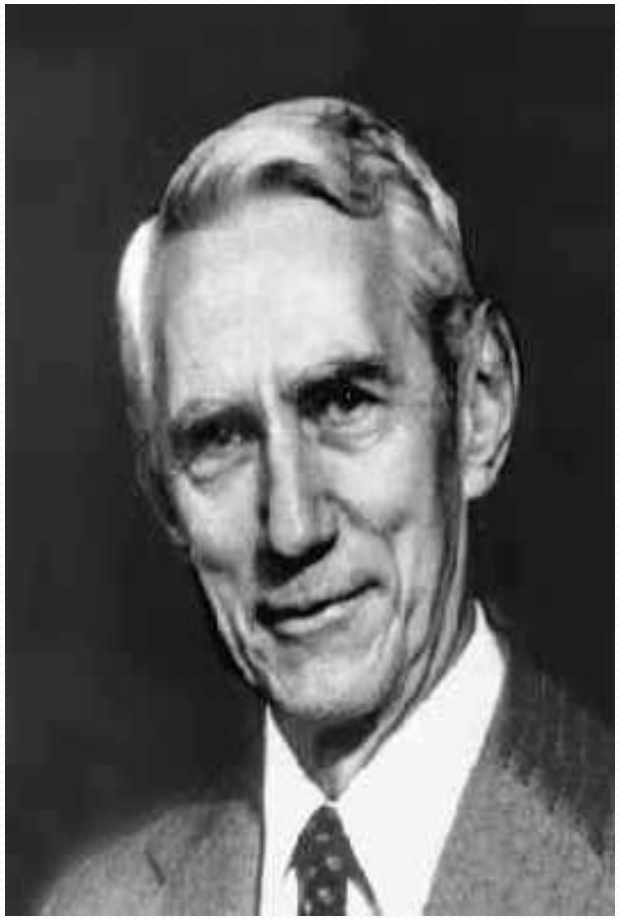
Basic Principles of „Confusion“ and „Diffusion“

•Shannon was the first to formulate these two principles explicitly,

„confusion“ standing for substitution operations and

„diffusion“ standing for transposition or permutation operations.

These two principles are still actively used in modern ciphers.



confusion

- Caesar and Vigenère cipher.
- S-Box in modern cipher.

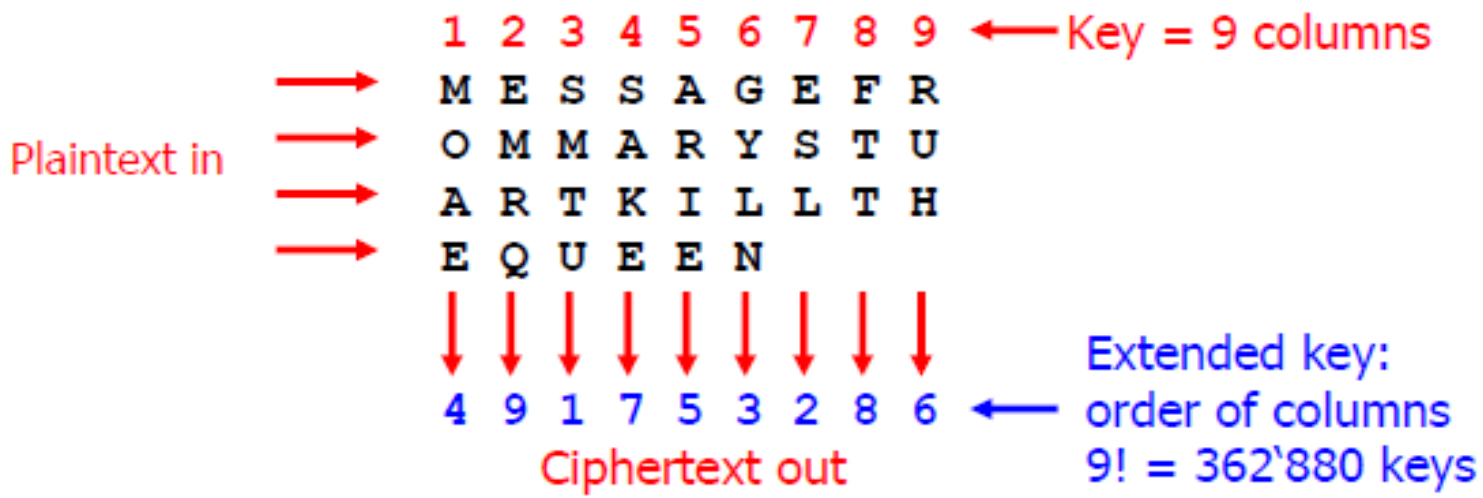
Transposition Cipher

- In a classical transposition cipher the plaintext is written on a piece of paper in horizontal rows of *c characters each*.
- The ciphertext is read out vertically column after column
- The columns could be chosen in any order.

- In modern ciphers a fixed number of bits are written in linear order into a buffer and are read out in a permuted order controlled by a fixed lookup table.
- A software or hardware module which implements this permutation operation is called a **P-Box.**

Transposition Cipher-1

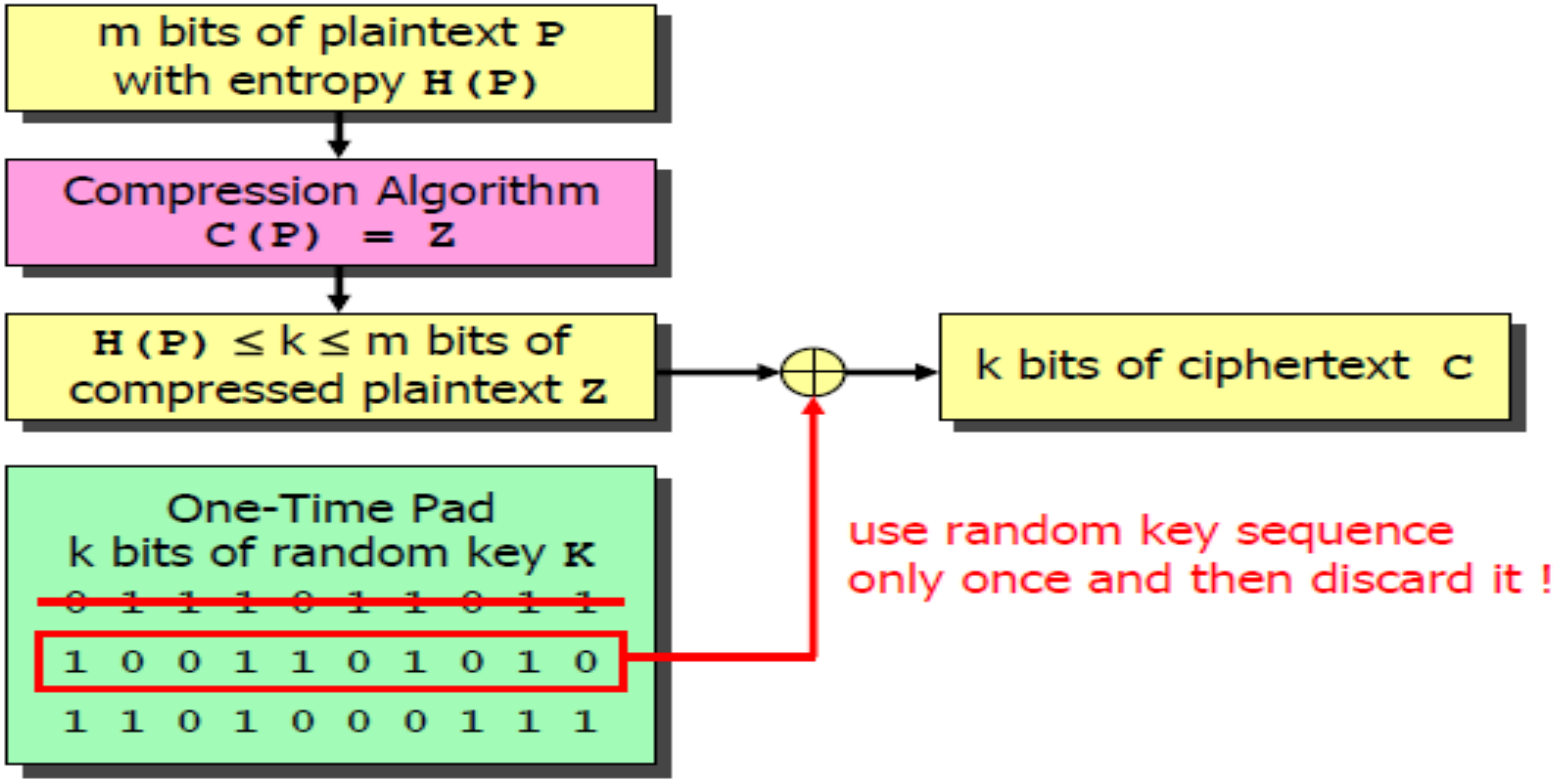
MESSAGE FROM MARY STUART KILL THE QUEEN



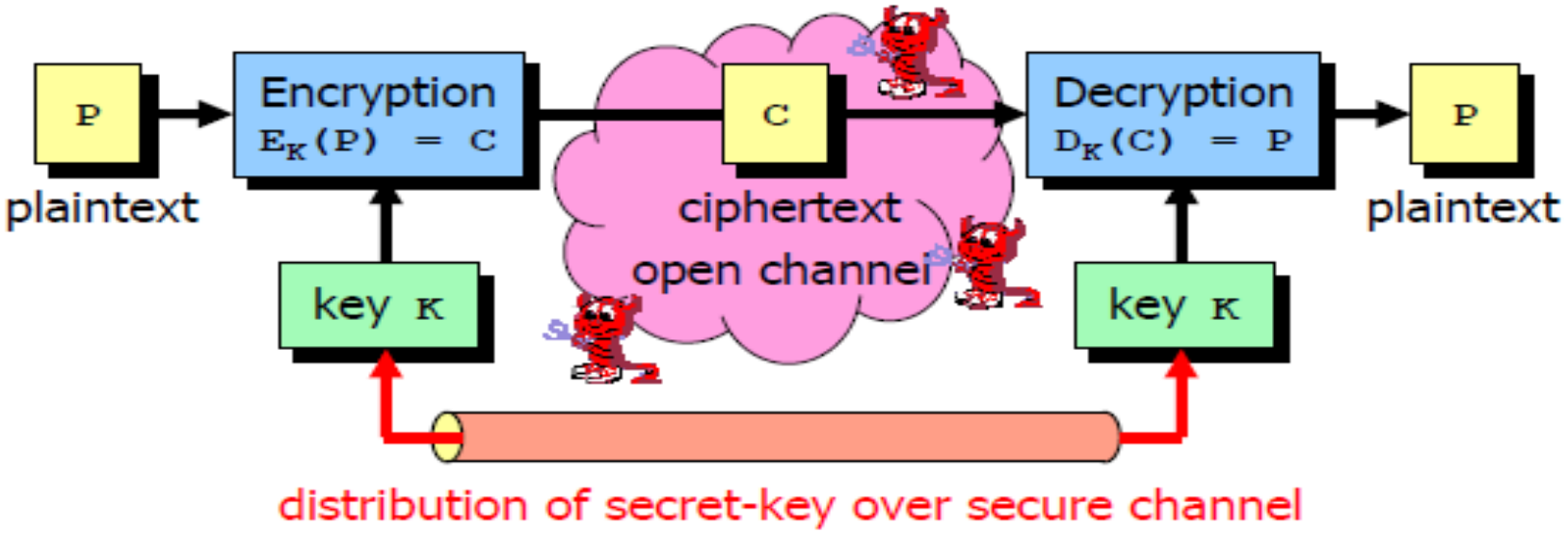
MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH
SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

Diffusion means permutation of bit or byte positions !

Perfect secrecy



Shannon‘s Model of a Secrecy System



- Same key used for encryption and decryption
- Key must be kept absolutely secret
- Same key can be used for several messages, but should be changed periodically → secure key distribution problem!