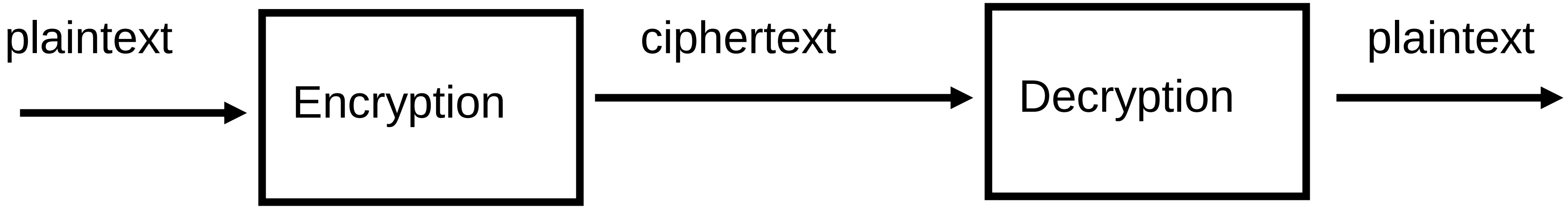
Classical Ciphers Analysis

Computer Science and Engineering
Indian Institute of Information Technology Sri City, India

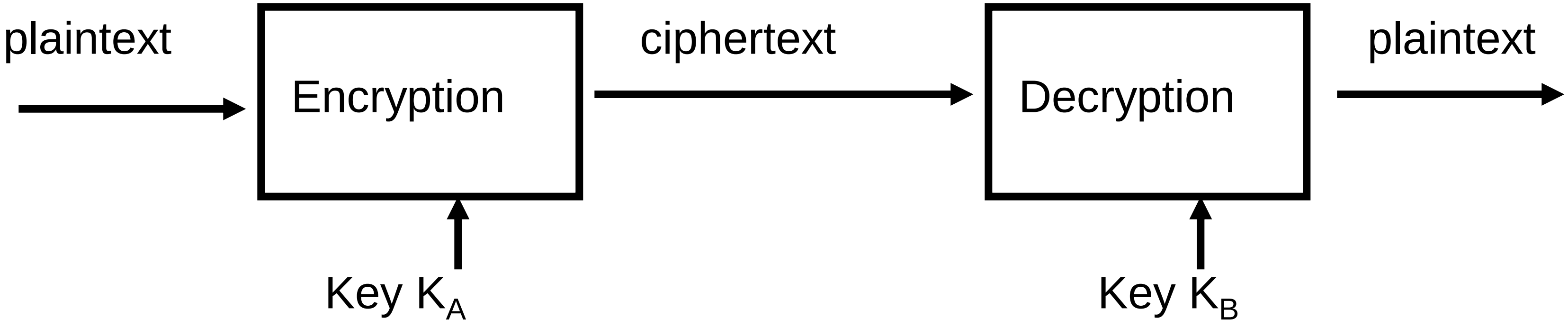
Cryptography



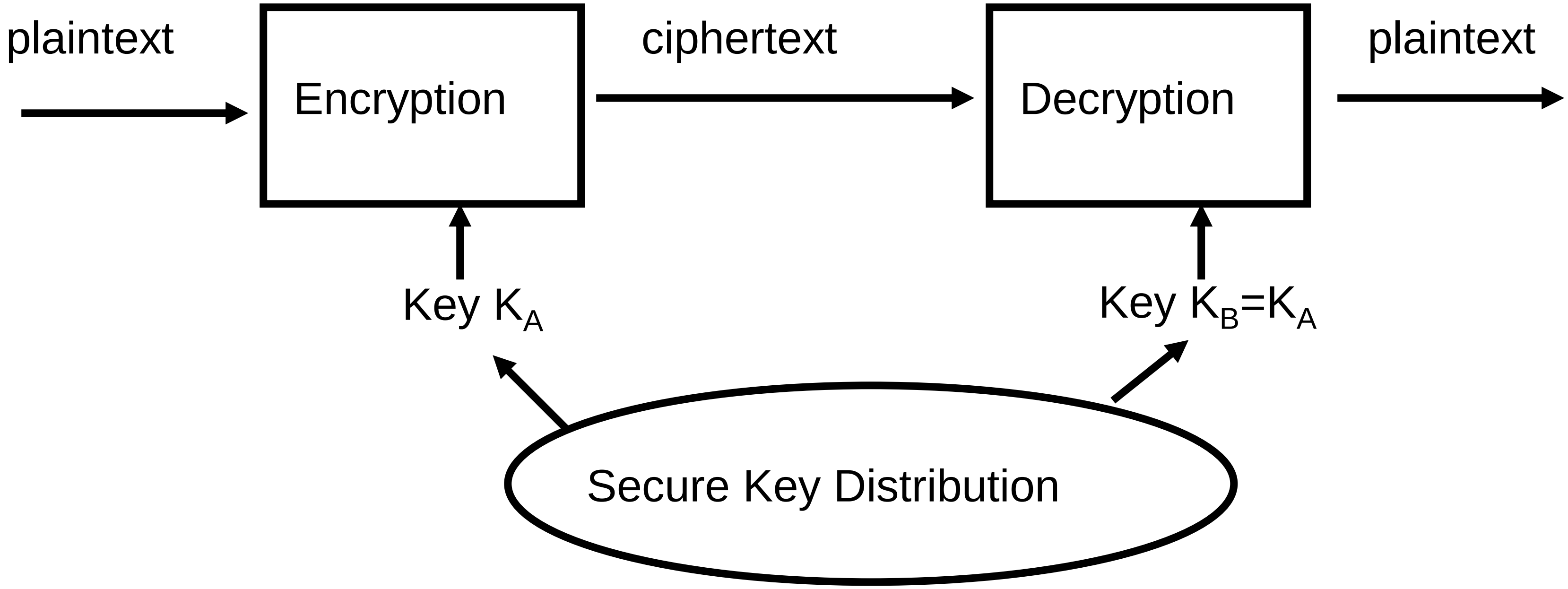
- Encryption algorithm also called a cipher
- Cryptography has evolved so that modern encryption and decryption use secret keys

Kerckhoffs' Principle

- Cryptographic algorithms can be openly published
- Only have to protect the keys



Symmetric-Key Cryptography



- Both sender and receiver keys are the same: $K_A=K_B$
- The keys must be kept secret and securely distributed
  - Thus, also called “Secret Key Cryptography”
- Data Encryption Standard (DES)

Classical Techniques

- Substitution Techniques
  - Shift Cipher – Caesar Cipher
  - Affine Cipher
  - Vigenere Cipher
  - Hill Cipher (Tutorial)
- Transposition Techniques
  - Rail Fencing
  - Permutation/Transposition cipher

Transposition cipher techniques

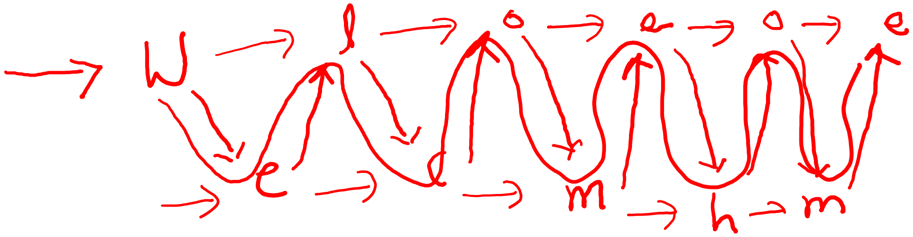
1. Rail Fence Cipher
2. Columnar Transposition
   - Simple Columnar Transposition
   - Double Columnar Transposition

Rail Fence Cipher

- In this method plain text is written downwards on “rails of fence “ , starting a new column when bottom is reached.
- Algorithm:

1. First write down plain text message as a sequence of diagonals.
2. Read the plain text written in first step as a sequence of rows.

Example: welcome home



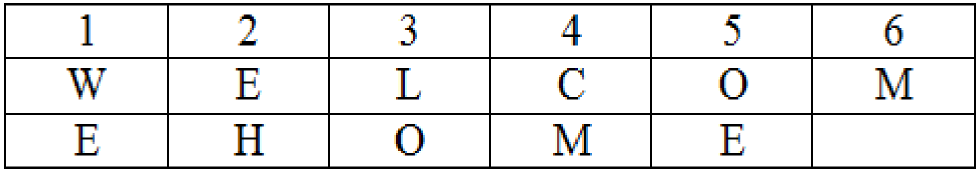
WLOEOE ECMHM

Simple Columnar Transposition

- Algorithm:
  1. Write the plain text message row by row in a rectangle of predefined size (length of key)
  2. Read the message column by column according to the selected order, thus obtained message is a cipher text.

plain text: welcome home

Key : 6 3 2 4 1 5



1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Cipher text:

Double Columnar Transposition

- Single columnar transposition can be attack by guessing possible column lengths.
- Therefore to make it stronger double transposition is used.
- This is simple columnar transposition technique applied twice.
- Here same key can be used for transposition or two different keys can be used.

Double Columnar Transposition

- First apply simple columnar transposition

plain text: welcome home

Key : 6 3 2 4 1 5

1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	Z

Z

Cipher text: MLOEHCMWEOE

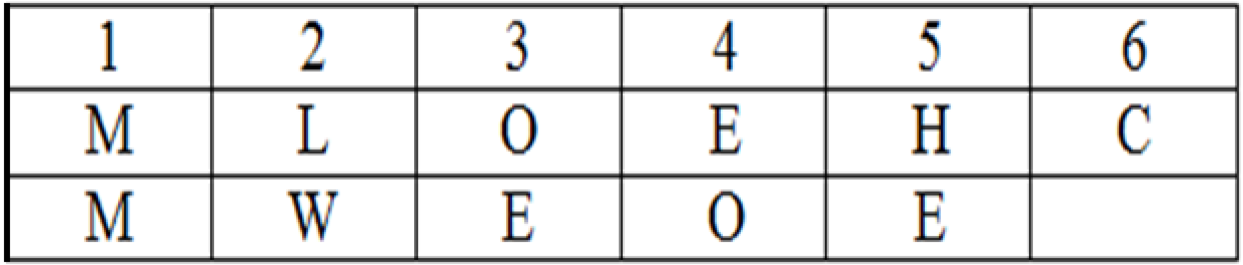
HELWZMOEMCEO

1	2	3	4	5	6
M	Z	L	O	E	H
C	M	W	E	O	E

Double Columnar Transposition

Cipher text 1: MLOEHCMWEOE

Order : 6 3 2 4 1 5



1	2	3	4	5	6
M	L	O	E	H	C
M	W	E	O	E	

Final Cipher Text: COELWEOMMHE

Plaintext : Cryptography Course

Key : 2 3 1 4

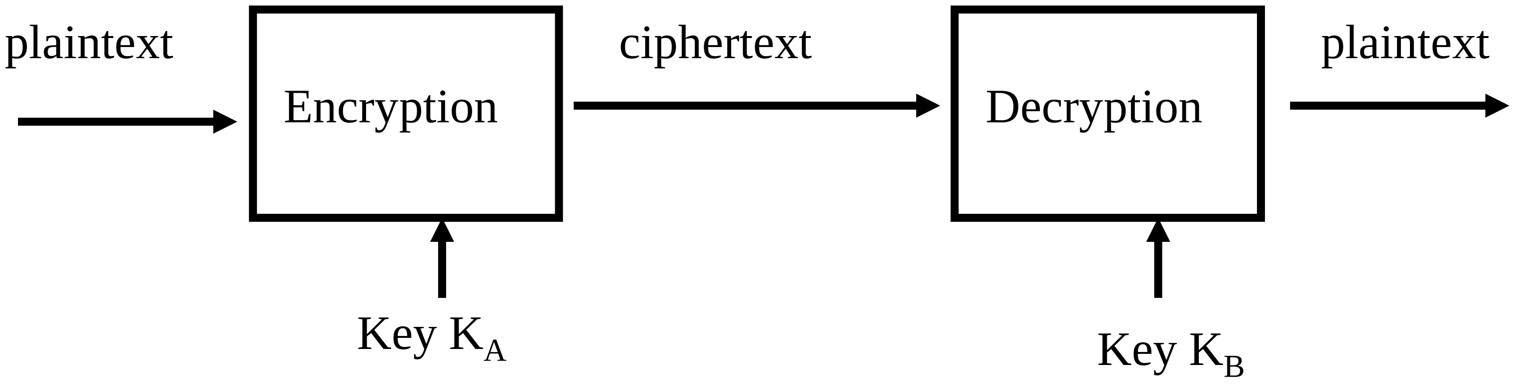
Cyphertext :

⇒ ROPOEYGHUZCTACS
PRYRZ

⇒

1	2	3	4
c	r	y	p
t	o	g	r
a	p	h	y
c	o	u	r
s	e	z	z

Confusion and Diffusion



plaintext

Encryption

ciphertext

Decryption

plaintext

Key K_A

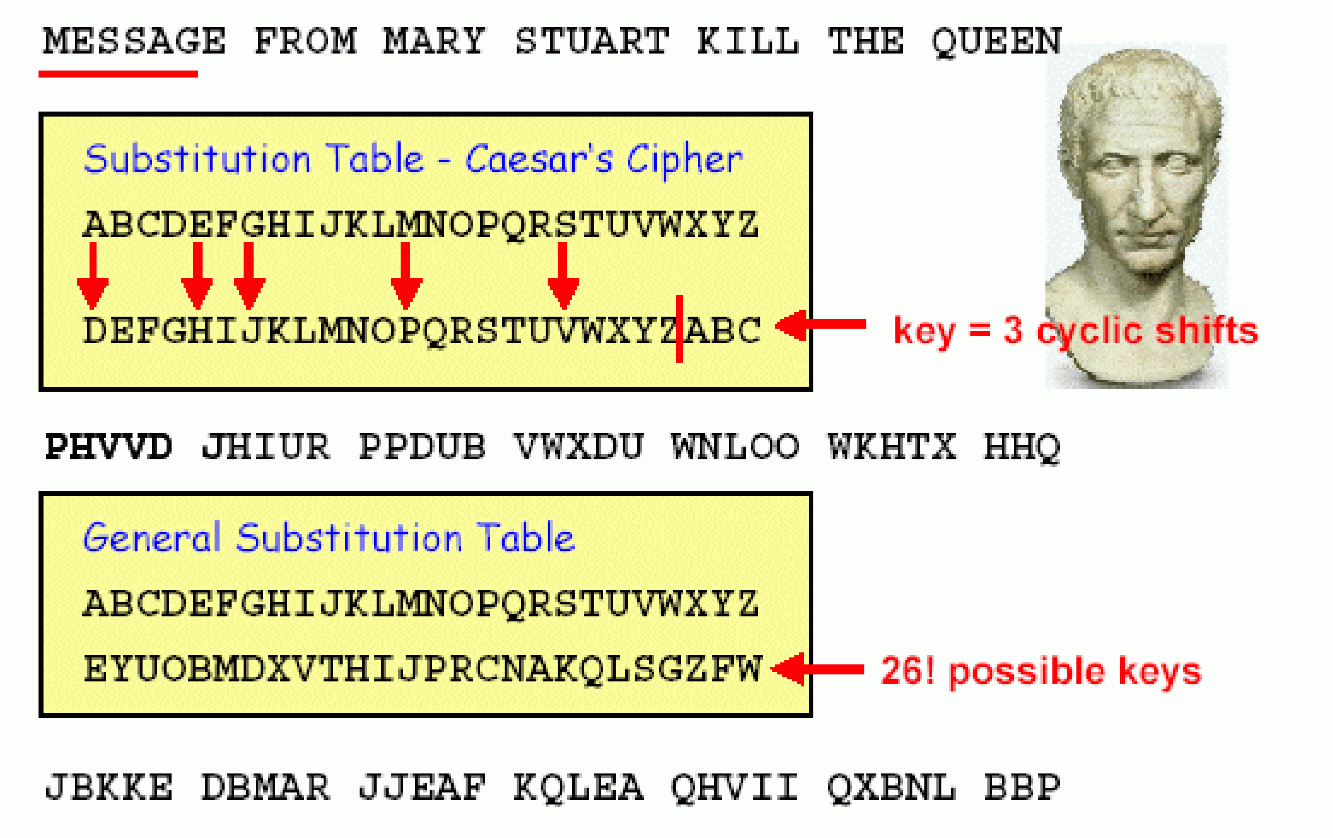
Key K_B

Terms courtesy of Claude Shannon, father of Information Theory

- "Confusion" = Substitution
  - a -> b
  - Caesar cipher
- "Diffusion" = Transposition or Permutation
  - abcd -> dacb

Confusion and Diffusion

- “Confusion” : a classical 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

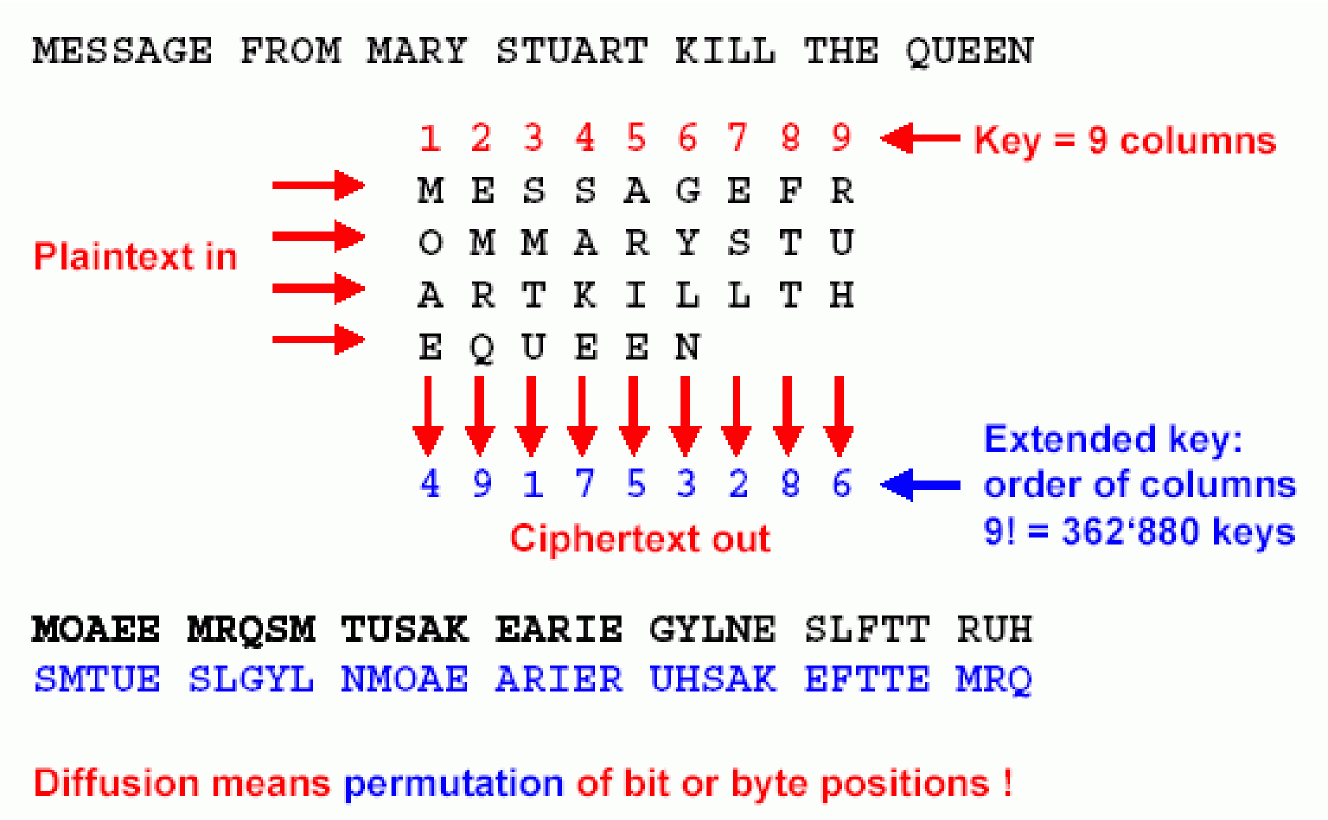
26! possible keys

JBKKE DBMAR JJEAF KQLEA QHVII QXBNL BBP

- Modern substitution ciphers take in N bits and substitute N bits using lookup table: called S-Boxes

Confusion and Diffusion

- “Diffusion” : a classical Transposition cipher



MESSAGE FROM MARY STUART KILL THE QUEEN

Key = 9 columns

Plaintext in

1	2	3	4	5	6	7	8	9
M	E	S	S	A	G	E	F	R
O	M	M	A	R	Y	S	T	U
A	R	T	K	I	L	L	T	H
E	Q	U	E	E	N			
4	9	1	7	5	3	2	8	6

Extended key:
order of columns
9! = 362‘880 keys

Ciphertext out

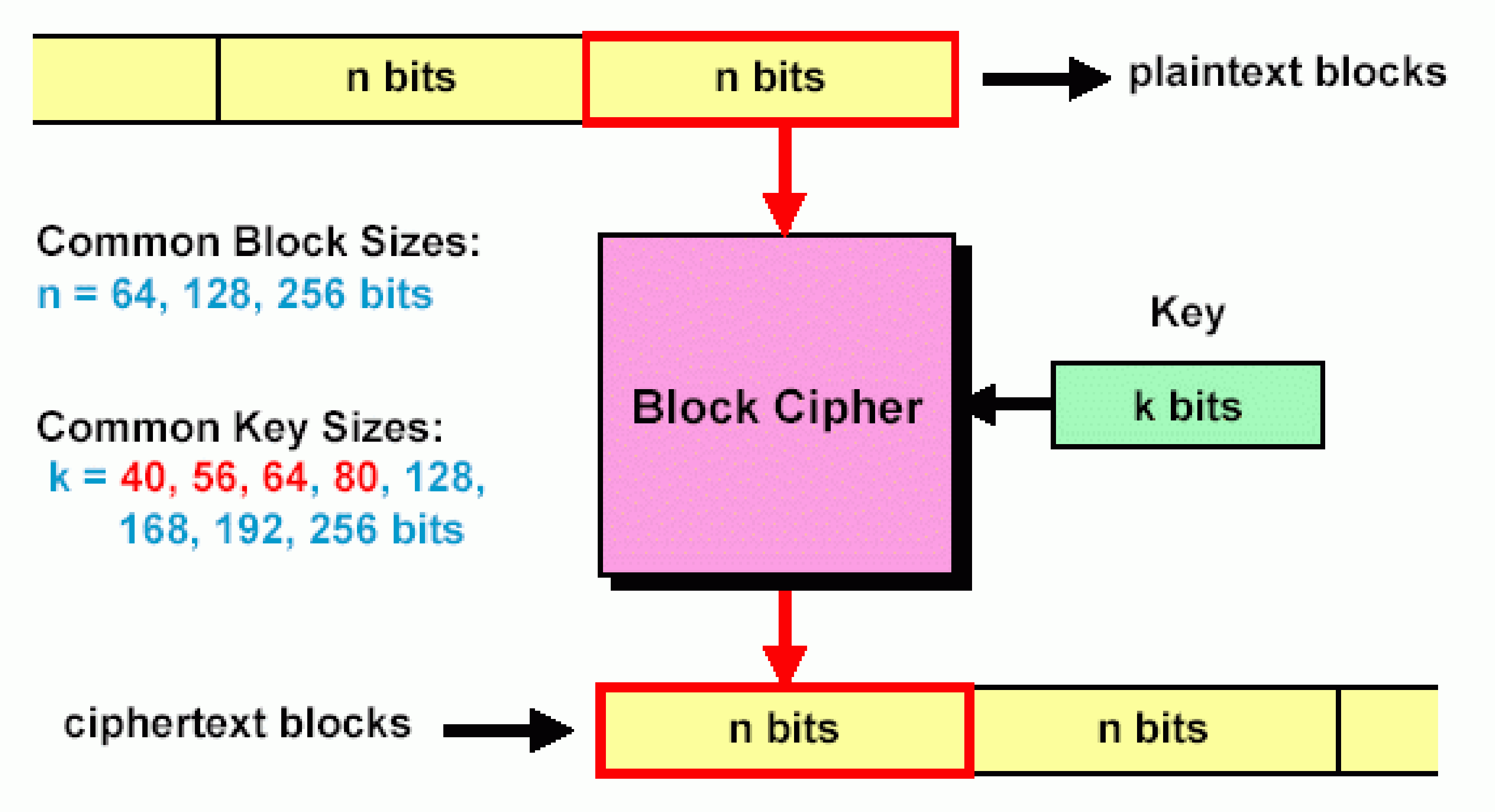
MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH
SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

Diffusion means permutation of bit or byte positions !

- Modern Transposition ciphers take in N bits and permute using lookup table : called P-Boxes

Block Cipher

- Divide input bit stream into n-bit sections, encrypt only that section, no dependency/history between sections



Example: DES

- Data Encryption Standard (DES)
  - Block size 64 bits
  - Key size 56 bits
  - A combination of **diffusion** and **confusion**

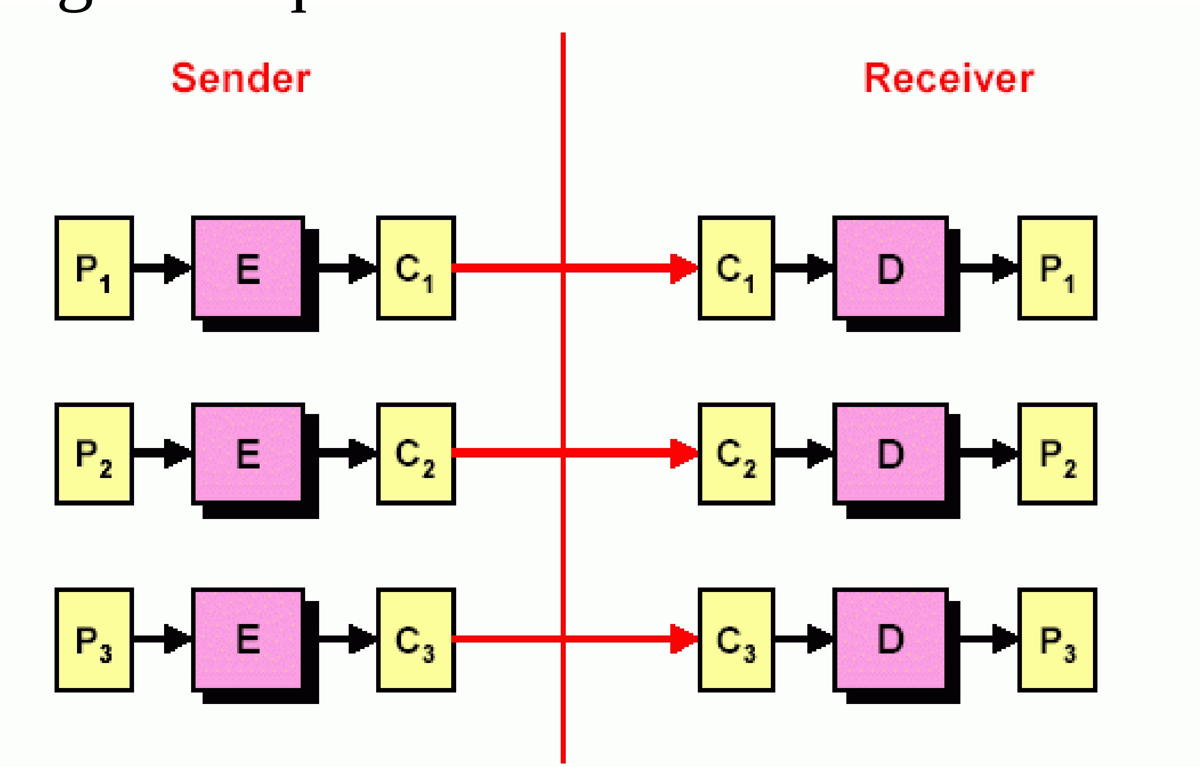
  - Cracked in 1997
    - Parallel attack – exhaustively search key space

Beyond DES

- **Triple-DES:**
  - put the output of DES back as input into DES again with a different key, loop again: 3*56 = 168 bit key
- **Advanced Encryption Standard (AES)**
  - Requirements:
    - **The key length may be increased as needed.**
    - **Block size n = 128 bits**
    - **Key size k = 128, 192, 256 bits**
- **Candidates:** MARS, twofish, RC6, Serpent, Rijndael
- **Successor (Rijndael)**

Encryption Mode (ECB)

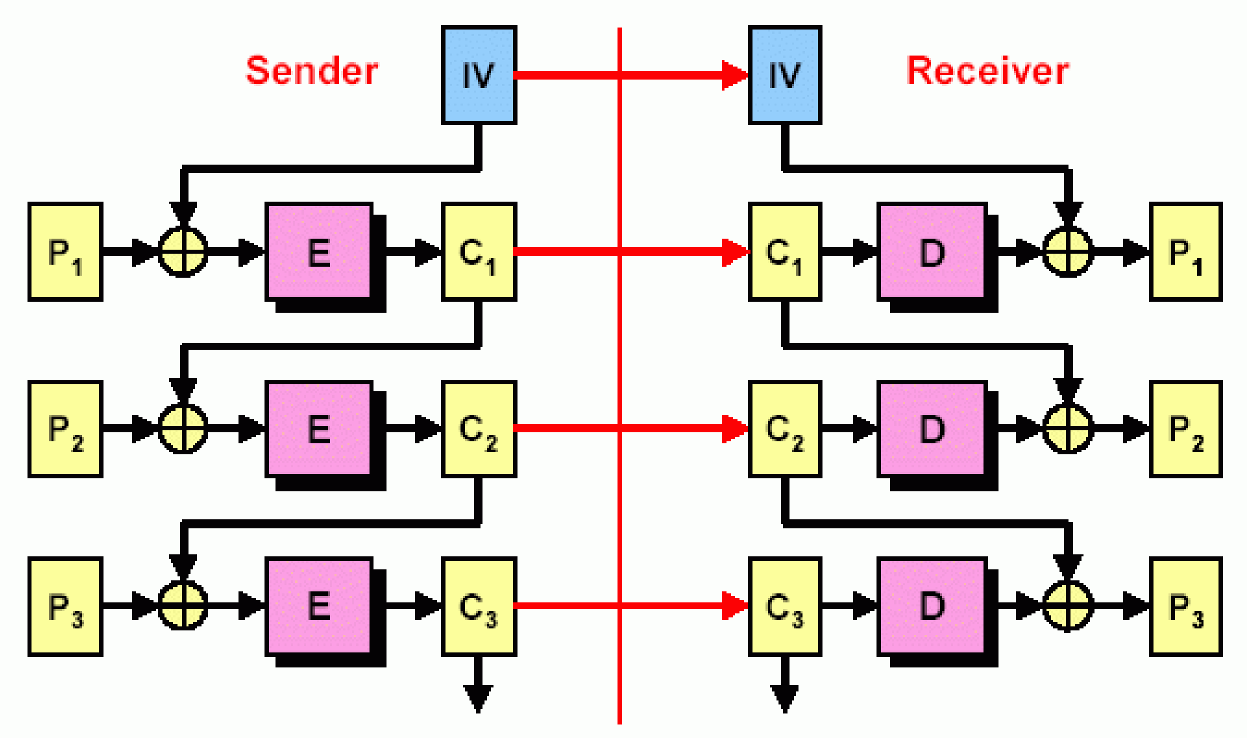
- Electronic Code Book (ECB) mode for block ciphers of a long digital sequence



- **Vulnerable to replay attacks:** If an attacker thinks block C_2 corresponds to X amount, then substitute another C_k
- Attacker can also build a codebook of <C_k, guessed P_k> pairs

Encryption Mode (CBC)

- **Cipher Block Chaining (CBC) mode for block ciphers**



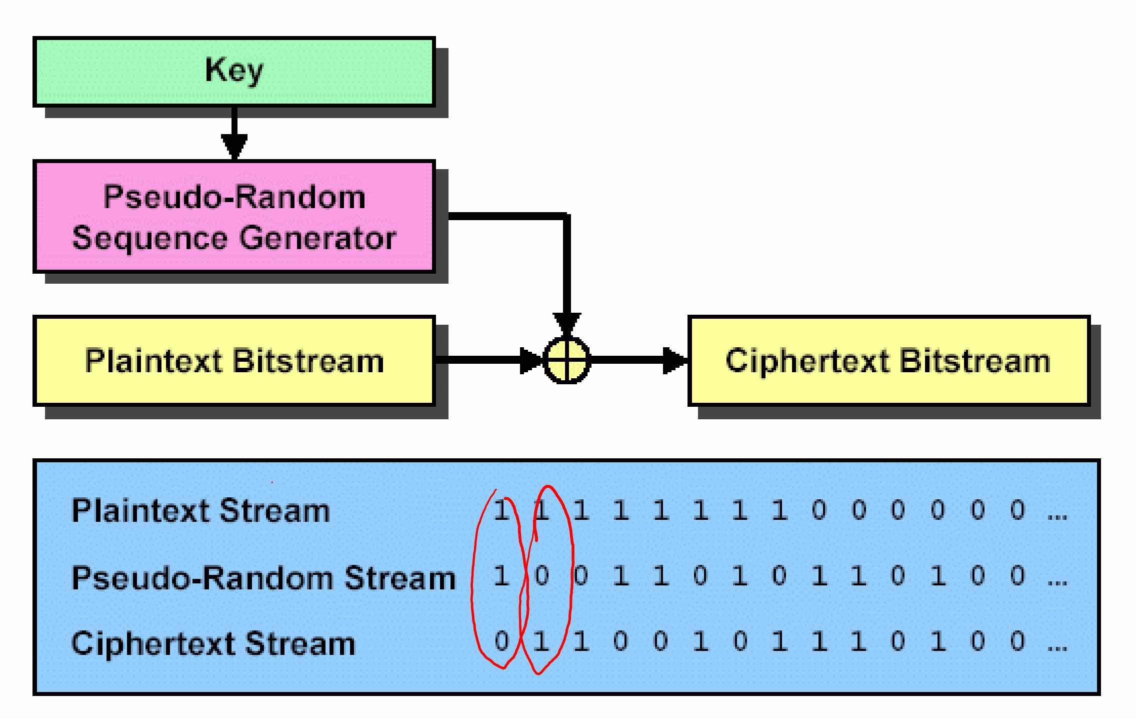
- **Inhibits replay attacks and codebook building:**

  Identical input plaintext $P_i = P_k$ won’t result in same output code due to memory-based chaining

- IV = Initialization Vector – use only once

Stream Cipher

- *Stream* ciphers

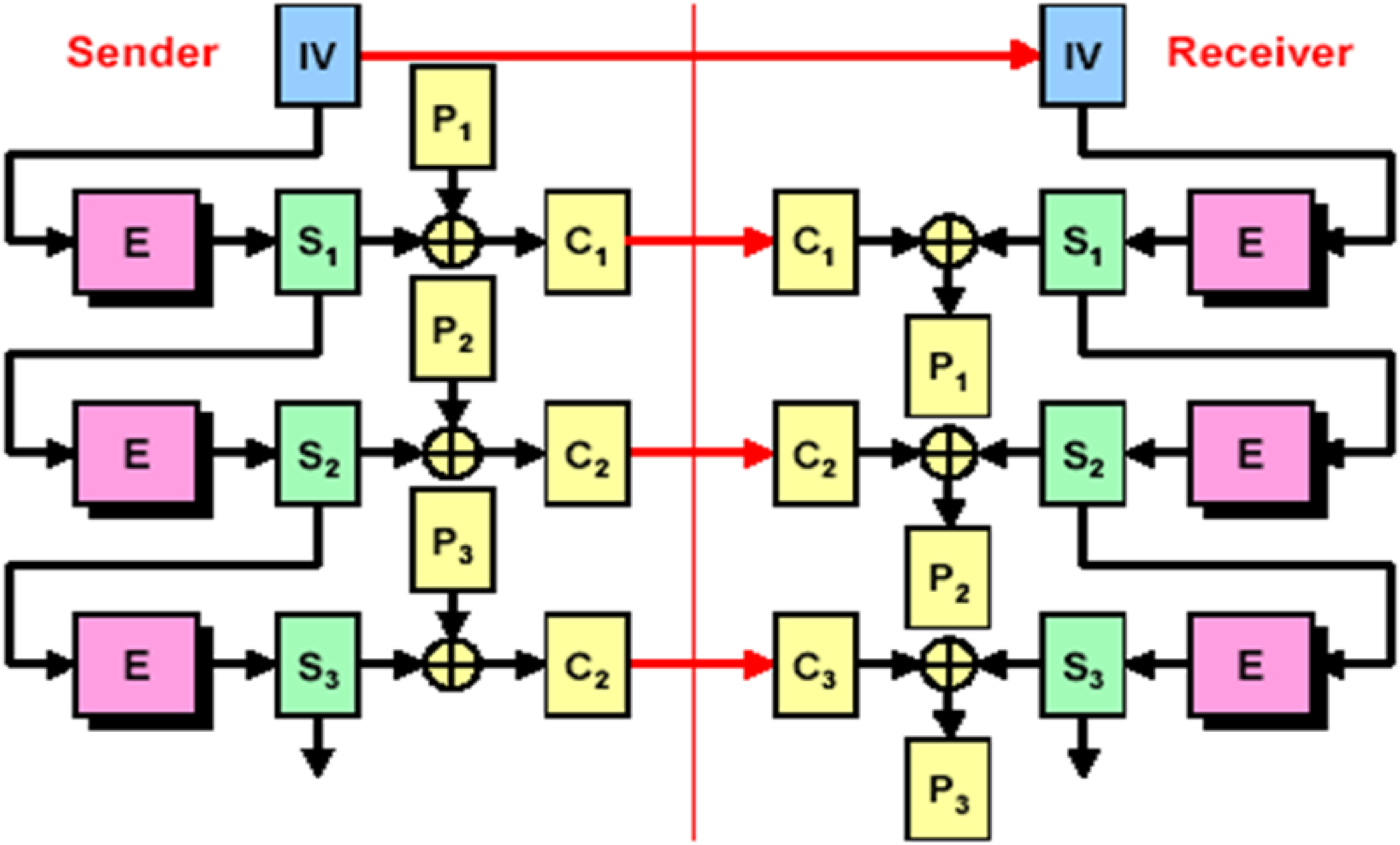


Plaintext Stream	1	1	1	1	1	1	1	1	0	0	0	0	0	0	...
Pseudo-Random Stream	1	0	0	1	1	0	1	0	1	1	0	1	0	0	...
Ciphertext Stream	0	1	1	0	0	1	0	1	1	1	0	1	0	0	...

- XOR each bit of your plaintext continuous stream with a bit from a pseudo-random sequence
- At receiver, use same symmetric key, XOR again to extract plaintext

Encryption Mode (OFB)

- *Output Feedback* (OFB) mode makes a block cipher into a synchronous stream cipher



THANK YOU