Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

Spring 2025

Cryptography

Why Cryptography?

- Cryptography for Confidentiality

Basics

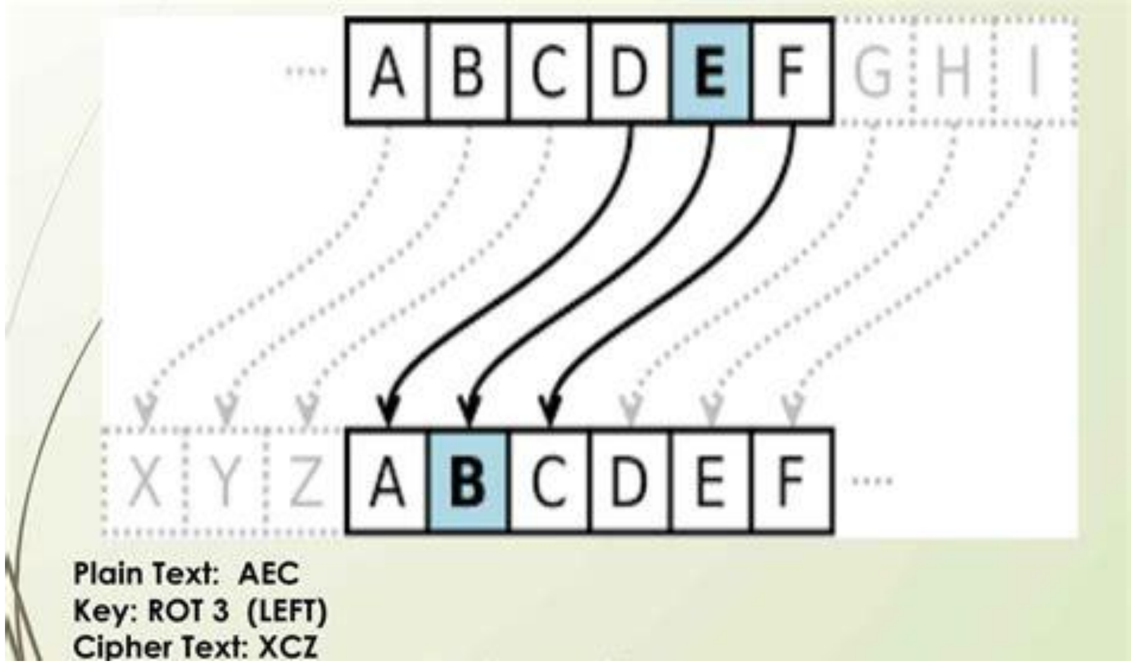
- Plaintext: Original message
  - Plaintext= I love you
- Ciphertext: Encrypted message
  - Ciphertext= 19 de 0b a3 ef 08 12 cf b5 7c
- Cipher: algorithm for transforming plaintext to ciphertext
  - Cipher= AES-128
- Key: info used in cipher known only to sender/receiver
  - Key= myEncryptionKey
  - Key= 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

Basics

- **Encrypt**: converting plaintext to ciphertext
- **Decrypt**: recovering plaintext from ciphertext

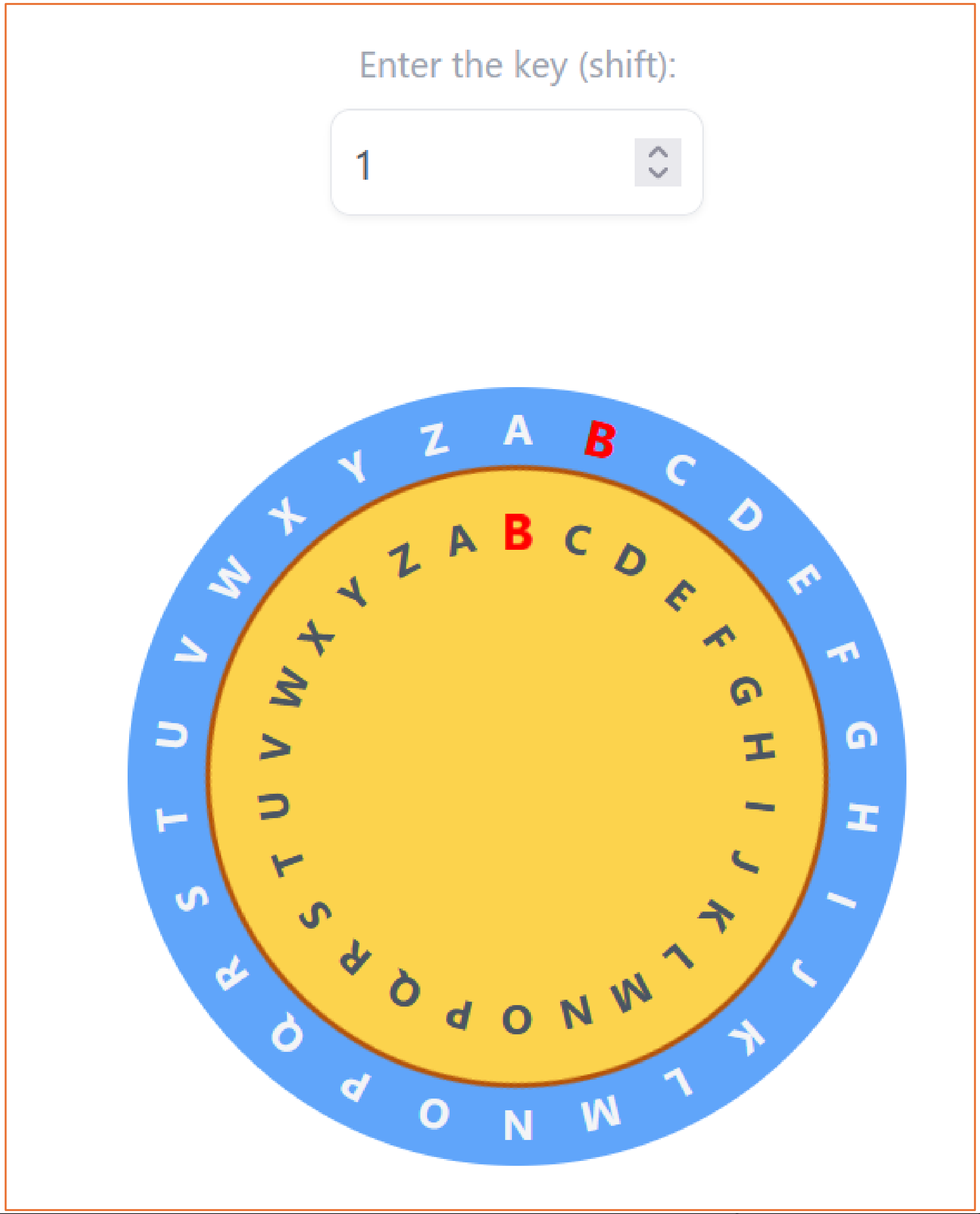
Caesar Cipher

- The Caesar Cipher, also known as the Caesar Shift Cipher
- Belongs to the category of substitution ciphers.
- Julius Caesar, who used this Caesar Cipher technique to encrypt his military commands.



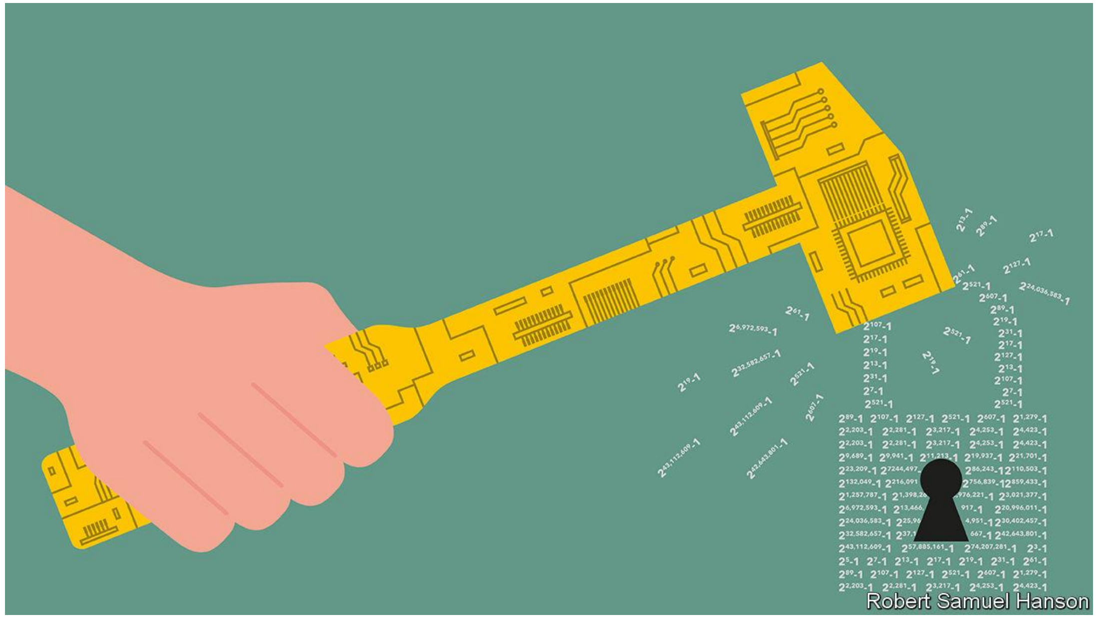
Caesar Cipher

- https://caesar-cipher.com/caesar-cipher-wheel



Breaking Caesar Cipher

- How we can decrypt Caesar Cipher?
  - Encrypted text: jgnnq
  - Encrypted text2: dwwdfn wlph wrpruurz 8
- Try different numbers:
  - Try 1: jgnnq -1-> ifmmp
  - Try 2: jgnnq -2-> hello
- We can use auto tools
  - https://caesarcipher.org/decoder



Brute Force

- A hacking method that uses trial and error to crack
- In Caesar Cipher we must test just 25 key.
  - If check of each key take 1 second
  - Check all key take 1*25=25 second
  - In average it takes 25/2=12.5 second to decrypt
  - It's a weak algorithm

Brute Force

Table 4.5 Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Security of encryption

- **Unconditionally Secure:** if the ciphertext does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.
  - no matter how much time an opponent has, it is impossible for him/her to decrypt the ciphertext
  - With the exception of a onetime pad, there is no encryption algorithm that is unconditionally secure.
- **Computationally Secure:** if two criteria are met
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information

My Encryption

- Clear text: play football in 16
- Key: Use Even cells

1	2	3
4	5	6
7	8	9

1	play	3
football	5	in
7	16	9

My Encryption

- Decryption
  - Key: Use Even cells
  - Clear text: play football in 16

read	play	Ping pong
football	buy	in
12	16	19

Substitution Cipher – 1 Character

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Examples
    - Playfair Cipher
    - Hill Cipher

Cryptoanalyses

- Brute force
- Frequency Analyze

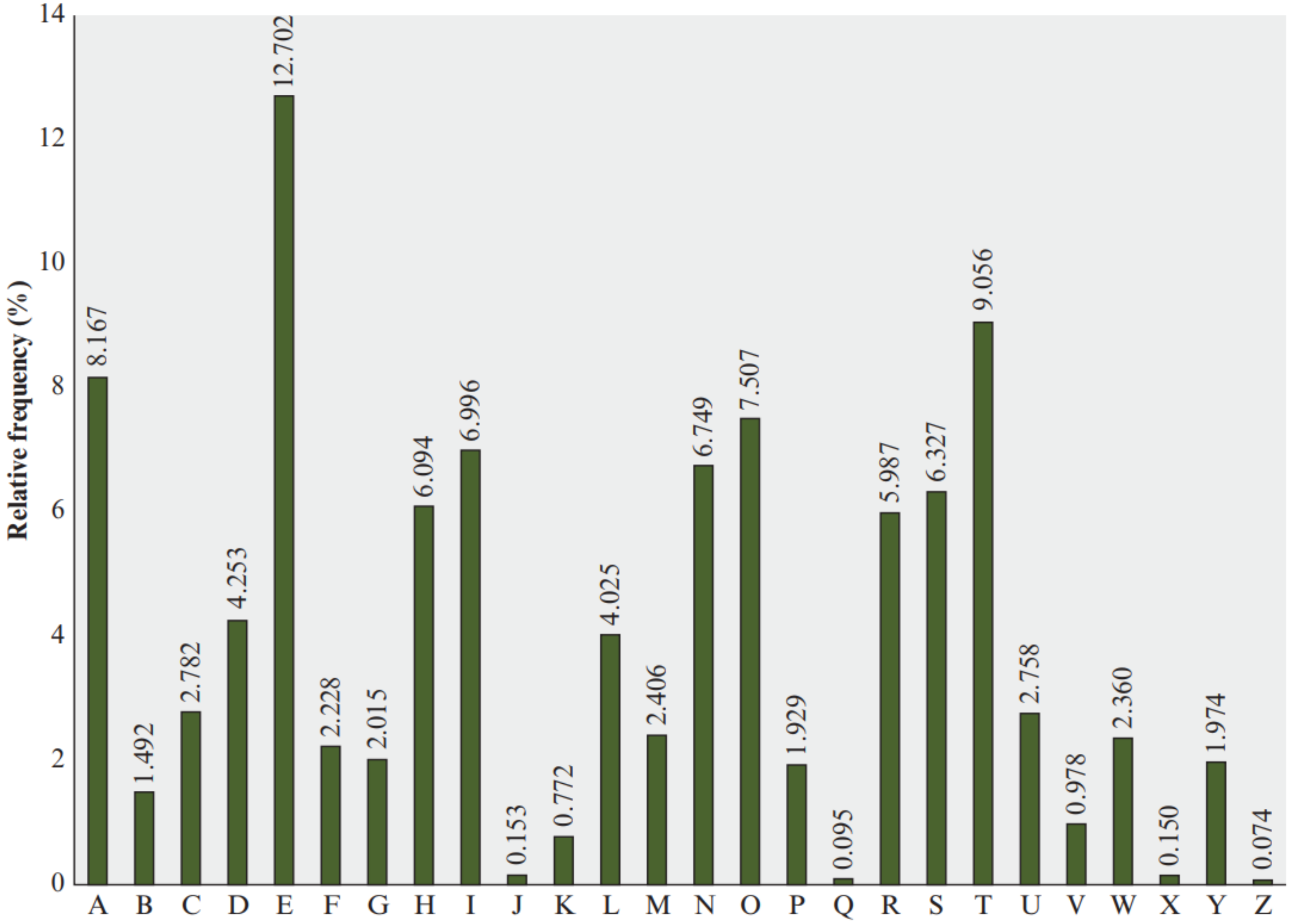


Figure 3.5 Relative Frequency of Letters in English Text

Classic Encryptions

- Two main approach
  - Substitution like Cesar
  - Transposition
- Transposition
  - performing some sort of permutation on the plaintext letters
  - Decryption is Harder

Transposition Example

- Example:
  - the key is 4312567
  - To encrypt, start with the column that is labeled 1, in this case column 3.
  - Write down all the letters in that column.
  - Proceed to column 4, which is labeled 2, ...

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Symmetric Encryption

- Encryption & Decryption keys are same

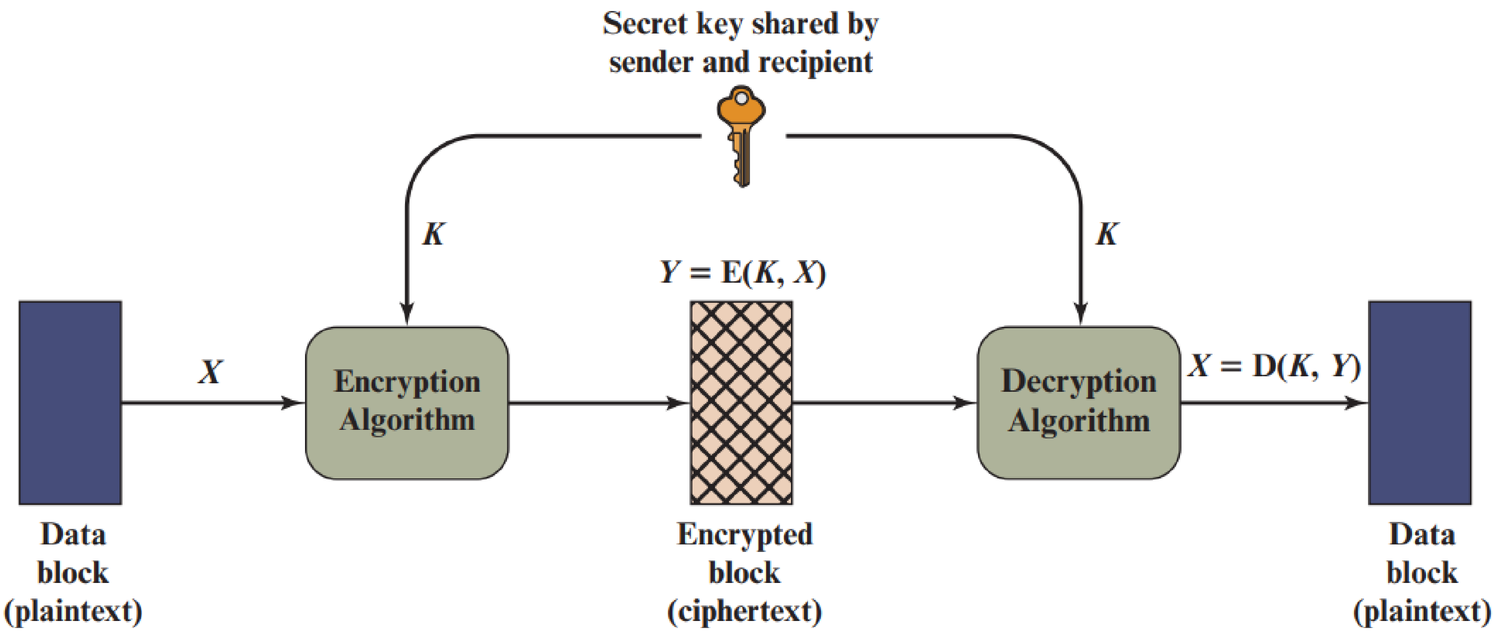


Figure 3.1 Simplified Model of Symmetric Encryption

Symmetric Encryption

- Need secure channel for key exchange

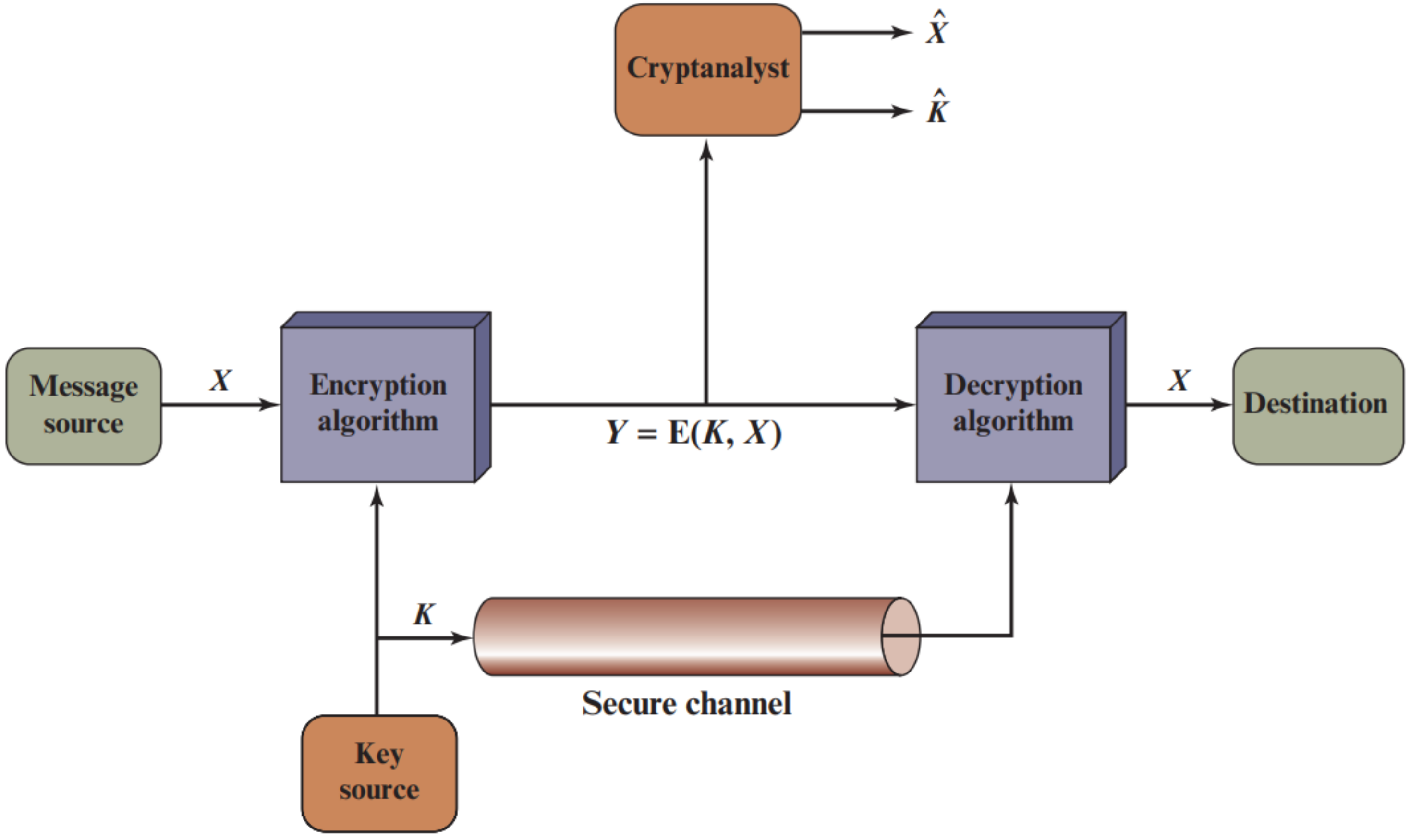


Figure 3.2 Model of Symmetric Cryptosystem

Usage in internet

- I want encrypt my Gmail emails with symmetric algorithm
    1. Go to Google company ✈️ 🌎
    2. Give my key to them 📥
    3. They encrypt my emails with this key 🏢 ⚒️

Usage in internet

- Problems
  1. So many letters!
  2. Slow encryption
  3. Hard to change my key

What is the solution?

- What if, we can encrypt message with Key1 & Decrypt with Key2 ?!
- Key1 and Key2 are different.
- Let’s think about it. 🤔