Mobile and Wireless Security
CSCE 496/896

Lecture # 2
Basics of cryptography and security

Instructor: Nirnimesh Ghose
Computer Science and Engineering

UNIVERSITY of NEBRASKA–LINCOLN

Lecture Set Overview

Information and network security

Security goals

Security attacks

Security mechanisms

Introduction to cryptography

Symmetric key cryptography

What is Security?

Information and Network Security

Information security:

What is information?

The object transmitted/distributed through the network.

Protecting the information from is the notion of information security.

Eg.: Encrypting the information before transmitting prevents unauthorized users from eavesdropping.

Network security:

What is network?

The infrastructure for transmitting/distributing the information.

Protecting the network to ensure information delivery is network security

Eg.: Preventing an adversary from launching denial-of-service attack on the network.

Notions of Security

The security in the electronic world is based on the ideas of security in the physical world.

E.g.:

Physical world: Add a lock to a door to control entry access.

Electronic world: Add an encryption to control information access.

Physical world: Add a watermark to a bank note to prevent counterfeiting.

Electronic world: Add message authentication code to prevent information tampering.

And many more……

Security Goals

Confidentiality

Authentication

Integrity

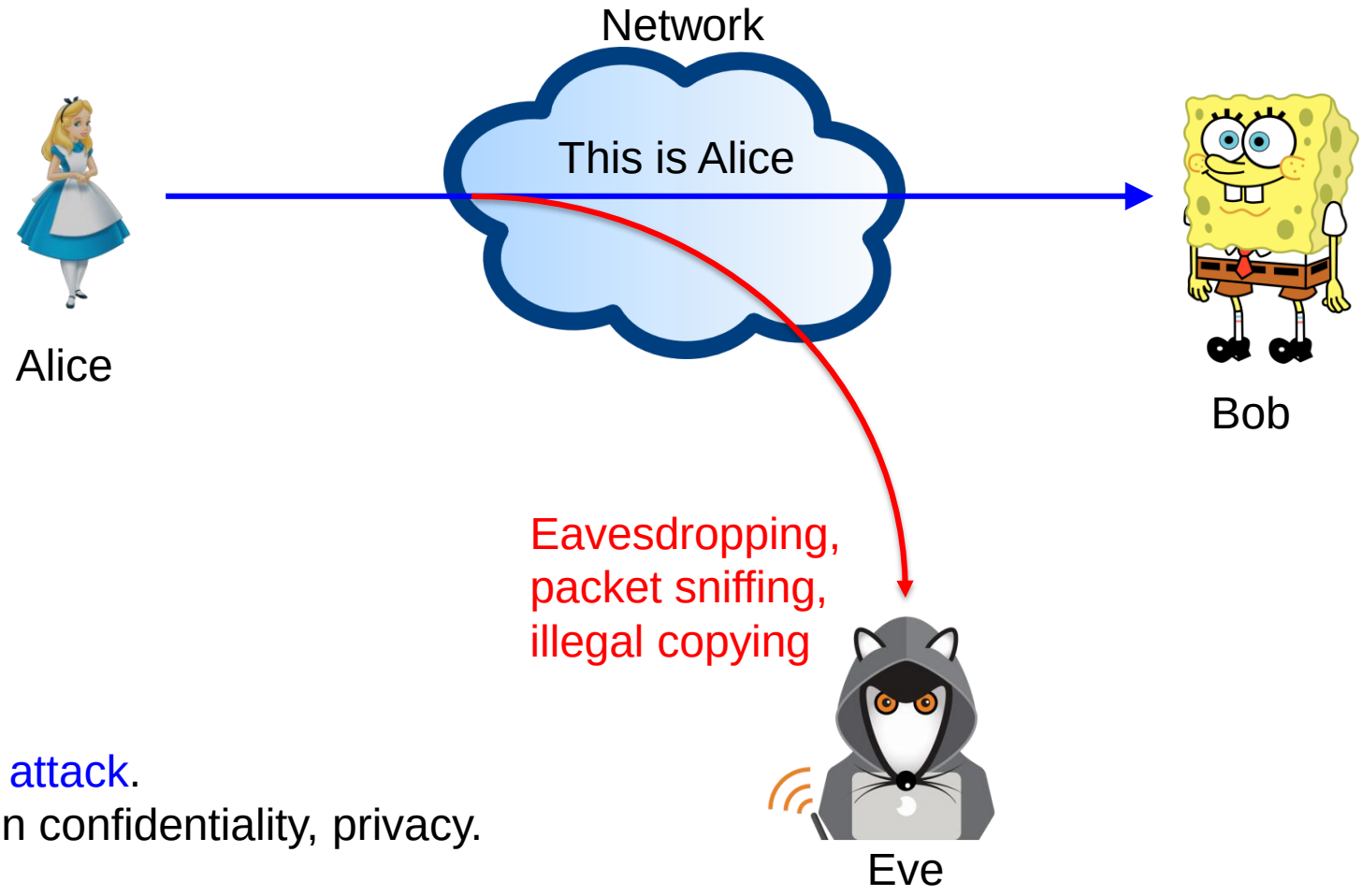
Availability

Non-repudiation

Anonymity

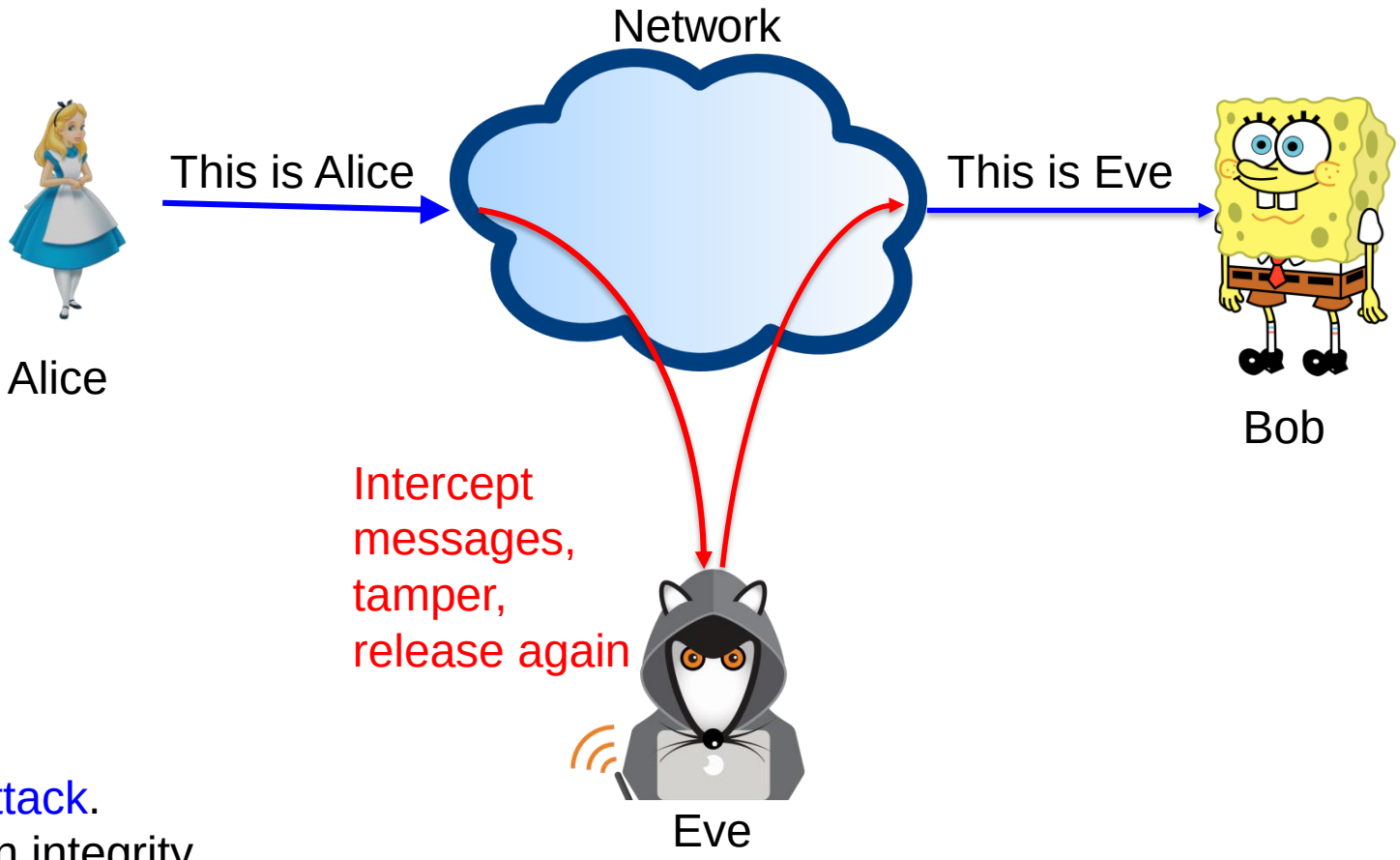
…

Is this Communication Confidential?



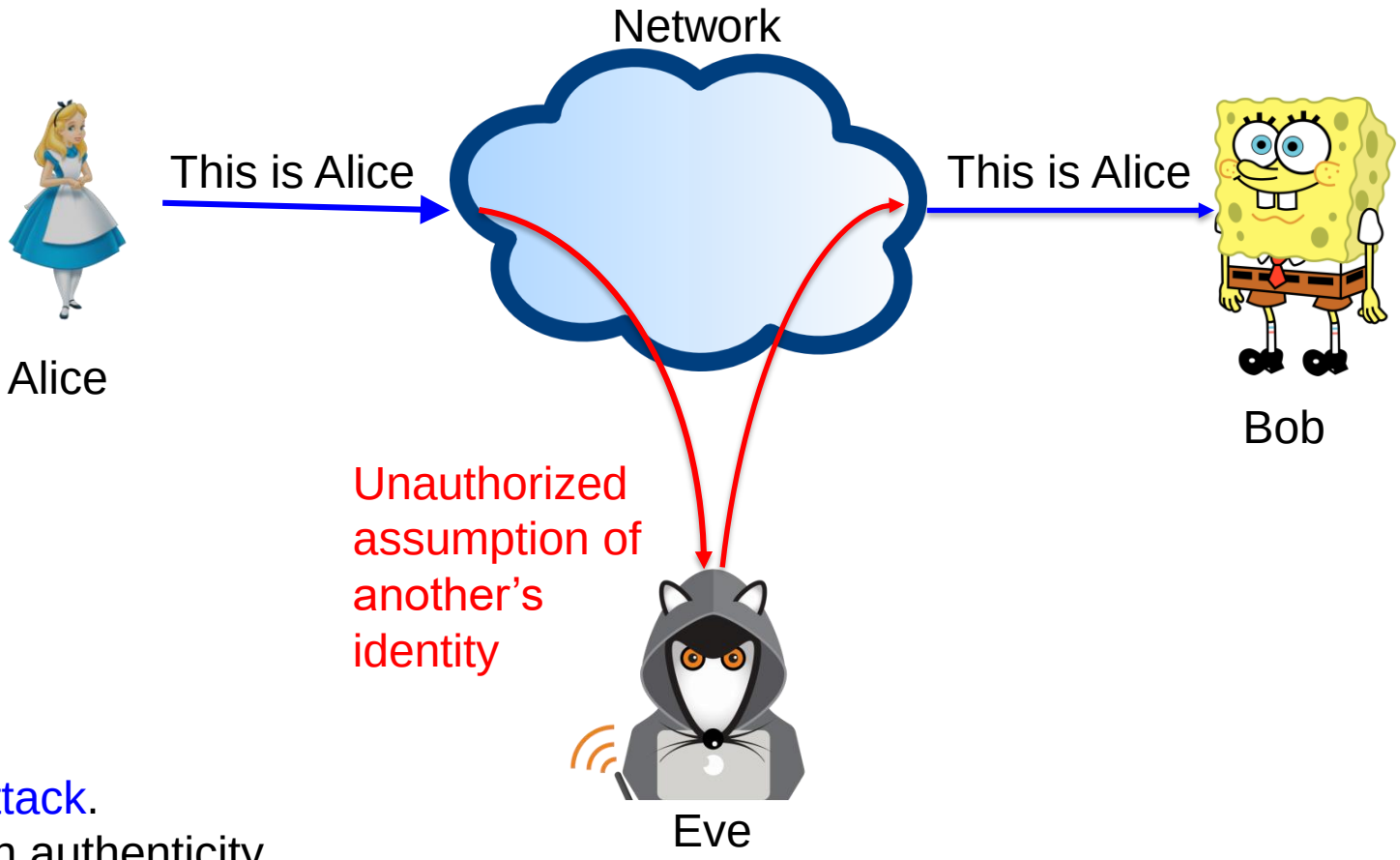
Passive attack.
Attack on confidentiality, privacy.

Will Bob Receives the Message Sent by Alice?



Active attack.
Attack on integrity.

Is Alice Authenticated to Bob?



Active attack.
Attack on authenticity.

Is Alice's Connection Available to Bob?

Alice

This is Alice

Network

Bob

Overwhelm or crash servers, disrupt infrastructure

Eve

Active attack.
Attack on availability.

What are the Different Security Attacks?

Passive attacks:

Eavesdropping, packet sniffing, traffic analysis….

Active attacks:

Delay, replay, deletion, modification, insertion….

How Can We Achieve Security?

Policy:

A security policy is a statement of what is, and what is not, allowed (regarding the security requirements).

Mechanism:

A security mechanism is a method, tool, or procedure for enforcing a security policy.

Tools to achieve security goals:

Prevention: password, encryption, digital signature, access control, authentication, data integrity, firewall, etc..

Detection: monitoring, log, auditing, intrusion detection

Recovery: backups, bug fixes, retaliation

What is Cryptography?

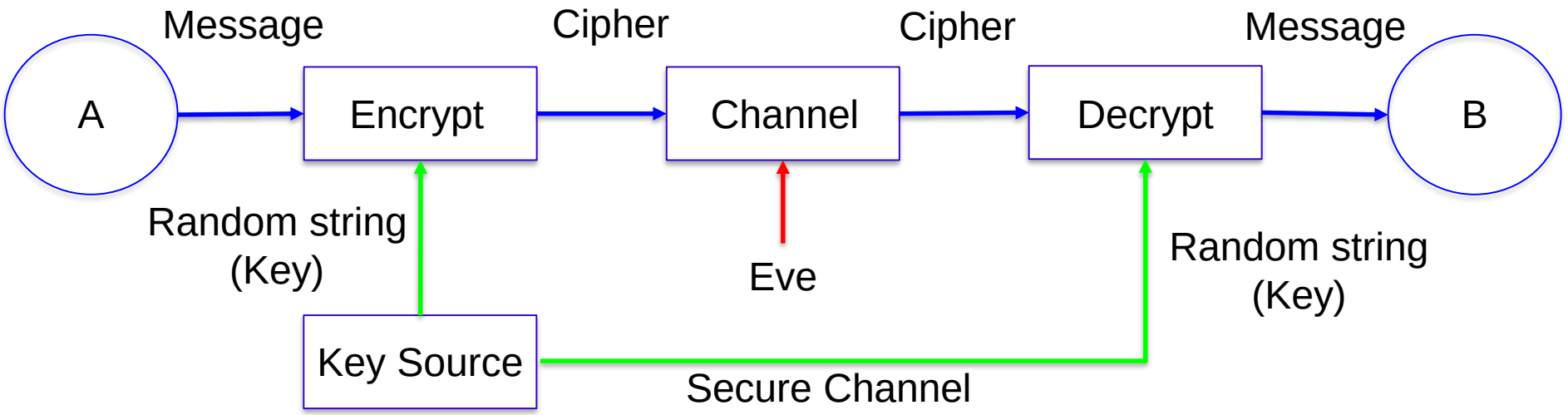
= Crypto(Hidden) + Logos (word)

= Cryptography + Cryptanalysis

= Code Writing + Code Breaking

Classical Cryptography

Send information securely over an insecure (public) channel



A cryptosystem is a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

1. $\mathcal{P}$ is the set of possible plaintexts
2. $\mathcal{C}$ is the set of possible ciphers
3. $\mathcal{K}$ is the set of possible keys
4. $\mathcal{E}$ is the encryption rule set
5. $\mathcal{D}$ is the decryption rule set

Shannon's Theory (1949)

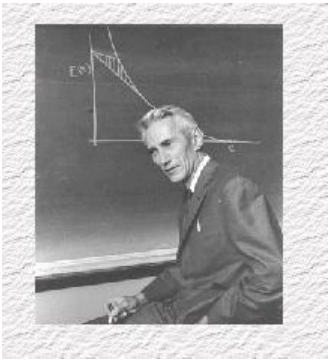
Confusion:

The ciphertext statistics should depend on the plaintext statistics in a manner too complicated to be exploited by the enemy cryptanalyst.

Diffusion:

Each digit of the plaintext should influence many digits of the ciphertext, and/or

Each digit of the secret key should influence many digits of the ciphertext.



What are the Types of Cryptography

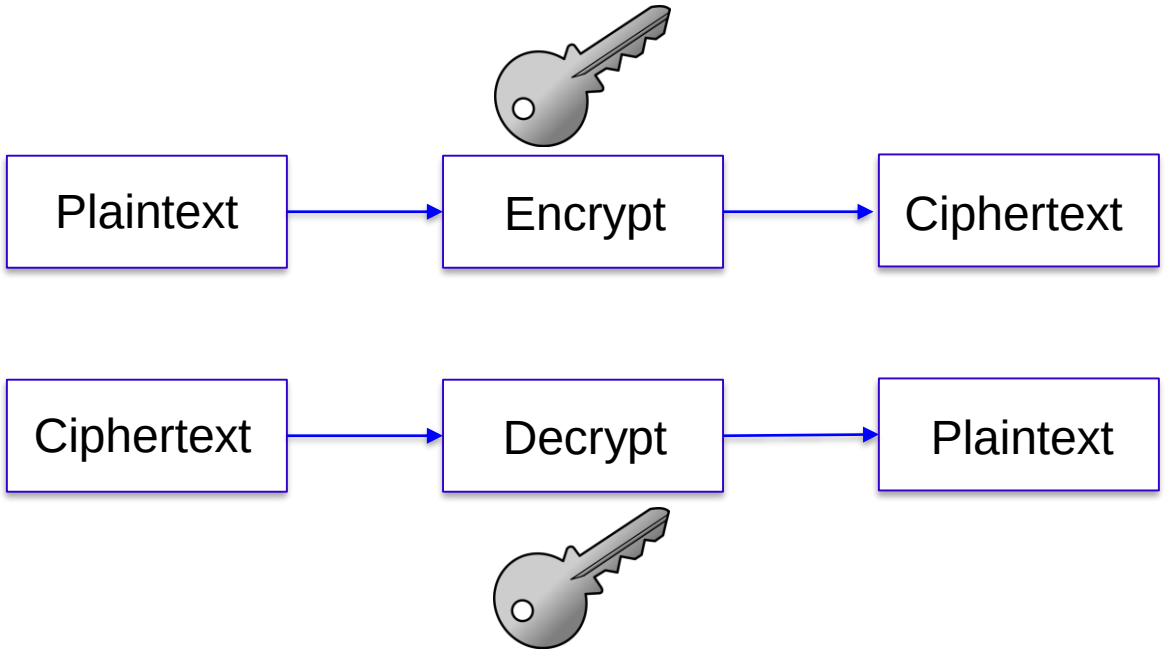
Symmetric key cryptography (one key)

Asymmetric key cryptography (two keys)

Symmetric Key Cryptography

The same key *K* is used for enciphering and deciphering of messages:

Eg: Shift cipher, Substitution Cipher, DES, 3DES, AES, ...



Basic Modular Arithmetic

$$A \bmod B = R \iff \frac{A}{B} = Q; Remainder\ R$$

Modular Addition and Multiplication

Modulus and congruence: $A \equiv B \pmod m \iff \frac{A-B}{m}$ has remainder of 0

Additive inverse of *x* is the number we need to add to *x* to get 0 for a modulo.

Let $\mathbb{Z}_m$ denote the set of integers {0, 1, 2...*m* − 1}.
This forms a *Group*, also a *Ring*.

Prime number: an integer with no other factors than 1 and itself

Substitution Cipher

Confusion is created by letters of plaintext are replaced by other letters or by numbers or symbols.

Shift Cipher

Plaintext: this is a security class

Ciphertext: WKLV LV D VHFXULWB FODVV

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$

Encryption function: $y = e_K(x) = (x + K) mod\ 26$

Decryption function: $x = d_K(y) = (y + K) mod\ 26$

For *K* = 3, is known as Ceaser cipher.

How secure is shift cipher?

Brute-force attack: Requires only 25 tries to break.

Other Substitution Ciphers

Affine ciphers: Encryption function: $y = e_K(x) = (ax + b) mod\ 26$

Decryption function: $x = d_K(y) = a^{-1}(y - b) mod\ 26$

Multiplicative inverse: if $x \times y = 1\ mod\ n$, then x and y are each other's multiplicative inverse mode n

Eg: $3 \times 7 = 1\ mod\ 10$

Vigenère Cipher: Best known polyalphabetic cipher. Key is *m*-length vector. Use different monoalphabetic substitutions as one proceeds through the plaintext message.

Plaintext: this is security class

Key: cryptii

Ciphertext: vygh ba i uvajkqba tjpla

Block Cipher

Let B_n denote the set of bit strings of length n.

A block cipher is an encryption algorithm $\mathcal{E}$ such that $\mathcal{E}_K$ is a permutation of B_n for each key K.

Characteristics:

Based on Shannon's theory of 1949

Same $\mathcal{P}$ gives same $\mathcal{C}$

$\{|\mathcal{P}|,|\mathcal{C}|\} \geq 64$bits, $|\mathcal{P}| \neq |\mathcal{K}| \geq 56$ bits.

Data Encryption Standards (DES)

Designed by IBM, publish by NIST (NBS) in 1977

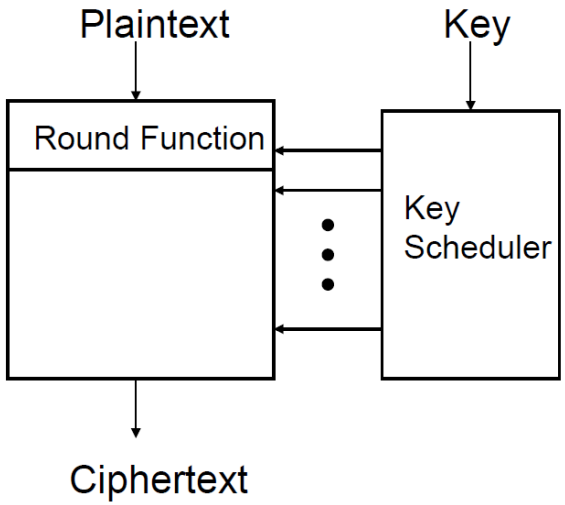
56-bit key, mapping a 64-bit input block to a 64-bit output block

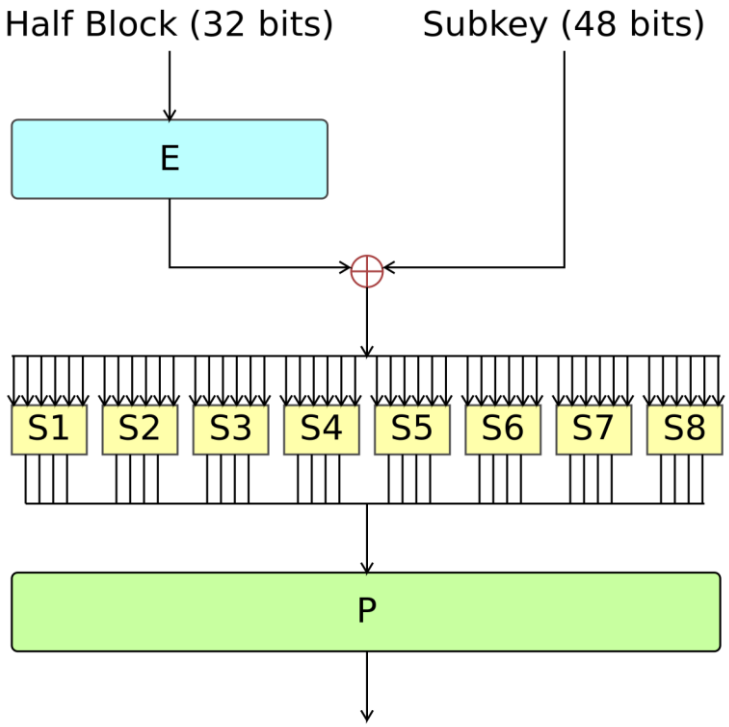
Not secure any more

- First broken in 1994 by Mitsuru Matsui
- Now 56 bits key can be recovered under 2 days
- Keys must grow by about 1 bit every 2 years

Triple DES, 112-bit key

Basic Structure of DES





Other Symmetric key Encryption

IDEA: International Data Encryption Algorithm

- Key length: 128 bits
- Data block length: 64 bits

AES: Advanced Encryption Standards

- Key length: 128 bits, 192 bits, 256 bits
- Data block length: 64 bits
- Introduced in 2001, to replace DES

How a Ciphertext be Attacked?

Cryptanalysis:

Cryptanalysis is the process of attempting to discover the plaintext and / or the key.

Types of cryptanalysis:

Ciphertext only attack: specific patterns of the plaintext may remain in the ciphertext (frequencies of letters, digraphs, etc.)

Known ciphertext / plaintext pairs

Chosen plaintext or chosen ciphertext

Newer developments: differential cryptanalysis, linear cryptanalysis

Classification of Security

Unconditionally secure : Unlimited power of adversary, perfect (*eg.* : one-time pad).

Provably secure : Under the assumption of well known hard mathematical problem.

Computationally secure : Amount of computational effort by the best-known methods (*Practical Secure*).

Provable Security

This refers to mathematical proofs, which are common in cryptography.

The aim of the proof is to show that the attacker (attacker model is defined) must solve the underlying hard problem in order to break the security of the modelled system.

Such a proof generally does not consider side-channel attacks or other implementation-specific attacks.

Computational Security

Against Brute-force attack and currently best-known cryptanalysis approach

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