Cryptography

Some constraints in military organizations :

- Ability of the code clerk to perform necessary transformations, often on a battlefield with little equipment
- Difficulty in switching over quickly from one cryptographic method to another one. Requires retraining a large number of people.
- Danger : code clerk may be captured by the enemy. Necessity to change the cryptographic method, if required.

DBC

Cryptography

Some useful terms and definitions

Plaintext : Messages to be encrypted

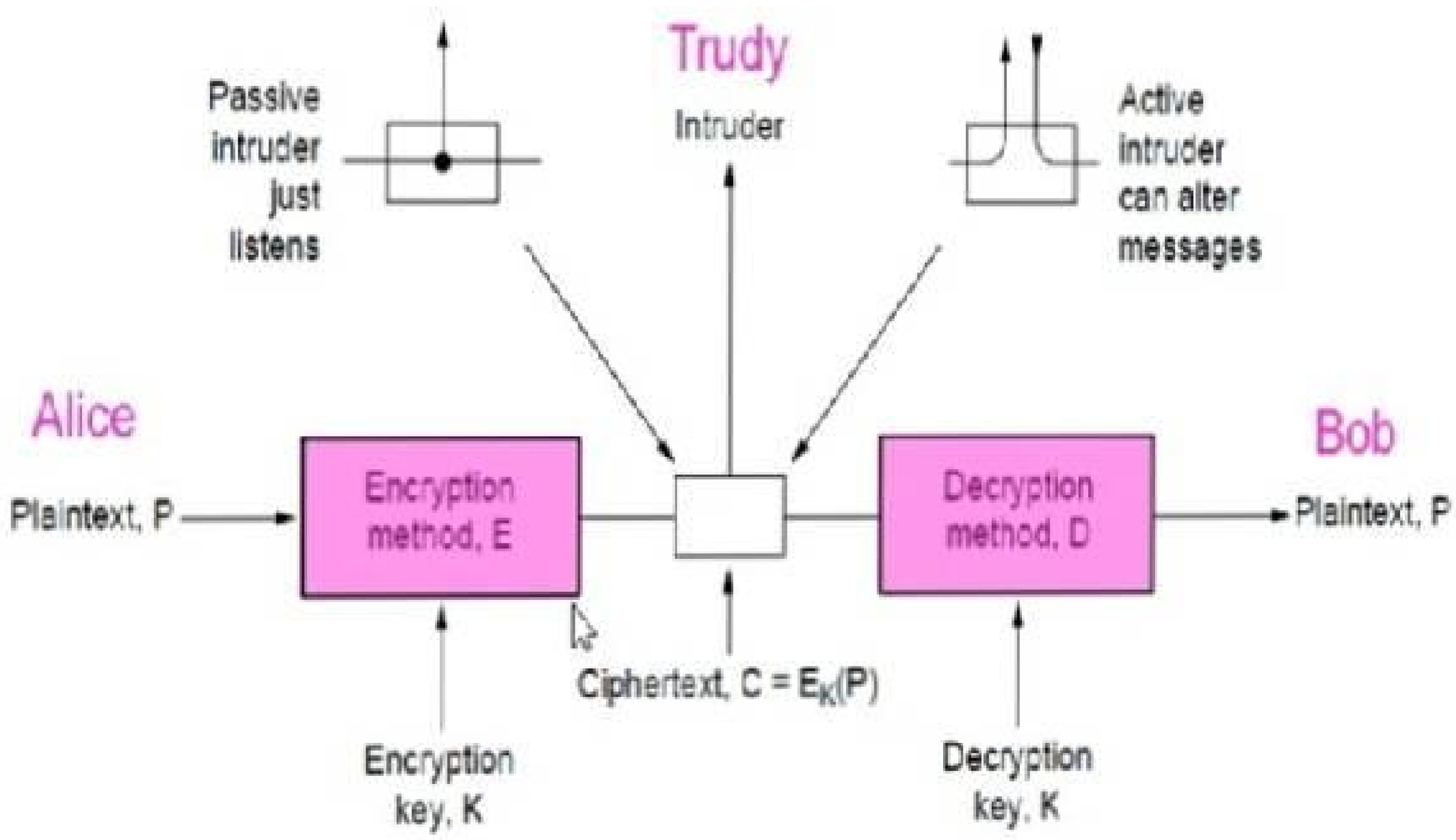
Ciphertext : The output of the encryption process.

Cryptanalysis : The art of breaking ciphers.

Cryptography : The art of devising ciphers.

Cryptology : The art of devising ciphers (cryptography) and the art of breaking ciphers (cryptanalysis) is collectively known as cryptology.

DBC



Stop sharing

DBC

Cryptography

Some useful notations

The encryption of the plaintext P using key K gives the ciphertext C.

$$\mathbf{C = E_k(P)}$$

The decryption of the ciphertext C using the key K gives the plaintext P.

$$\mathbf{P = D_k(C)}$$

Cryptography Basics

- Plaintext is transformed by a function that is parametrized by a key.

$$\mathbf{D_k(E_k(P)) = P}$$

where E and D are mathematical functions.

- **Key** : a short string that selects one of many potential encryptions.

  It can be changed as often as required.

- Secrecy lies in the key.
- **Length of key** : a major design issue. The longer the key, the higher the **work factor** the cryptanalyst has to deal with. The work factor for breaking the system by exhaustive search of key space is exponential in key length.
- **Basic model** : a stable and **publicly-known general method** parameterized b [screen-sharing notice] Stop sharing [Hide] **d key**.

Cryptography Basics

- Plaintext is transformed by a function that is parametrized by a key.

$$\mathbf{D_k(E_k(P)) = P}$$

where E and D are mathematical functions.

- **Basic model** : a stable and **publicly-known general method** parameterized by **a secret and easily changed key**.

- The cryptanalyst knows the algorithms and the secrecy lies exclusively in the keys.

Kerckhoff's principle : All algorithms must be public; only the keys are secret.

DBC

Cryptography Basics

- Amount of effort necessary to invent, test and install a new method
- Difficulty in switching over quickly from one cryptographic method to another one.
- Ability of a code clerk to perform necessary transformations, without computer systems.
- Ciphertext only problem : availability of a quantity of ciphertext and no plaintext.
- Known plaintext problem : some matched ciphertext and plaintext.
- Chosen plaintext problem : Cryptanalyst has an ability to encrypt pieces of plaintext of his own choosing.
- Two major categories of encryption methods : substitution ciphers and transposition ciphers.

Cryptography

- Two major categories of encryption methods :

  substitution ciphers and transposition ciphers

- Substitution Ciphers
  - preserve the order of plaintext symbols
  - each letter or a group of letters is replaced by another letter or a group of letters to disguise it.
- Example : Caesar cipher

  Usage of a circularly shifted alphabet.
- Slight generalization of the Caesar cipher :

  Ciphertext alphabet may be shifted by k letters instead of always 3.

  K becomes a key.

DBC

Substitution Ciphers

- Monoalphabetic substitution :

  Have each letter or symbol in the plaintext map onto some other letter or symbol.
- Letter for letter substitution.
- Example :

  plaintext : a b c d … … … z

  ciphertext : Q W E R… … … M

  Key : 26-letter string corresponding to the full alphabet.
- 26 ! possible keys. Trying all of them ? Not a promising approach.
- General method may be known. No problem.

Substitution Ciphers

Substitution ciphers replace each group of letters in the message with another group of letters to disguise it

plaintext:	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
ciphertext:	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

Simple single-letter substitution cipher

DBC

Transposition Cipher

- Reorder the symbols, but do not disguise them.
- Every letter represents itself.
- Example : Columnar transposition cipher.
- Cipher is keyed by a word/phrase not containing any repeated letters.
- Number the columns. Culumn 1 being under the key letter closest to the start of the lphabet, and so on.
- Plaintext is written horizontally in rows.
- Ciphertext is read out by columns.

Transposition Cipher

Transposition ciphers reorder letters to disguise them

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

← Key gives column order

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Column 5 6 7 8

Simple column transposition cipher

DBC

Fundamental Cryptographic Principles

1. Messages must contain some redundancy.

All encrypted messages decrypt to something.

Redundancy lets receiver recognize a valid message.

However, redundancy helps attackers break the design.

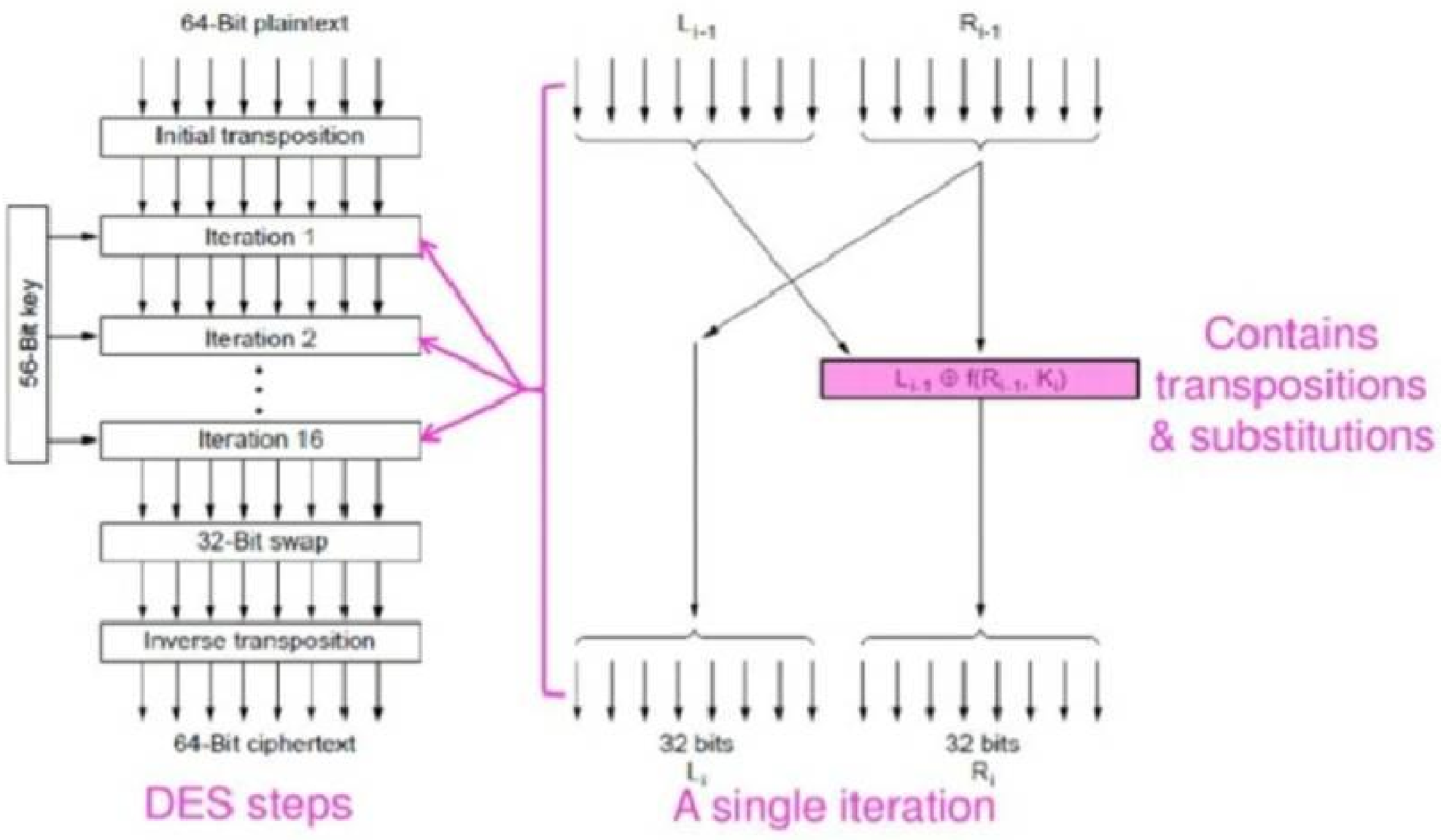
2. Some method is needed to foil replay attacks.

Without a way to check if messages are fresh then old messages can be copied and resent.

For example, add a date stamp to messages.

DES-The Data Encryption Standard

DES encryption was widely used (but no longer secure)



DBC

Public-Key Algorithms

Public-Key Algorithms

Encryption in which each party publishes a public part of their key and keep secret a private part of it

- RSA (by Rivest, Shamir, Adleman) »

Public-Key Algorithms

Downsides of keys for symmetric-key designs:

- Key must be secret, yet be distributed to both parties
- For N users there are N^2 pairwise keys to manage

Public key schemes split the key into public and private parts that are mathematically related:

- Private part is not distributed; easy to keep secret
- Only one public key per user needs to be managed

Security depends on the chosen mathematical property

- Much slower than symmetric-key, e.g., 1000X
- So use it to set up per-session symmetric keys

DBC

Public-Key Algorithms

- Diffie and Hellman (1976), Stanford University, proposed a new kind of cryptosystem :
- Encryption and decryption keys are different
- Decryption key cannot be feasibly derived from the encryption key.
- The (keyed) encryption algorithm, E, and the (keyed) decryption algorithm, D, have to meet the following three requirements :

1. D(E(P)) = P.
2. It is exceedingly difficult to deduce D from E.
3. E cannot be broken by a chosen plaintext attack.

RSA

RSA is a widely used public-key encryption method whose security is based on the difficulty of factoring large numbers

Key generation:

- Choose two large primes, p and q
- Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
- Choose d to be relatively prime to z
- Find e such that $e \times d = 1 \bmod z$
- Public key is (e, n), and private key is (d, n)

Encryption (of k bit message, for numbers up to n):

- $\text{Cipher} = \text{Plain}^e \pmod n$

Decryption:

- $\text{Plain} = \text{Cipher}^d \pmod n$

DBC

RSA

Small-scale example of RSA encryption

- For p=3, q=11 → n=33, z=20 → d=7, e=3

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
		Sender's computation		Receiver's computation		

Encryption: $C = P^3 \bmod 33$

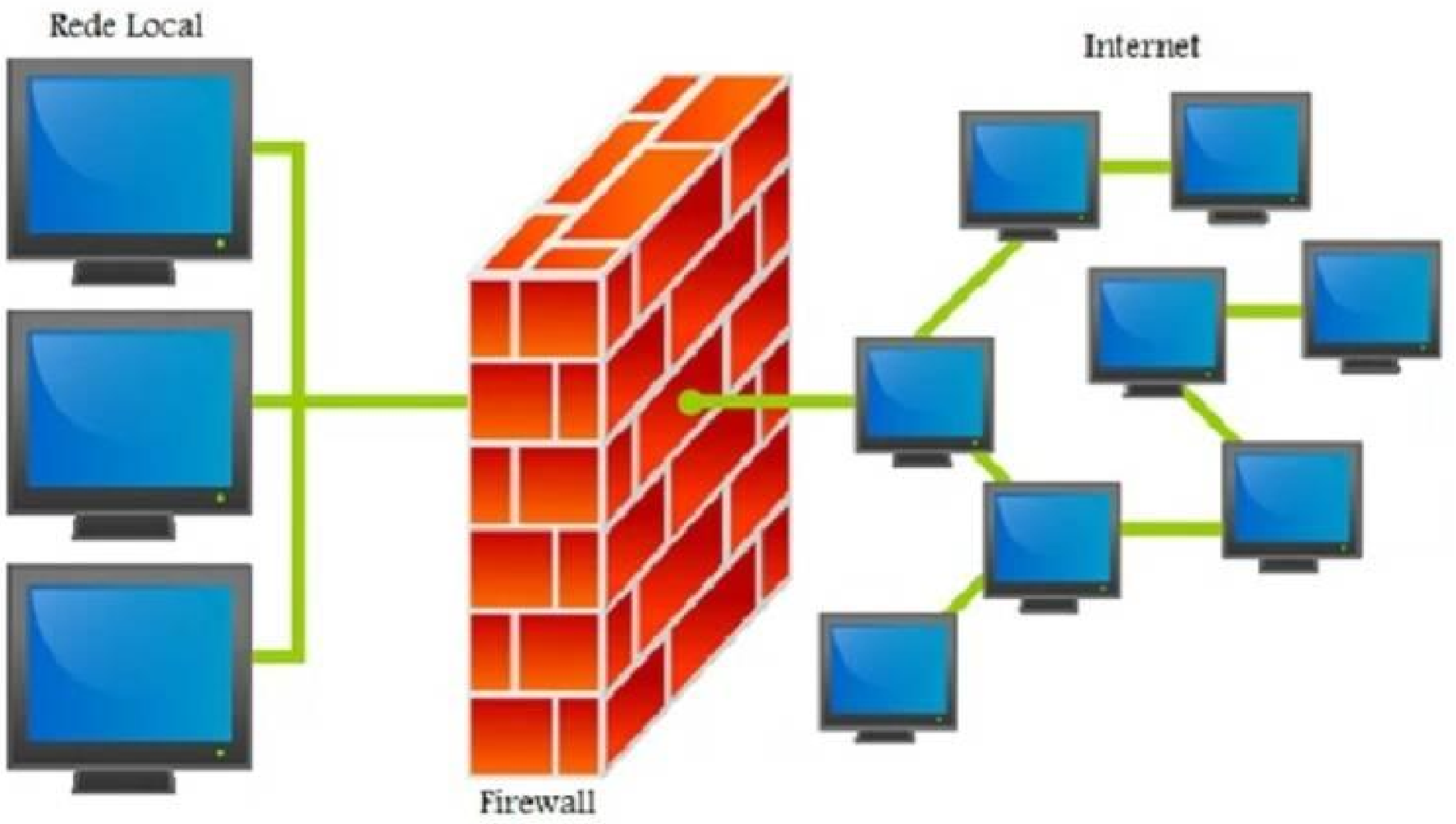
Decryption: $P = C^7 \bmod 33$

DBC

Firewalls

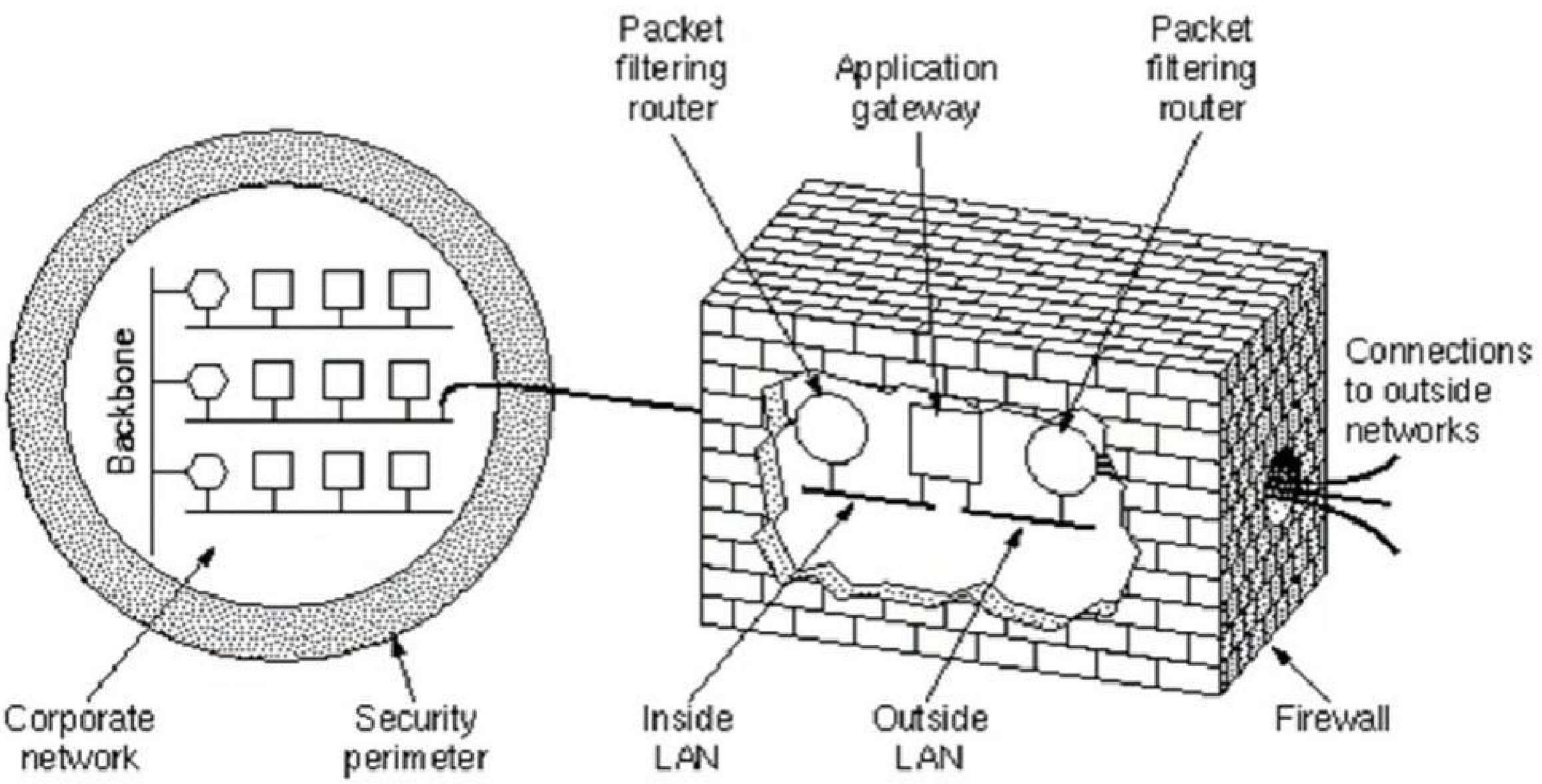
- Security mechanism used to protect your internal network from an external network.
- **Typical configuration :** two routers (used for packet filtering) and an application gateway (for further examination).
- Every packet must transit two filters and an application gateway to go in or out.
- Only one route exists.

Firewalls



DBC

Firewalls



DBC

Firewalls

Usage of packet filters :

- standard routers equipped with some extra functionalities.
- driven by tables configured by system administrators.
- contain information about sources/destinations that are acceptable/blocked, specification of default rules regarding what to do with packets coming from or going to other machines.

Firewalls

Firewalls

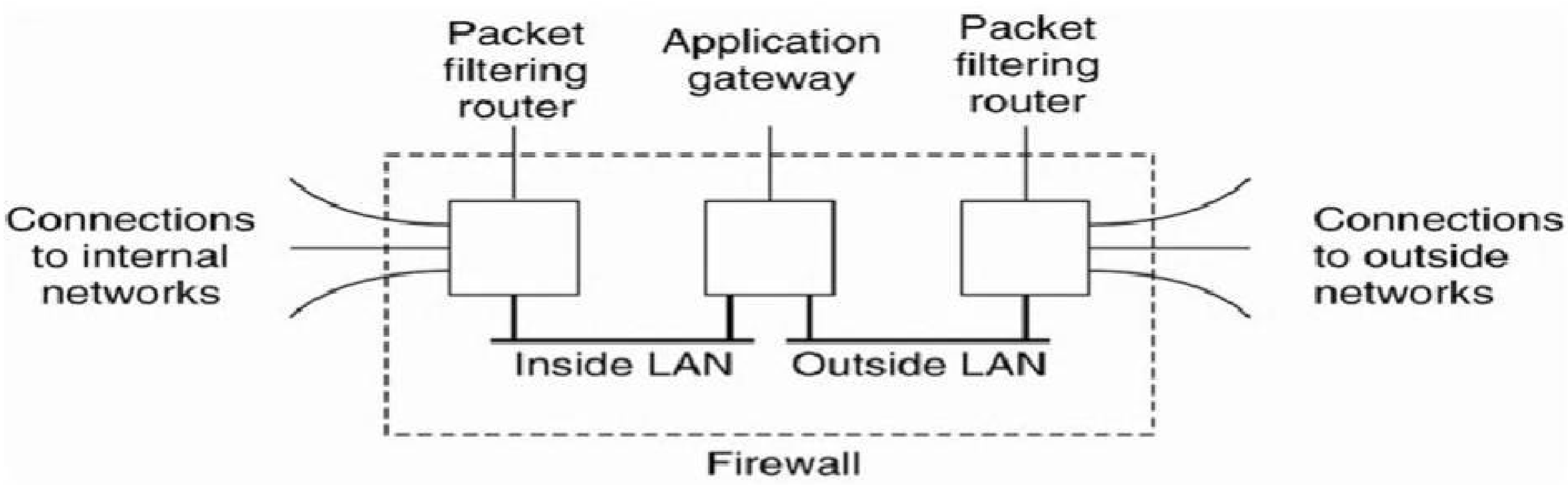


Figure 9-28. A common implementation of a firewall.

DBC

Firewalls

- Blocking incoming packets
- A common case of a TCP/IP setting

  Source/destinations address : IP address and a port number.

  TCP port Service

  23 : Telnet

  79 : Finger

  119 : USENET news

- An organization may block incoming packets for all IP addresses combined with selected ports.

Firewalls

- Blocking outgoing packets
- Standard port naming conventions
- FTP service : dynamic assignment of port #s.
- Blocking TCP/UDP connections.
- Usage of an application gateway : examining each message at an application level. Inspecting header fields, message size, message content, etc.

Firewalls

- Usage of an application gateway :
- examining each message at an application level.
- A mail gateway can be set up to examine each message going in or coming out.
- For each message, the gateway decides whether to transmit or discard the message based on

  header fields,

  message size,

  message content.

Firewalls

- Commonly used techniques :
  - packet filtering
  - IP masquerading
  - proxy services
  - encrypted tunneling
  - encrypted authentication