

# Defining Cryptography

# Objectives

- Define cryptography
- List the basic symmetric cryptographic algorithms
- Describe how asymmetric cryptography works
- List types of file and file system cryptography
- Explain how whole disk encryption works

# What Is Cryptography?

**Cryptography - scrambles data**

Cryptography derived its name from a Greek word called 'Kryptos' which mean Hidden Secrets.

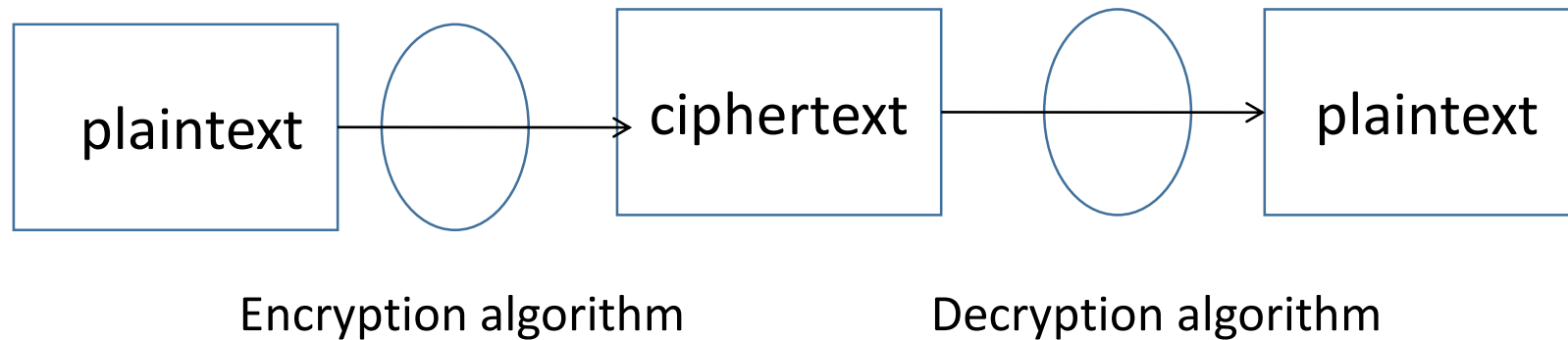
“The science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it”

## **Cryptography**

- Scrambling information so it cannot be read
- Transforms information into secure form so unauthorized persons cannot access it

# What is cryptography.....

- The science and study of hiding information
- ✓ Hiding information by converting plaintext into ciphertext (encryption).
- ✓ The back from ciphertext to plaintext(decryption).



# Steganography-hides data

Hides the existence of the data

What appears to be a harmless image can contain hidden data embedded within the image

Can use image files, audio files or even video files to contain hidden information

Achieved by dividing data and hiding in unused portions of the file

# Steganography

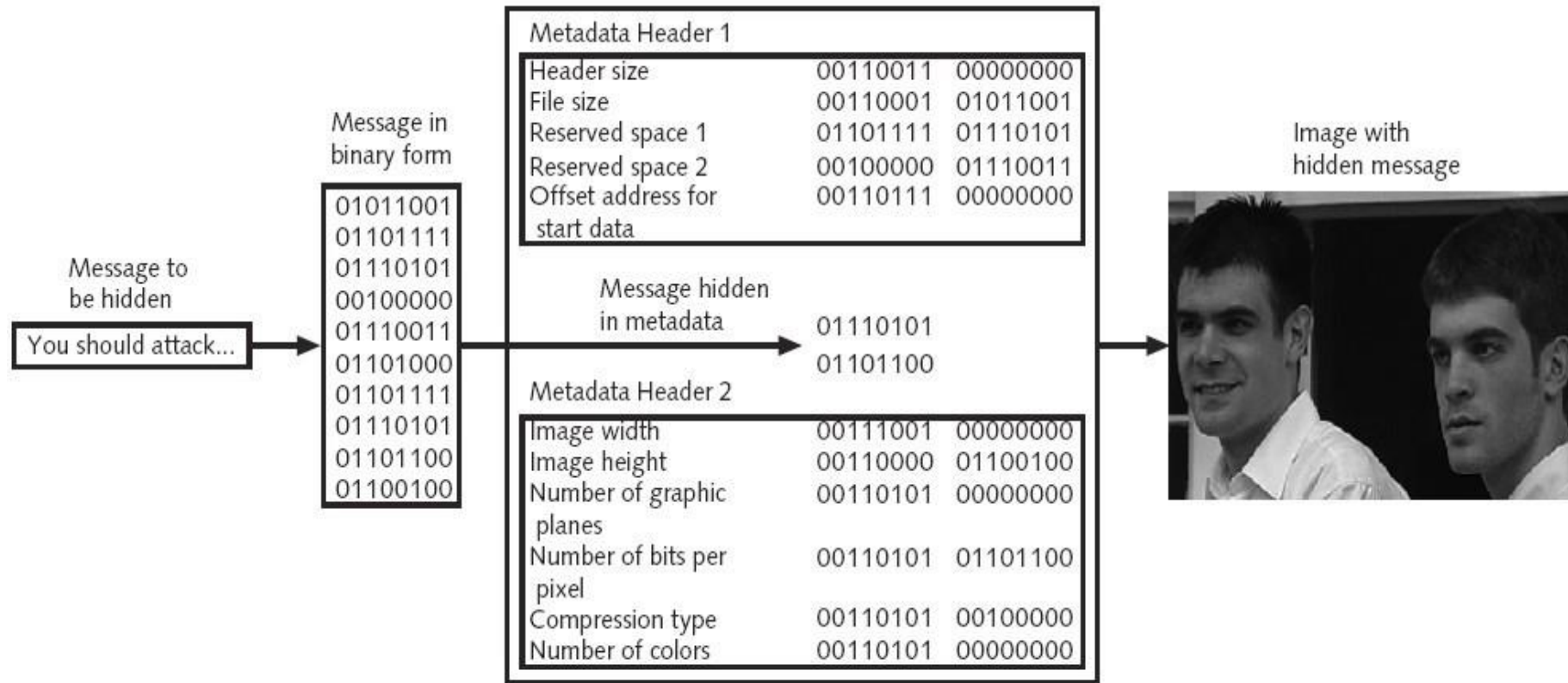


Figure 11-1 Data hidden by steganography

# Benefits of cryptography

- Confident of data.

Protecting data in transit.

protecting data at rest.

- Non-repudiation and authentication

A message encrypted with your private key or signed with your digital signature had to come from you.

- Access control

With symmetric encryption only the secret key holder can encrypt and decrypt the ciphertext.

With asymmetric encryption can be used for authentication and thus access control.



- Integrity

Message digests can be used to know if a message was tampered during transit.

## Characteristics of Modern Cryptography

There are three major characteristics that separate modern cryptography from the classical approach.

Classic Cryptography	Modern Cryptography
It manipulates traditional characters, i.e., letters and digits directly.	It operates on binary bit sequences.
The techniques employed for coding were kept secret and only the parties involved in communication knew about them.	It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secret key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.
It requires the entire cryptosystem for communicating confidentially.	Modern cryptography requires parties interested in secure communication to possess the secret key only.

# Encryption and Decryption

## **Encryption**

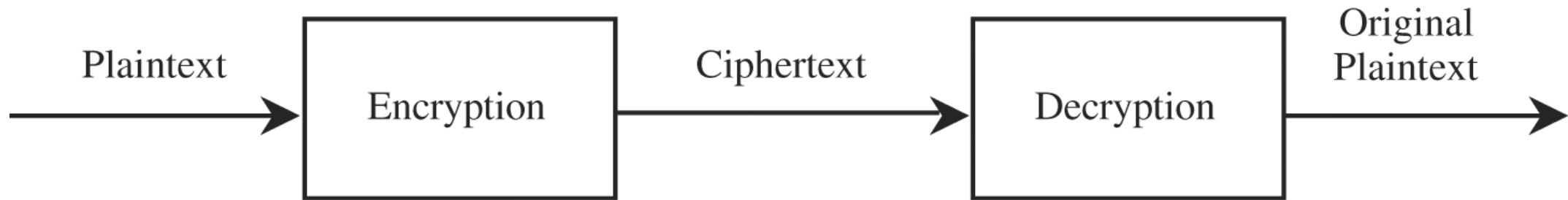
Changing the original text to a secret message using cryptography

## **Decryption**

Change the secret message back to its original form

# Encryption

- Process of scramble characters in text
- process of transform
- information using an algorithm to make it unreadable



# Encryption

- Symmetric key algorithm
  - both sender and receiver use the same key to encrypt and decrypt the message.
  - single-key
  - secret-key
  - conventional encryption
- Asymmetric key algorithm
  - sender and receiver use two deferent keys to encrypt and decrypt the message.
  - two-key
  - public-key encryption

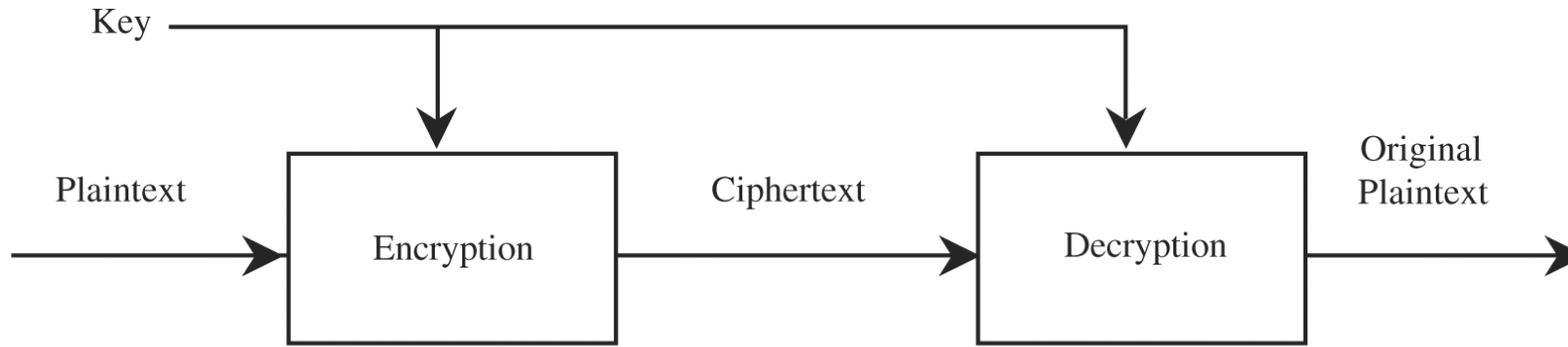
## Symmetric

- both sender and receiver use the same key to encrypt and decrypt the message.
- conventional encryption
- Single key/Secret Key encryption

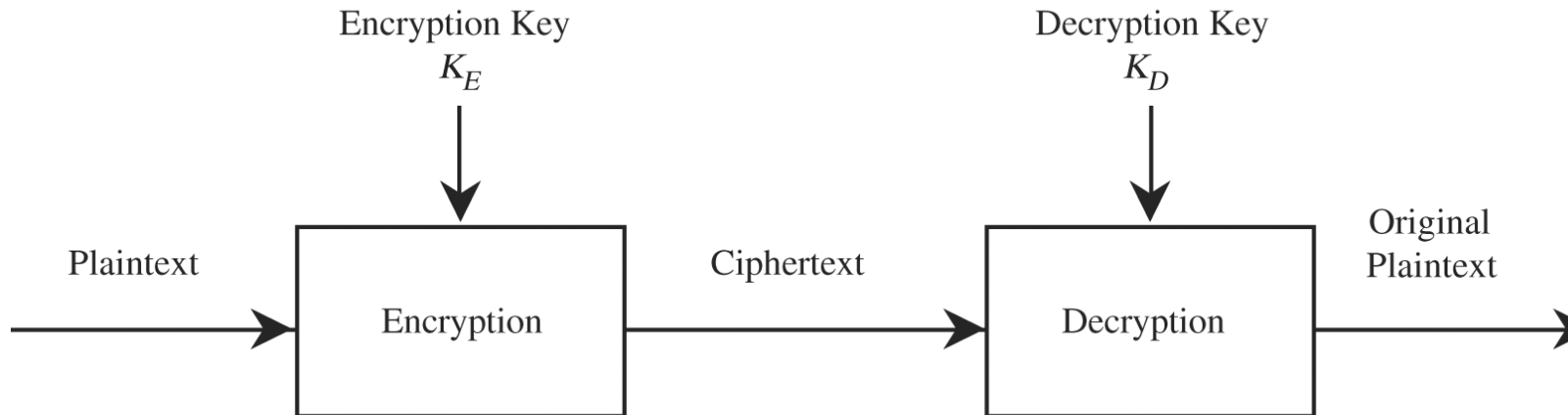
## Asymmetric

- sender and receiver use two different keys to encrypt and decrypt the message.
- two-key/ public key encryption

# Comparison



(a) Symmetric Cryptosystem

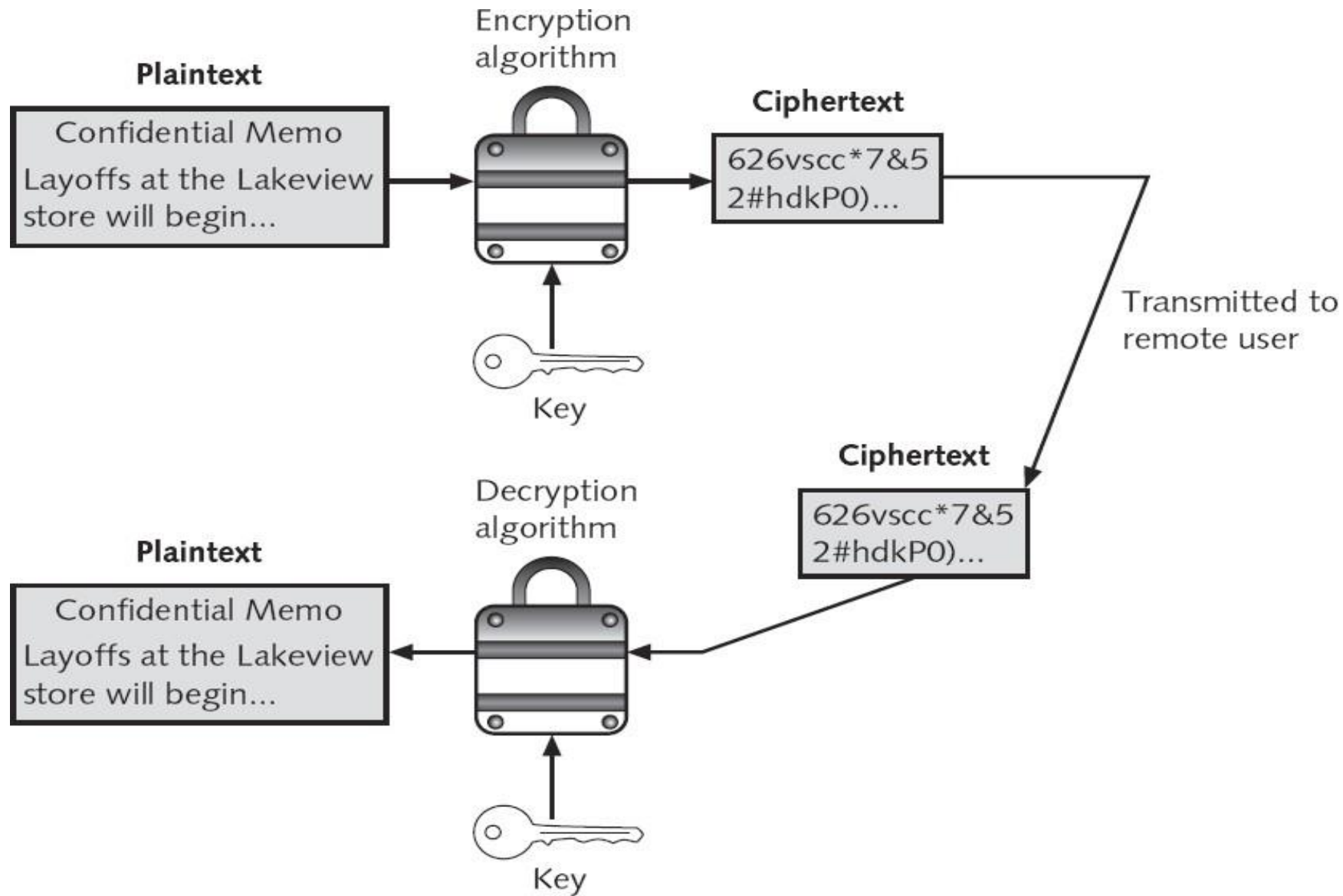


(b) Asymmetric Cryptosystem

# Basic Terminology

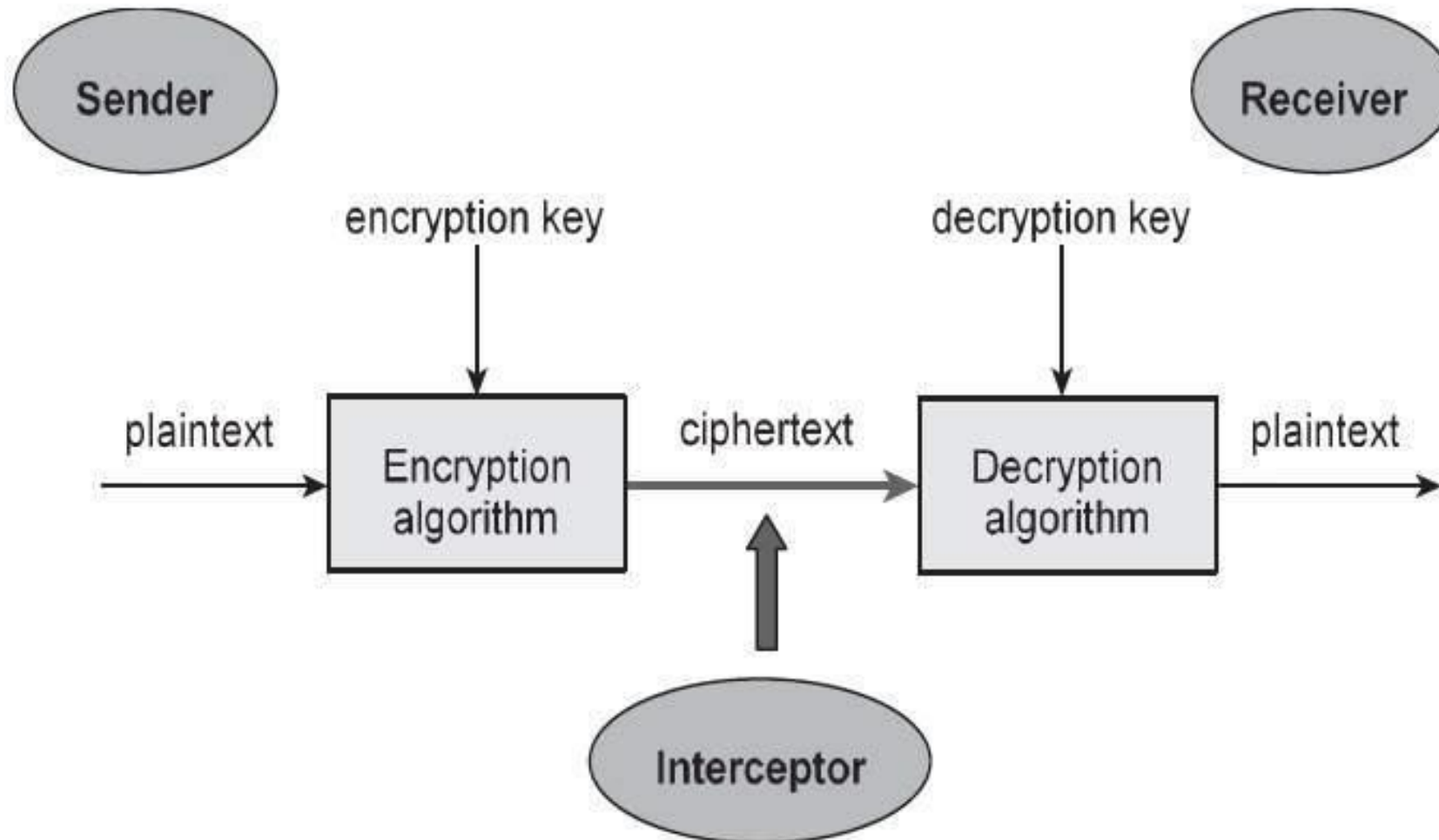
- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering from ciphertext to plaintext





**Figure 11-2** Cryptography process

simple model of a cryptosystem that provides confidentiality to the information being transmitted.



# Information Protection by Cryptography

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information
Authenticity	Provides proof of the genuineness of the user	Cryptography can prove that the sender was legitimate and not an imposter
Non-repudiation	Proves that a user performed an action	Cryptographic non-repudiation prevents an individual from fraudulently denying they were involved in a transaction

**Table 11-1** Information protections by cryptography

## Types of Cryptosystems

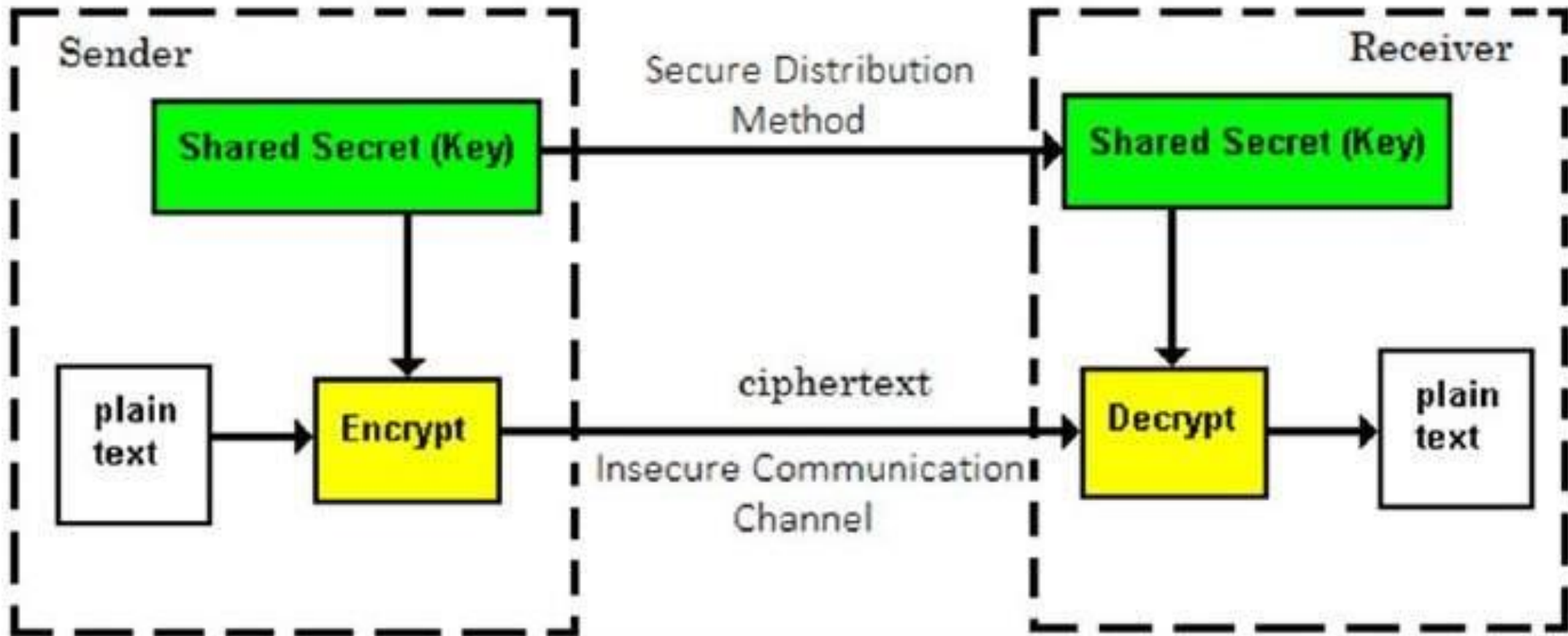
Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key.

# Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.



- **Symmetric Key Cryptography (Secret Key Cryptography)**
  - Same Key is used by both parties

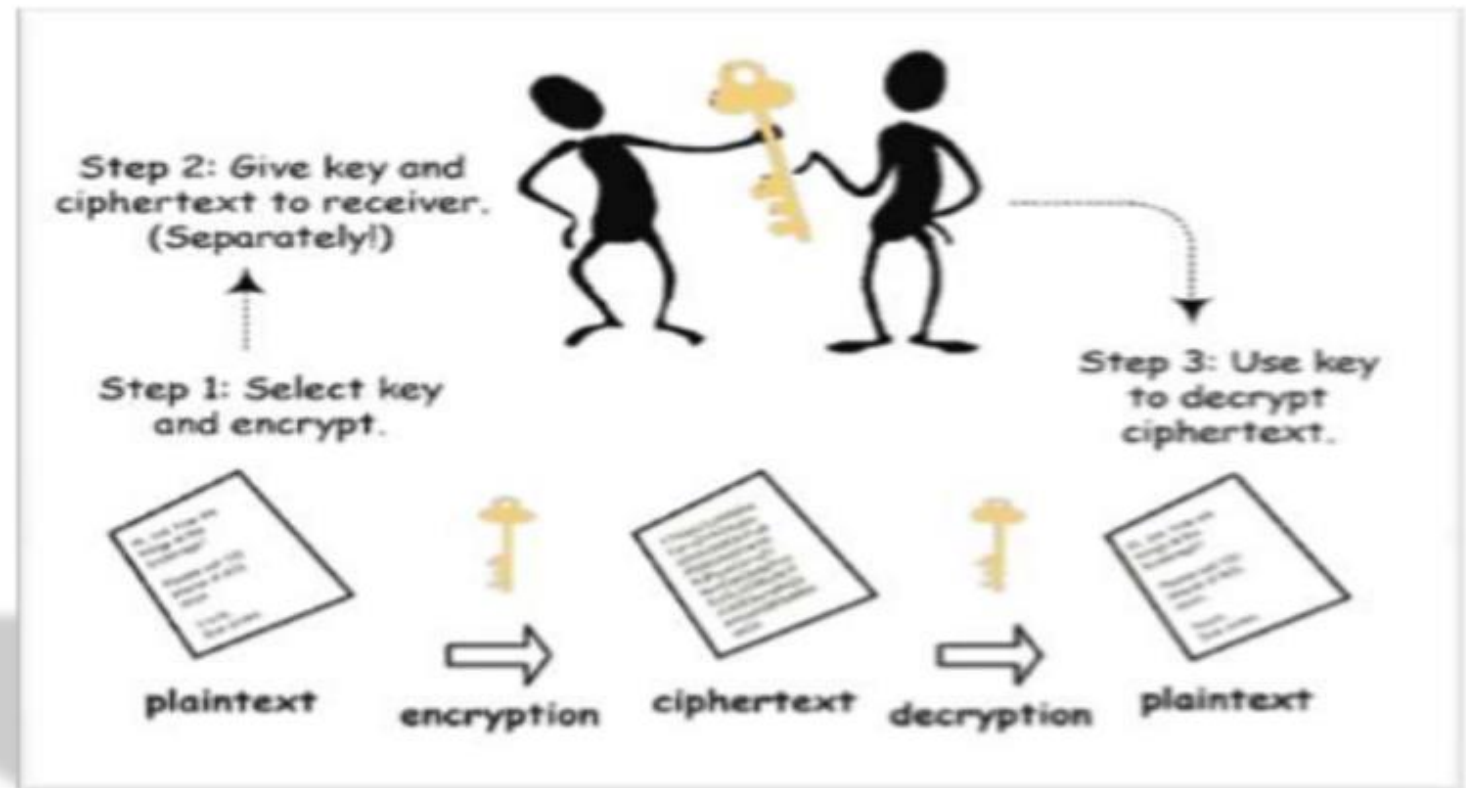
## Advantages

1. **Simpler and Faster**

## Disadvantages

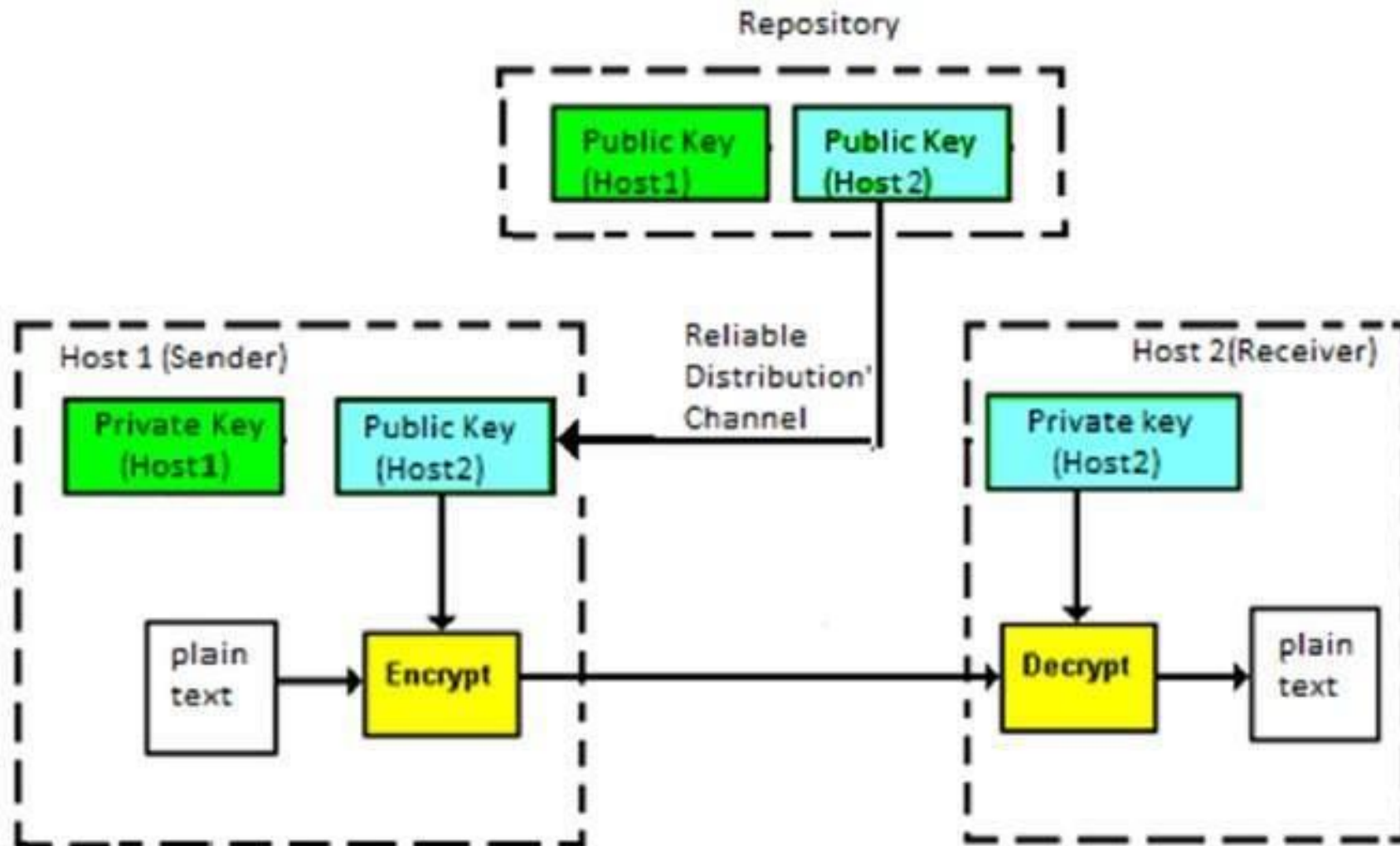
1. **Less Secured**

Image taken from :-  
[www.google.com](http://www.google.com)



# Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption.





- **Asymmetric Key Cryptography (Public Key Cryptography)**
  - 2 different keys are used
  - Users get the Key from an Certificate Authority

### Advantages

1. More Secured
2. Authentication

### Disadvantages

1. Relatively Complex

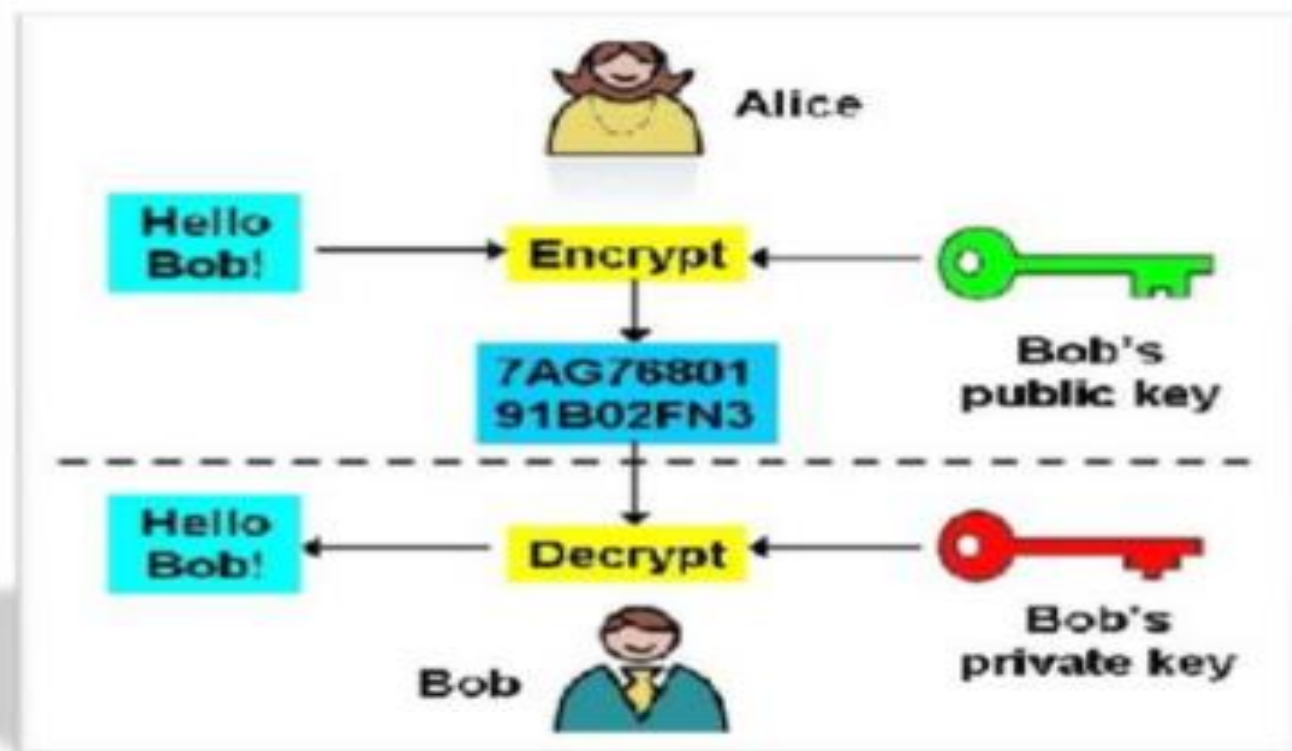


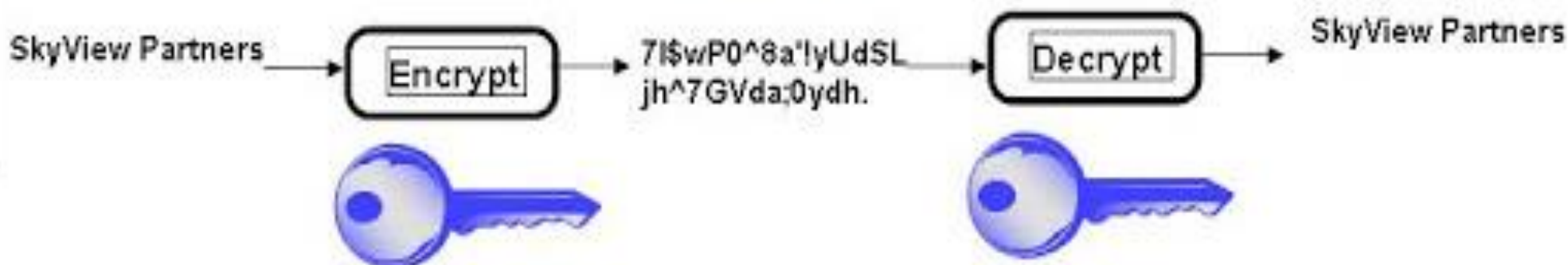
Image taken from :-  
[www.google.com](http://www.google.com)



DES  
TripleDES  
AES  
RC5

## Symmetric Keys

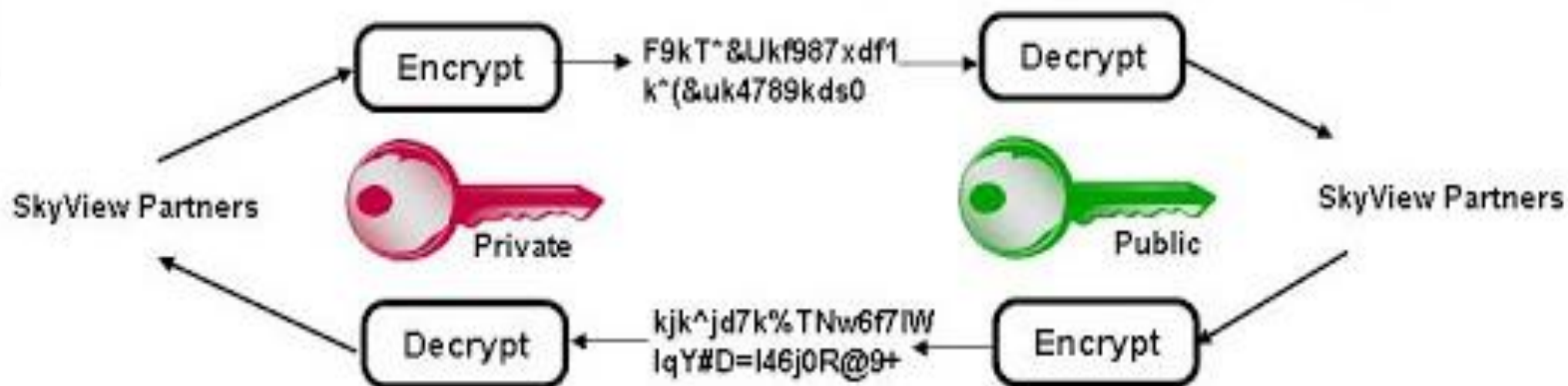
- Encryption and decryption use the **same key**.



RSA  
Elliptic  
Curve

## Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.

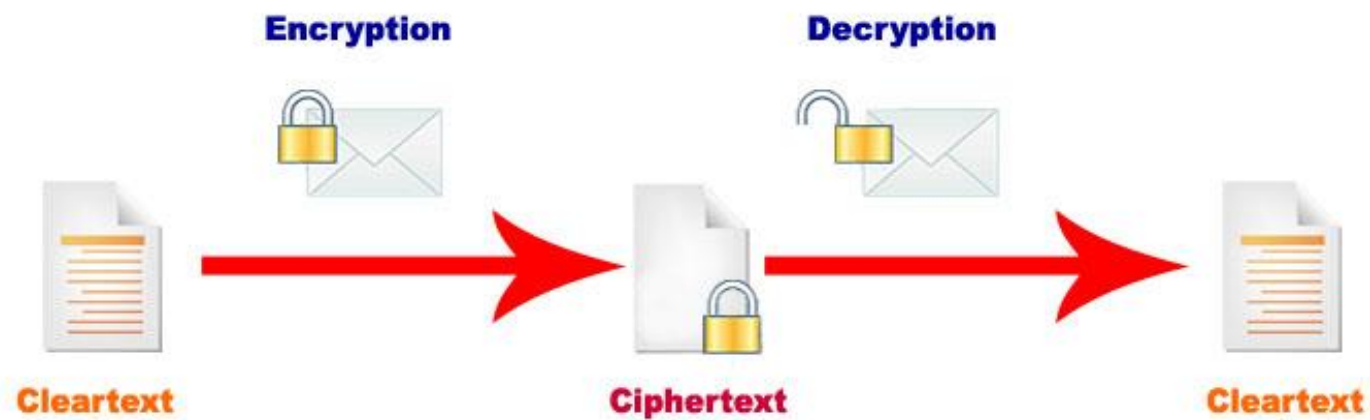
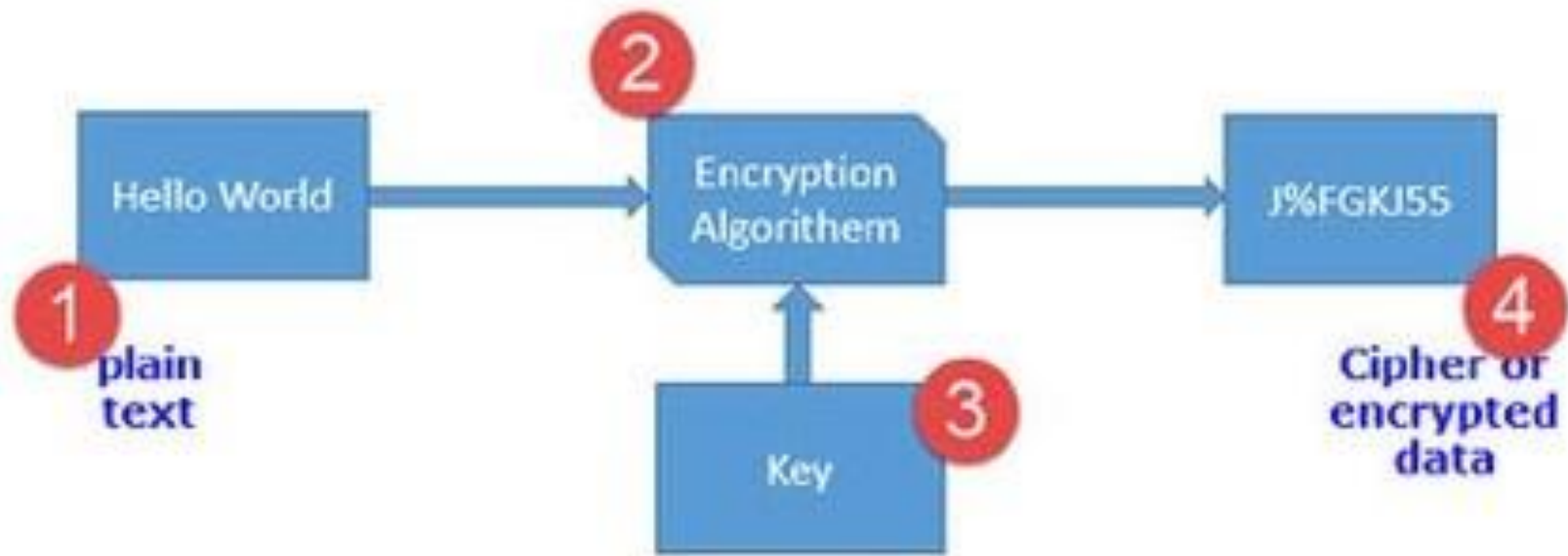


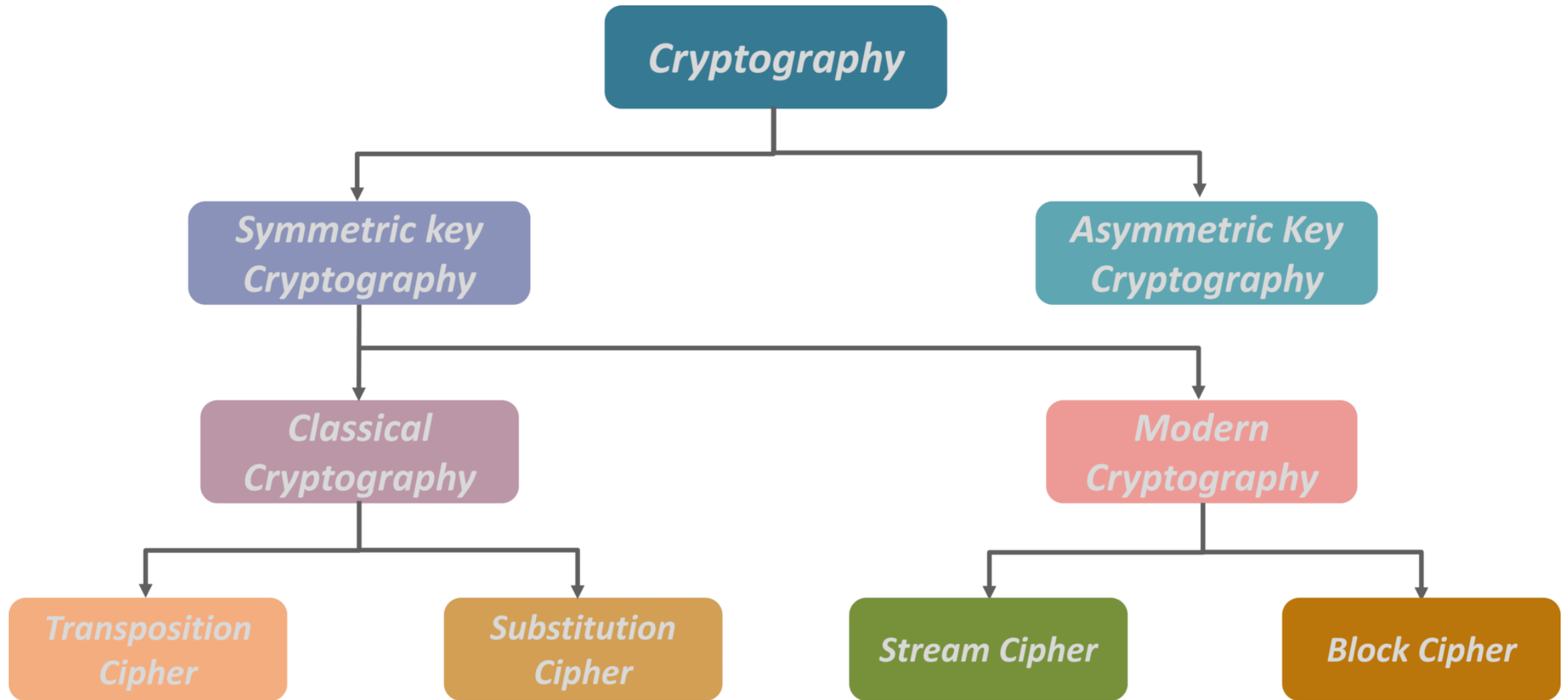
# Cipher

**Cipher** is an algorithm which is applied to plain text to get **ciphertext**.

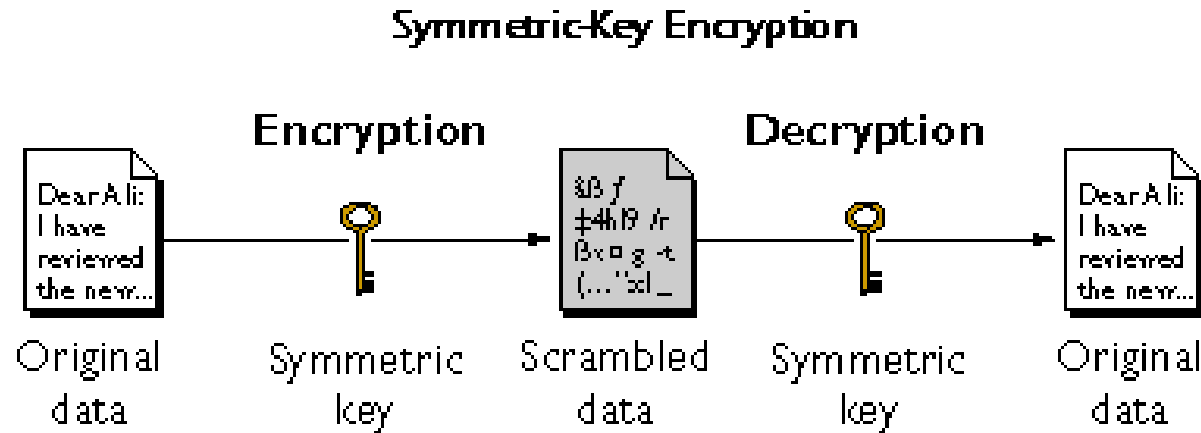
It is the unreadable output of an encryption algorithm.

A Cipher is a secret method of writing .  
Where plaintext is transformed into cipher text.





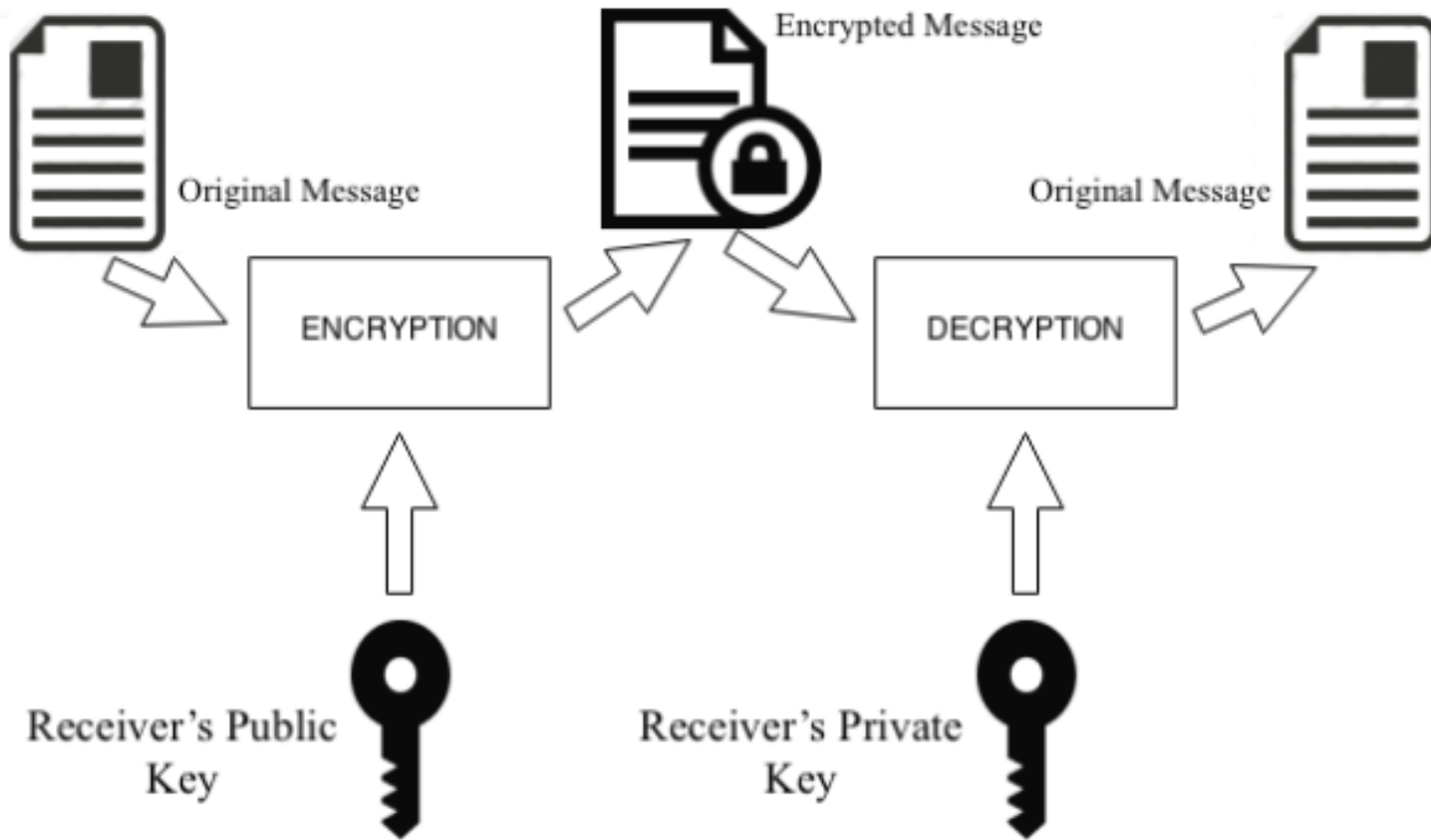
**symmetric cryptography** (or symmetric-key encryption), the same key is used for both encryption and decryption.



Symmetric key ciphers are valuable because:

01. It is relatively inexpensive to produce a strong key for these ciphers.
02. The keys tend to be much smaller for the level of protection they afford.
03. The algorithms are relatively inexpensive to process.

**Asymmetric cryptography**, also known as **public key cryptography**, uses **public** and private **keys** to encrypt and decrypt data. The **keys** are simply large numbers that have been paired together but are not identical. One **key** in the pair can be shared with everyone; it is called the **public key**



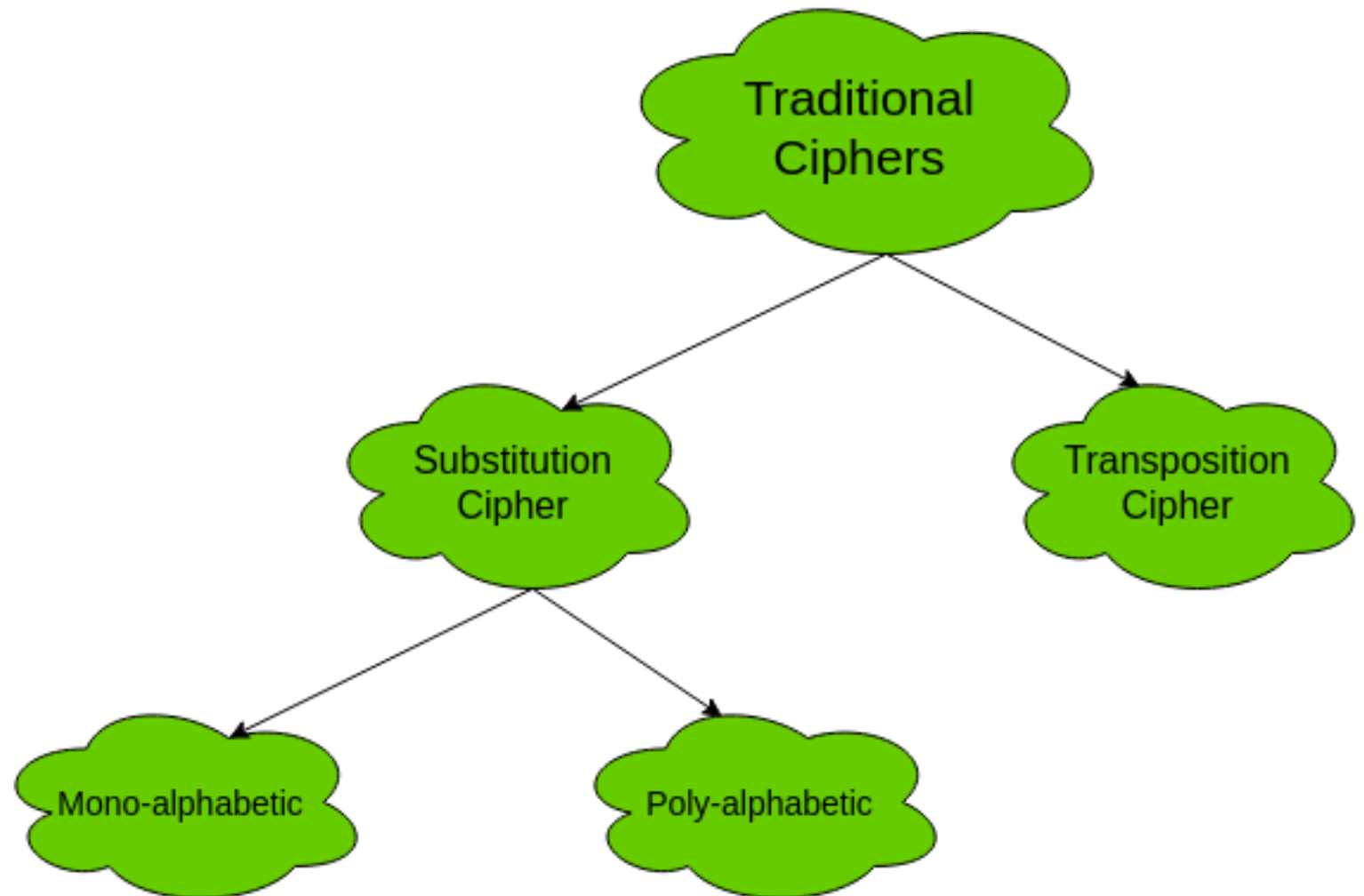
# Classical Symmetric Ciphers

The two types of traditional symmetric ciphers.

01. **Substitution Cipher**

02. **Transposition Cipher.**

The flowchart categorizes the classical ciphers.



## 1. Substitution Cipher:

Substitution Ciphers are further divided into **Mono-alphabetic Cipher** and **Poly-alphabetic Cipher**.

First, let's study about mono-alphabetic cipher.

### **Mono-alphabetic Cipher –**

In mono-alphabetic ciphers, each symbol in plain-text (eg; 'o' in 'follow') is mapped to one cipher-text symbol. No matter how many times a symbol occurs in the plain-text, it will correspond to the same cipher-text symbol.

For example, if the plain-text is 'follow' and the mapping is :

f -> g

o -> p

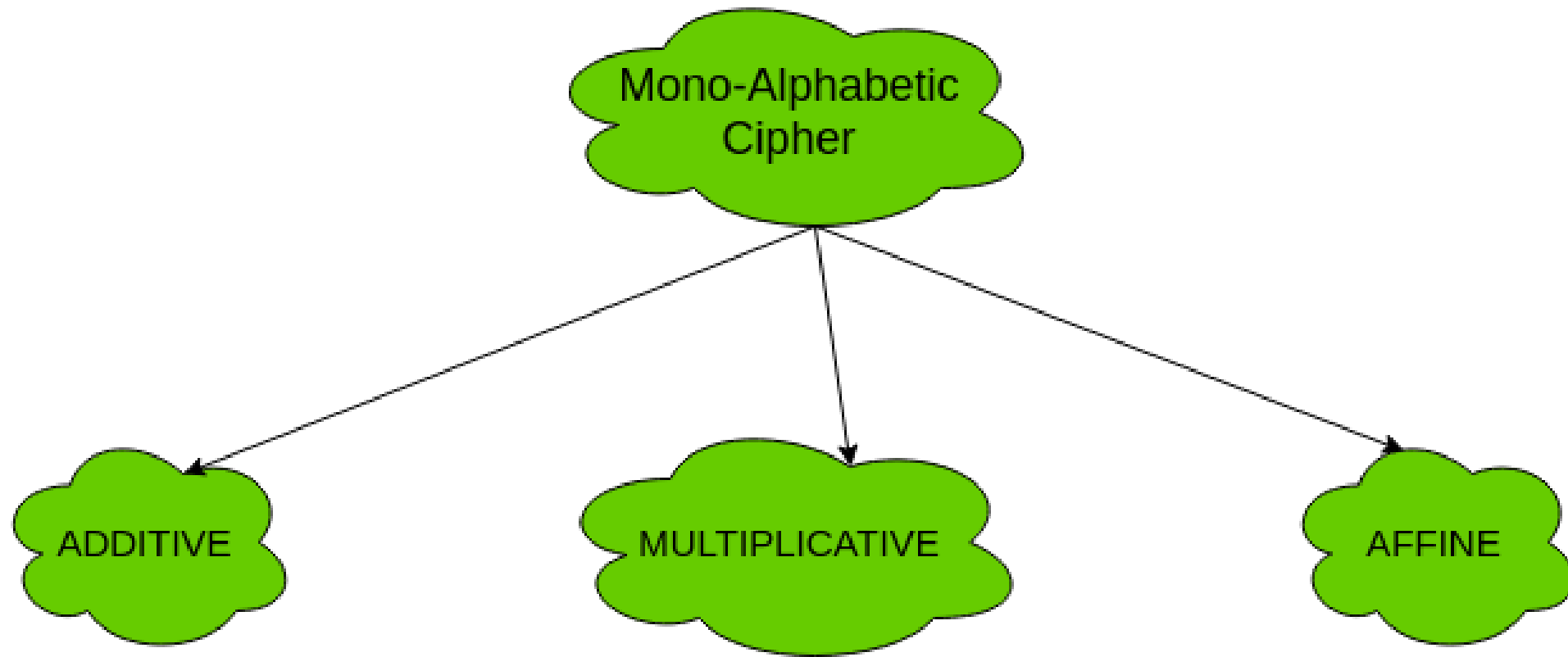
l -> m

w -> x

The cipher-text is 'gpmmpx'.

Types of mono-alphabetic ciphers are:





## (a). Additive Cipher (Shift Cipher / Caesar Cipher)

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher.

i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.

Encryption of a letter by a shift  $n$  can be described mathematically as.

$$E(x) = (x + n) \bmod 26$$

(Encryption Phase with shift  $n$ )

$$D(x) = (x - n) \bmod 26$$

(Decryption Phase with shift  $n$ )

Thus, it is not very secure. It can be broken by attack.

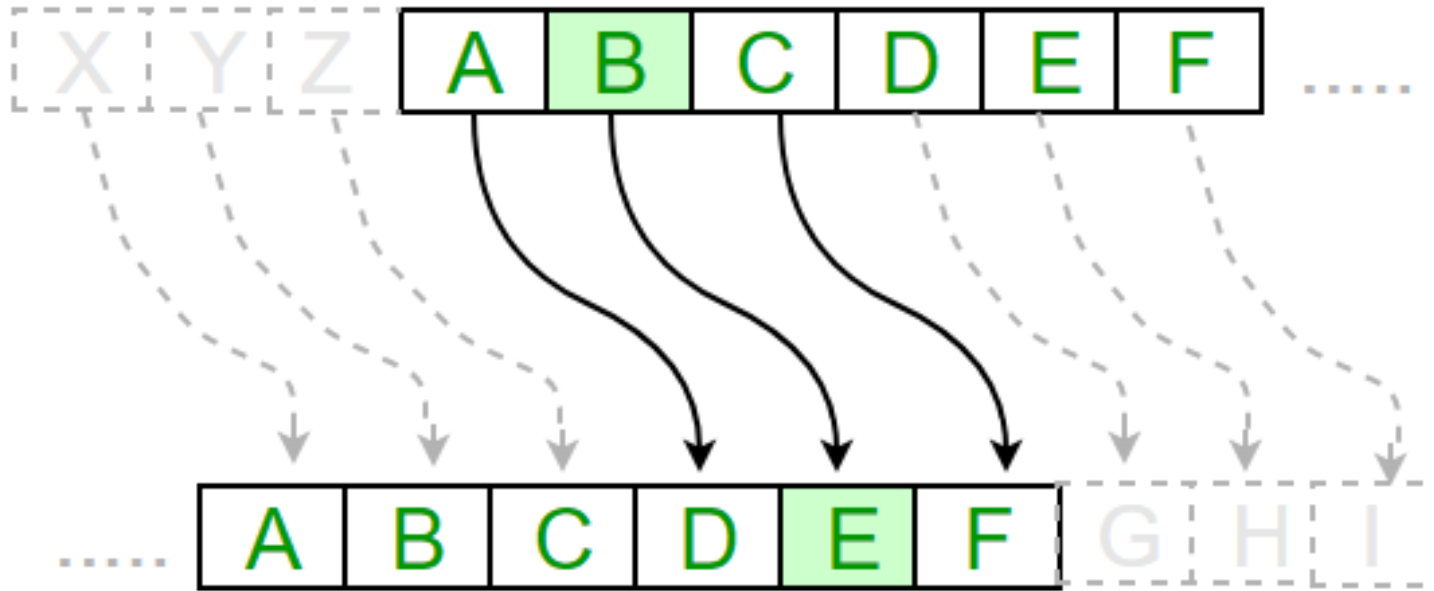
# Additive Cipher/Caesar cipher

The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a **shift cipher** and sometimes a **Caesar cipher**, but the term additive cipher better reveals its mathematical nature.

*Plaintext and ciphertext in  $Z_{26}$*

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 →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

**When the cipher is additive, the plaintext, ciphertext, and key are integers in  $Z_{26}$ .**



**Eg:**

**Text :** ABCDEFGHIJKLMNOPQRSTUVWXYZ

**Shift:** 23

**Cipher:** XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

**Text :** ATTACKATONCE

**Shift:** 4

**Cipher:** EXXEGOEXSRGI

### **(b). Multiplicative Cipher –**

The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

$$C = (M \times k) \bmod n$$

$$M = (C \times k^{-1}) \bmod n$$

where,

$k^{-1}$  -> multiplicative inverse of  $k$  (key)

Thus, it is also not very secure.

### **(c). Affine Cipher –**

The affine cipher is a combination of additive cipher and multiplicative cipher. The key space is  $26 \times 12$  (key space of additive  $\times$  key space of multiplicative) i.e. 312. It is secure than the above two as the key space is larger.

Here two keys  $k_1$  and  $k_2$  are used.

$$C = [(M \times k_1) + k_2] \bmod n$$

$$M = [(C - k_2) \times k_1^{-1}] \bmod n$$

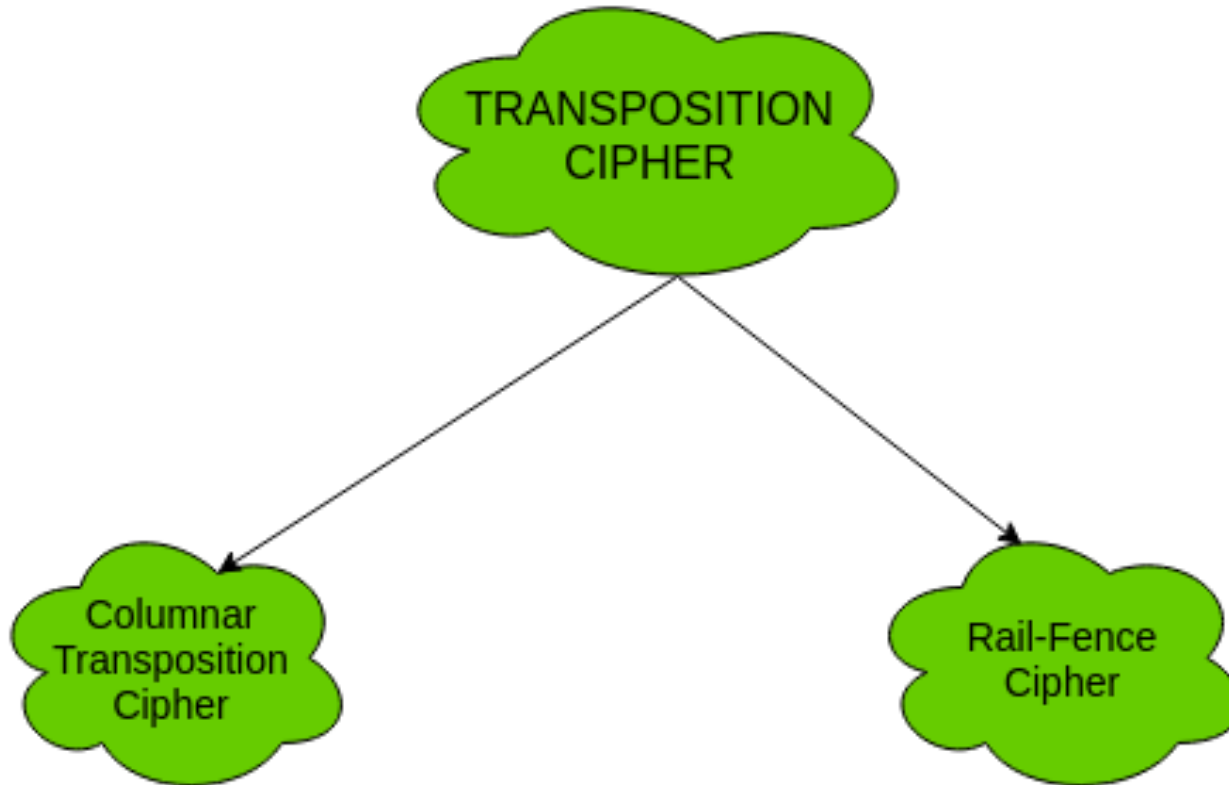
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

<b>Plaintext</b>	a	f	f	i	n	e		c	i	p	h	e	r
<b>x</b>	0	5	5	8	13	4		2	8	15	7	4	17
<b>5x+8</b>	8	33	33	48	73	28		18	48	83	43	28	93
<b>(5x+8) mod 26</b>	8	7	7	22	21	2		18	22	5	17	2	15
<b>Ciphertext</b>	I	H	H	W	V	C		S	W	F	R	C	P

## 2. Transposition Cipher:

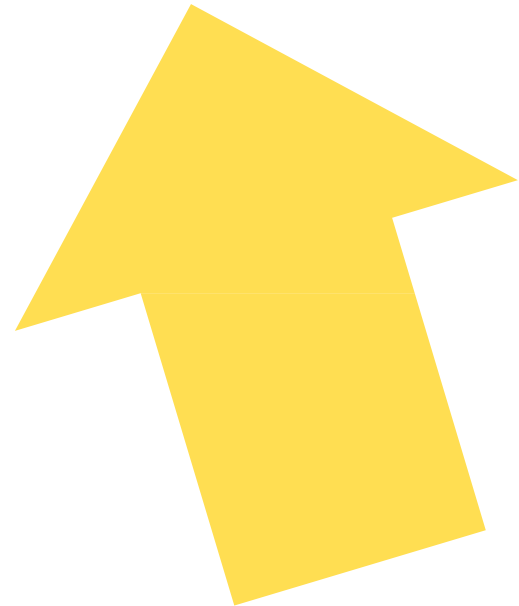
The transposition cipher does not deal with substitution of one symbol with another. It focuses on changing the position of the symbol in the plain-text. A symbol in the first position in plain-text may occur in fifth position in cipher-text.

Two of the transposition ciphers are:



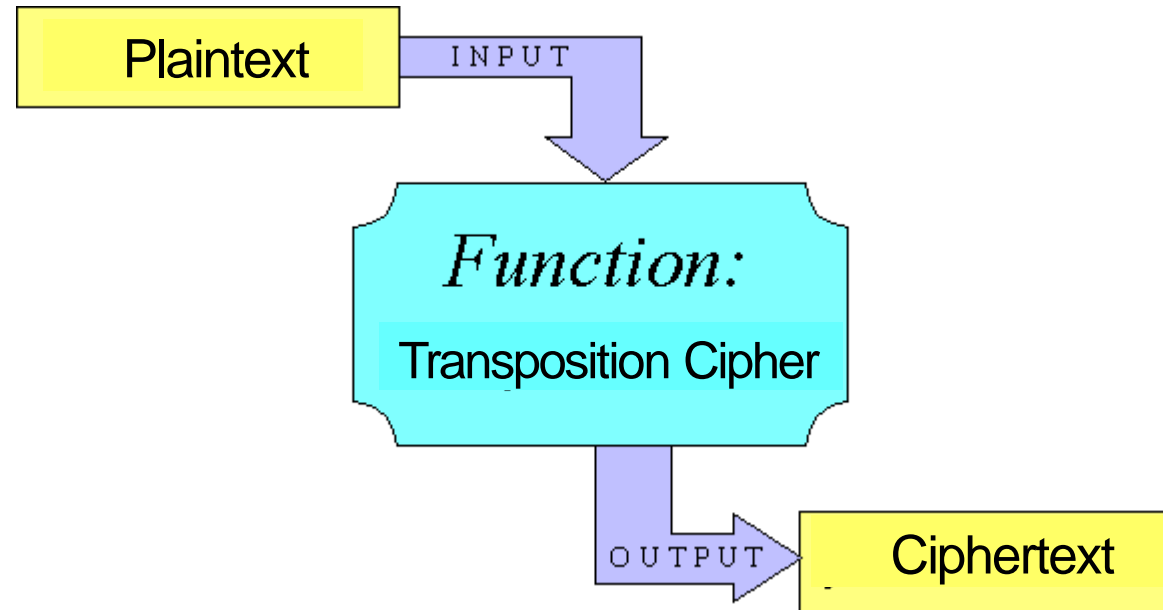
# Transposition Cipher

- Columnar
- A method of encryption in which the plaintext is shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.





# Columnar Transposition As A Function



$$\mathbf{f(\text{plaintext})=\text{ciphertext}}$$

# Columnar Transposition As A Function

- The columnar transposition cipher uses a objective function to encrypt the text and an inverse function to decrypt the text.

$$\mathbf{f(plaintext)=ciphertext}$$

$$\mathbf{f^{-1}(ciphertext)=plaintext}$$

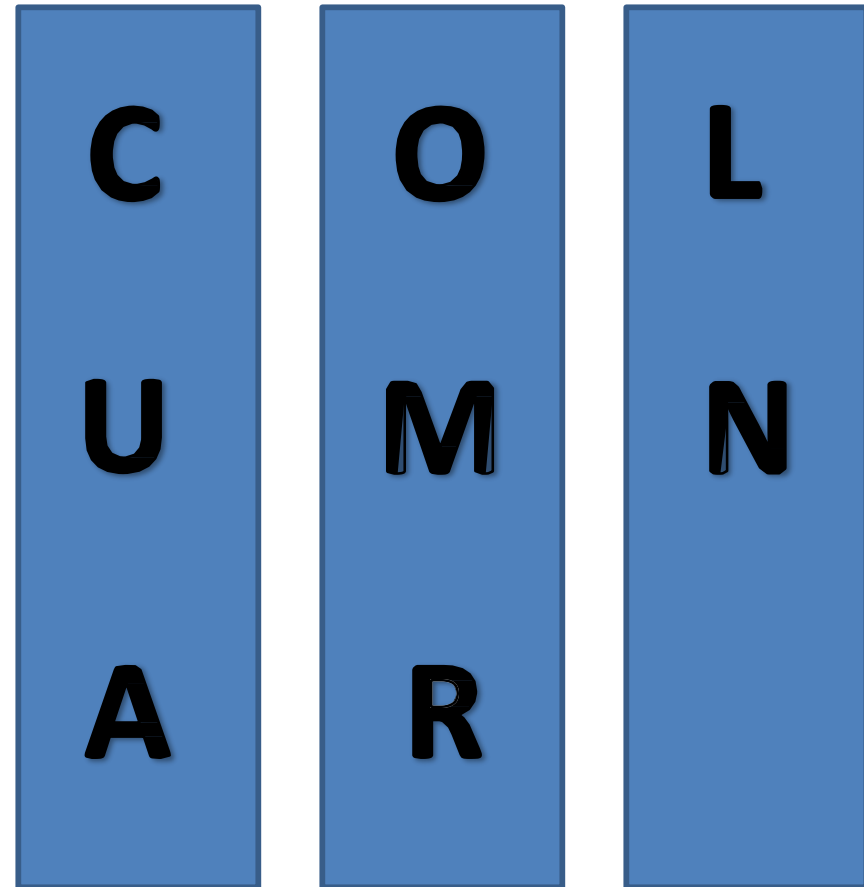
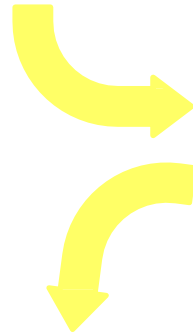
# Columnar Transposition

- Three Columns

$$C = 3$$

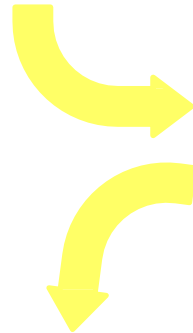
**COLUMNAR**

**CUAOMRLN**

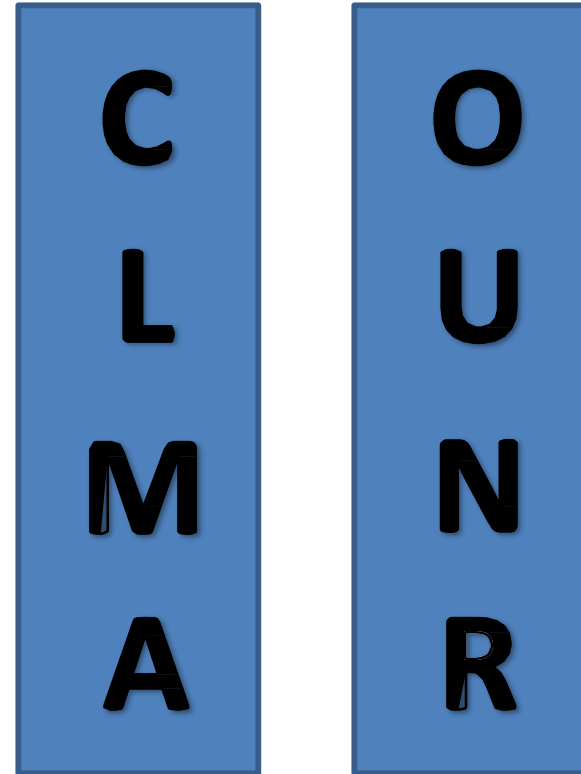


- Two Columns
- $C=2$

**COLUMNAR**



**CLMAOUNR**



# The Rail Fence Cipher

- The **rail fence cipher** (sometimes called zigzag cipher) is a **transposition cipher** that jumbles up the order of the letters of a message using a basic algorithm.
- The rail fence cipher works by writing your message on **alternate lines** across the page, and then reading off each line in turn.



example: let's consider the **plaintext** "This is a secret message".

Plaintext      T H I S I S A S E C R E T M E S S A G E

- To encode this message we will first write over two lines (the "rails of the fence") as follows:

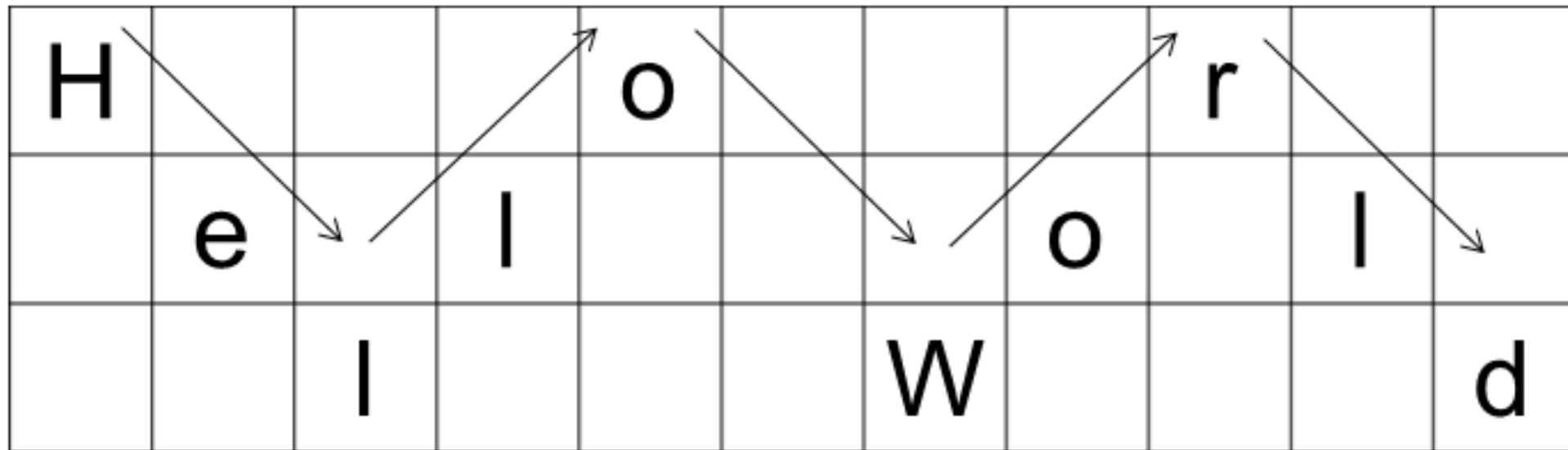
Rail Fence	T		I		I		A		E		R		T		E		S		G	
Encoding		H		S		S		S		C		E		M		S		A		E

- Note that **all white spaces have been removed** from the plain text.
- The **ciphertext** is then read off by writing the top row first, followed by the bottom row:

Ciphertext      T I I A E R T E S G H S S S C E M S A E

Eg:

**Original Message:** Hello World



**Encrypted Message:** Horel ollWd

Eg:

Plaintext

T H I S I S A S E C R E T M E S S A G E

Rail Fence

Encoding

*key = 3*

T				I				E				T				S			
	H		S		S		S		C		E		M		S		A		E
		I				A				R				E				G	

Ciphertext

T I E T S H S S S C E M S A E I A R E G

Plaintext

T H I S I S A S E C R E T M E S S A G E

Rail Fence

Encoding

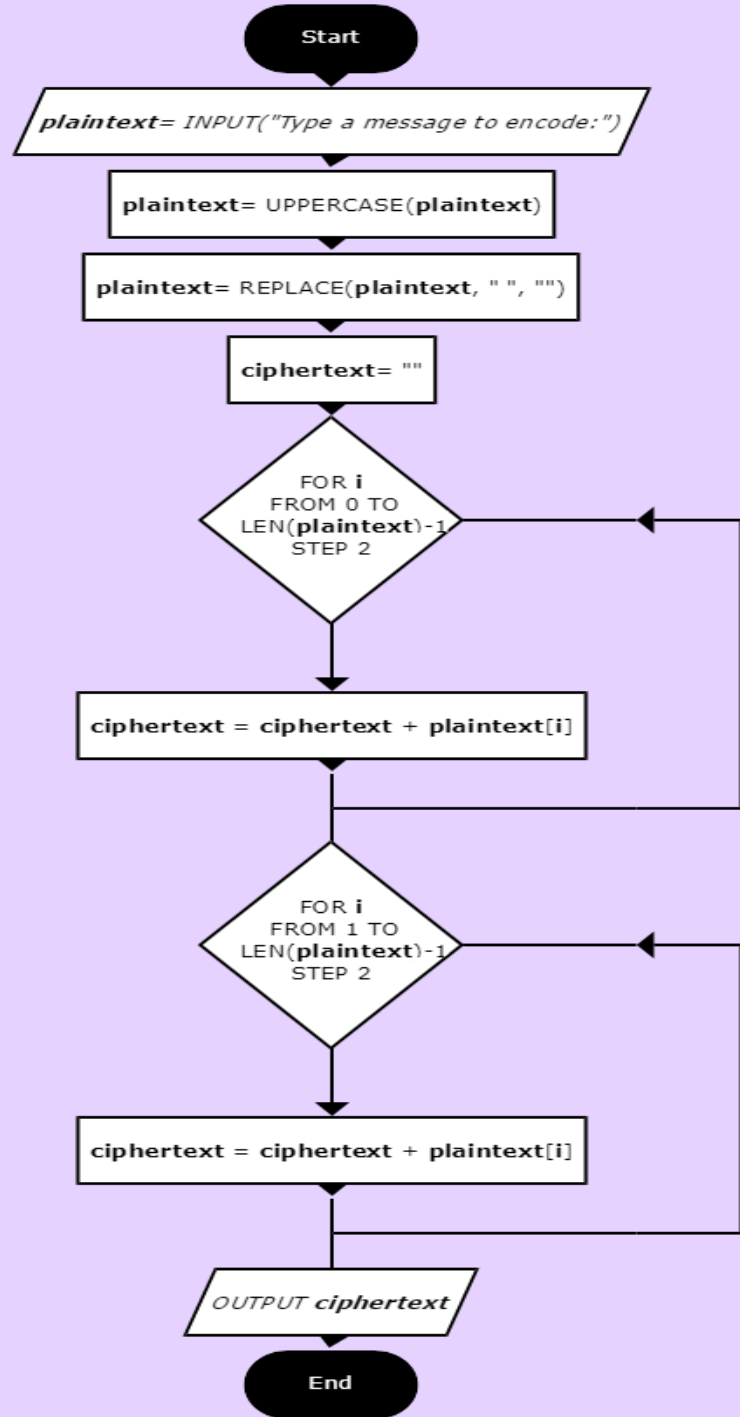
*key = 4*

T						A						T						G	
	H				S		S				E		M				A		E
		I		I				E		R				E		S			
			S						C						S				

Ciphertext

T A T G H S S E M A E I I E R E S S C S





# Cryptographic Algorithms

# Cryptographic Algorithms

There are three categories of cryptographic algorithms:

**Hashing** algorithms

**Symmetric encryption** algorithms

**Asymmetric encryption** algorithms

# Hashing Algorithms

# Hashing Algorithms

Hashing is a **one-way** process

Converting a hash back to the original data is difficult or impossible.

A hash is a unique “signature” for a set of data

This signature, called a **hash** or **digest**, represents the contents.

Hashing is used only for **integrity** to ensure that:

Information is in its original form.

No unauthorized person or malicious software has altered the data.

**Common hash algorithms**

MD5, SHA-1

# Message Digest (MD)

## Message Digest (MD) algorithm

One common hash algorithm

### Three versions

Message Digest 2 (MD2)

Message Digest 4 (MD4)

Message Digest 5 (MD5)

#### ONLINE MD5, MD4, MD2 HASH CALCULATOR



Paste plain-text data into the below textarea or upload a file up to 100KB and click the Calculate button. The resulting hashes will be shown in the box below.

If you encounter any errors with this tool please drop me a line at [info@sharethis.com](mailto:info@sharethis.com)

MD5: 361fadf1c712e812d198c4cab5712a79

MD4: c85e5fdf3a18840f9041ac70f241deb0

MD2: 8a4b081d657c2099cbfaee796217759f

# Secure Hash Algorithm (SHA)

More secure than MD

A family of hashes

## **SHA-1**

Patterned after MD4, but creates a hash that is 160 bits in length instead of 128 bits

## **SHA-2**

Comprised of four variations, known as SHA-224, SHA-256, SHA-384, and SHA-512

Considered to be a secure hash

## **Message Digest 5 (MD5)**

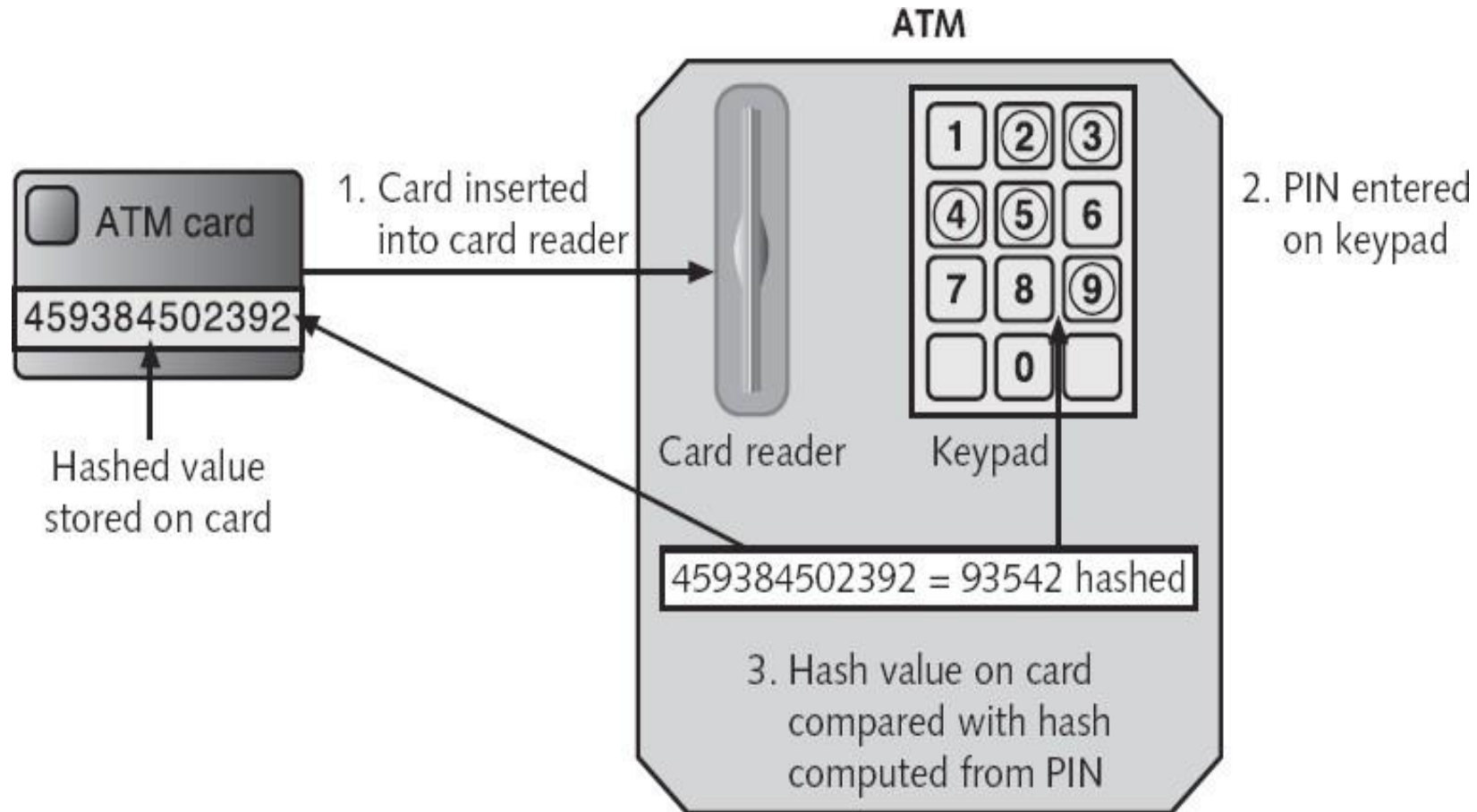
- Most well-known of the MD hash algorithms
- Message length to 512 bits
- Weaknesses in compression function could lead to collisions
- Some security experts recommend using a more secure hash algorithm

## **Secure Hash Algorithm (SHA)**

- More secure than MD
- SHA-2 is currently considered to be a secure hash
- SHA-3 was announced as a new standard in 2015 and may be suitable for low-power devices



# Hashing Algorithms (continued)



**Figure 11-3** Hashing at an ATM

# PIN Crackers Nab Holy Grail of Bank Card Security

By Kim Zetter  April 14, 2009 | 10:55:00 PM Categories: [Crime](#)

Hackers have crossed into new frontiers by devising sophisticated ways to steal large amounts of personal identification numbers, or PINs, protecting credit and debit cards, says an investigator. The attacks involve both unencrypted PINs and encrypted PINs that attackers have found a way to crack, according to an investigator behind a new report looking at the data breaches.

The attacks, says Bryan Sartin, director of investigative response for Verizon Business, are behind some of the millions of dollars in fraudulent ATM withdrawals that have

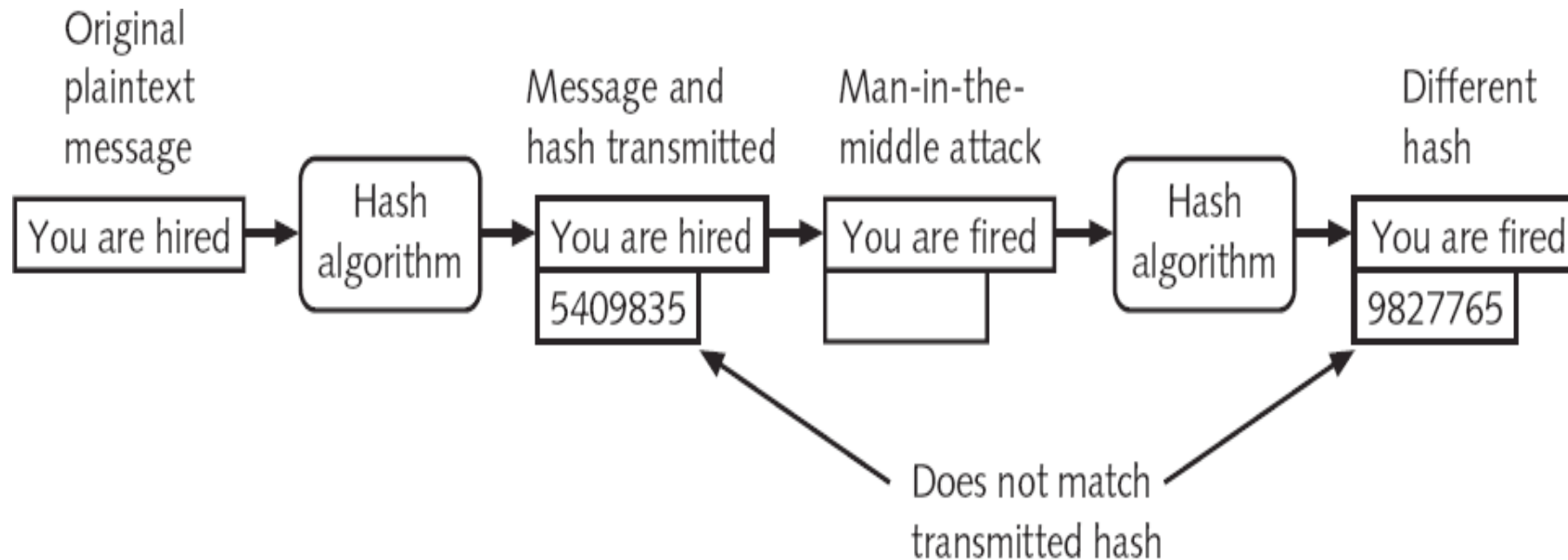


# Hashing Algorithm Security

A hashing algorithm is considered secure if:

- The ciphertext hash is a fixed size
- Two different sets of data cannot produce the same hash, which is known as a **collision**
- It should be impossible to produce a data set that has a desired.
- The resulting hash ciphertext cannot be reversed to find the original data

# Preventing a Man-in-the-Middle Attack with Hashing

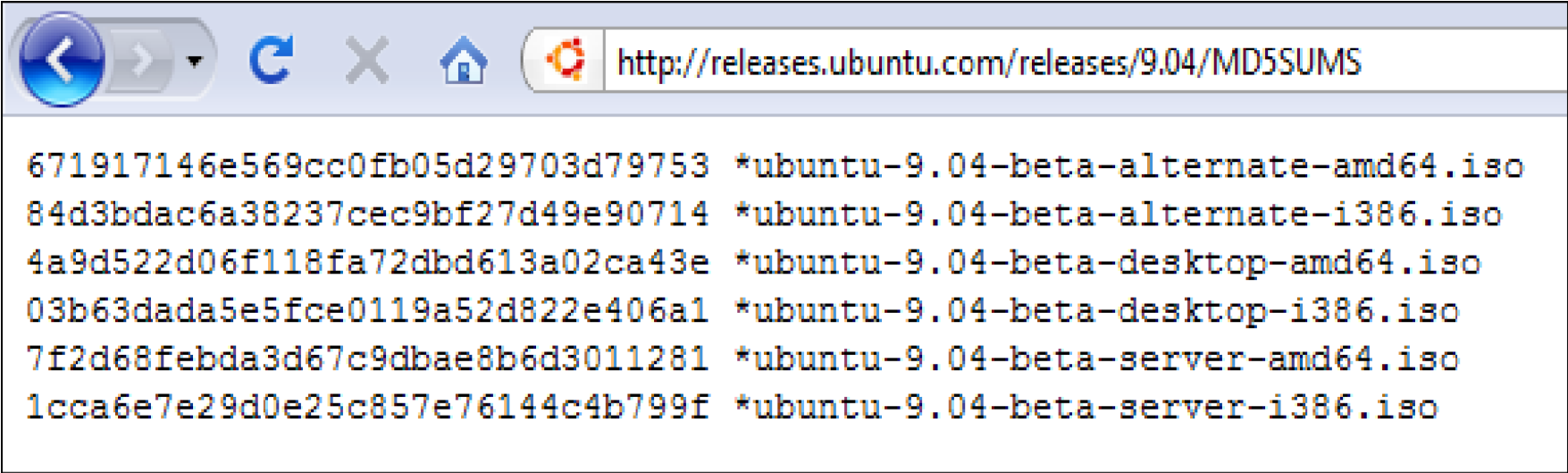


**Figure 11-4** Man-in-the-middle attack defeated by hashing

# Hashing Algorithms (continued)

Hash values are often posted on Internet sites

In order to verify the file integrity of files that can be downloaded



A screenshot of a web browser window. The address bar shows the URL <http://releases.ubuntu.com/releases/9.04/MD5SUMS>. The main content area displays a list of MD5 hash values followed by the names of the corresponding ISO files. The text is as follows:

```
671917146e569cc0fb05d29703d79753 *ubuntu-9.04-beta-alternate-amd64.iso
84d3bdac6a38237cec9bf27d49e90714 *ubuntu-9.04-beta-alternate-i386.iso
4a9d522d06f118fa72dbd613a02ca43e *ubuntu-9.04-beta-desktop-amd64.iso
03b63dada5e5fce0119a52d822e406a1 *ubuntu-9.04-beta-desktop-i386.iso
7f2d68febda3d67c9dbae8b6d3011281 *ubuntu-9.04-beta-server-amd64.iso
1cca6e7e29d0e25c857e76144c4b799f *ubuntu-9.04-beta-server-i386.iso
```

# Hashing Algorithms Only Ensure Integrity

Characteristic	Protection?
Confidentiality	No
Integrity	Yes
Availability	No
Authenticity	No
Non-repudiation	No

**Table 11-2** Information protections by hashing cryptography

# Password Hashes

Another use for hashes is in storing passwords.

When a password for an account is created, the password is hashed and stored.

The Microsoft NT family of Windows operating systems hashes passwords in two different forms

- 01.LM (LAN Manager) hash

- 02.NTLM (New Technology LAN Manager) hash

Most Linux systems use password-hashing algorithms such as MD5.

Apple Mac OS X uses SHA-1 hashes

# Symmetric Cryptographic Algorithms



# Symmetric Cryptographic Algorithms

Use the same single key to encrypt and decrypt a message

- Also called private key cryptography

(the key is kept private between sender and receiver)

## **Stream cipher**

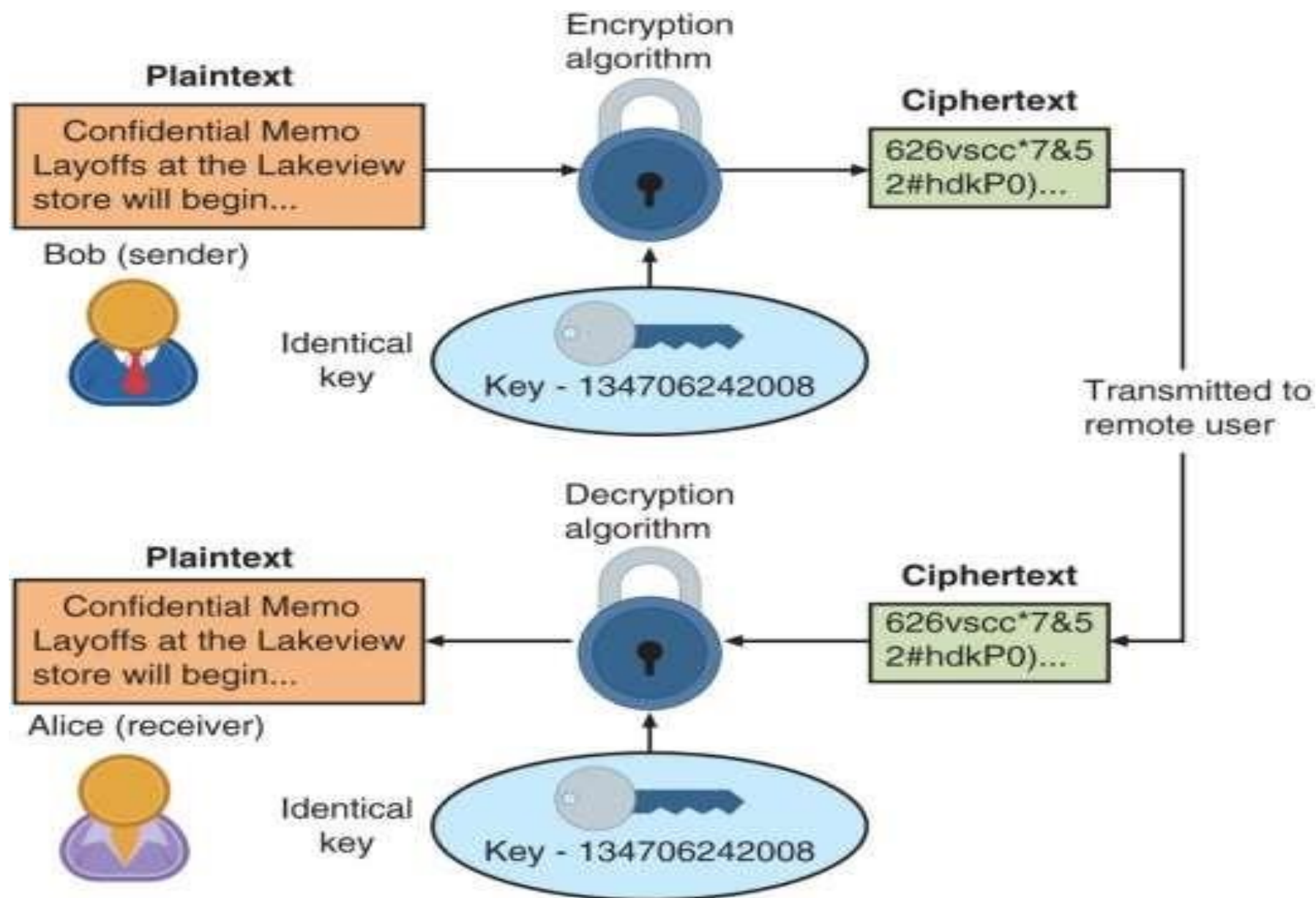
Takes one character and replaces it with one character

WEP (Wired Equivalent Protocol) is a stream cipher

## **Substitution cipher**

The simplest type of stream cipher

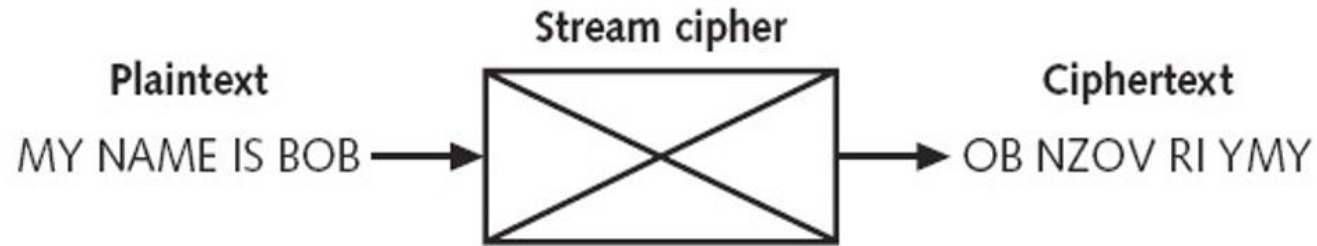
Simply substitutes one letter or character for another



**Figure 3-6** Symmetric (private key) cryptography

# Stream Cipher

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 - **Plaintext letters**  
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A - **Substitution letters**



# Substitution Cipher



# XOR(eXclusive OR)

With most symmetric ciphers, the final step is to combine the cipher stream with the plaintext to create the ciphertext

The process is accomplished through the exclusive OR (XOR) binary logic operation

## **One-time pad (OTP)**

Combines a truly random key with the plaintext



# Block Cipher

Manipulates an entire block of plaintext at one time

Plaintext message is divided into separate blocks of 8 to 16 bytes

And then each block is encrypted independently

Stream cipher advantages and disadvantages

01.Fast when the plaintext is short

02.Block ciphers are more secure than stream ciphers

# Information Protections by Symmetric Cryptography

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	No
Non-repudiation	No

**Table 11-3** Information protections by symmetric cryptography

## **Common algorithms include:**

- Data Encryption Standard (DES)
- Triple Data Encryption Standard(3DES)
- Advanced Encryption Standard (AES)
- Several other algorithms



# **DES and 3DES**

## **Data Encryption Standard(DES)**

Declared as a standard by the U.S Government.

DES is a block cipher and encrypts data in 64-bit blocks.

Uses 56-bit key, very insecure.

Has been broken many times.

## **Triple Data Encryption Standard (3DES)**

Uses three rounds of DES encryption.

Effective key length 112 bits.

Considered secure

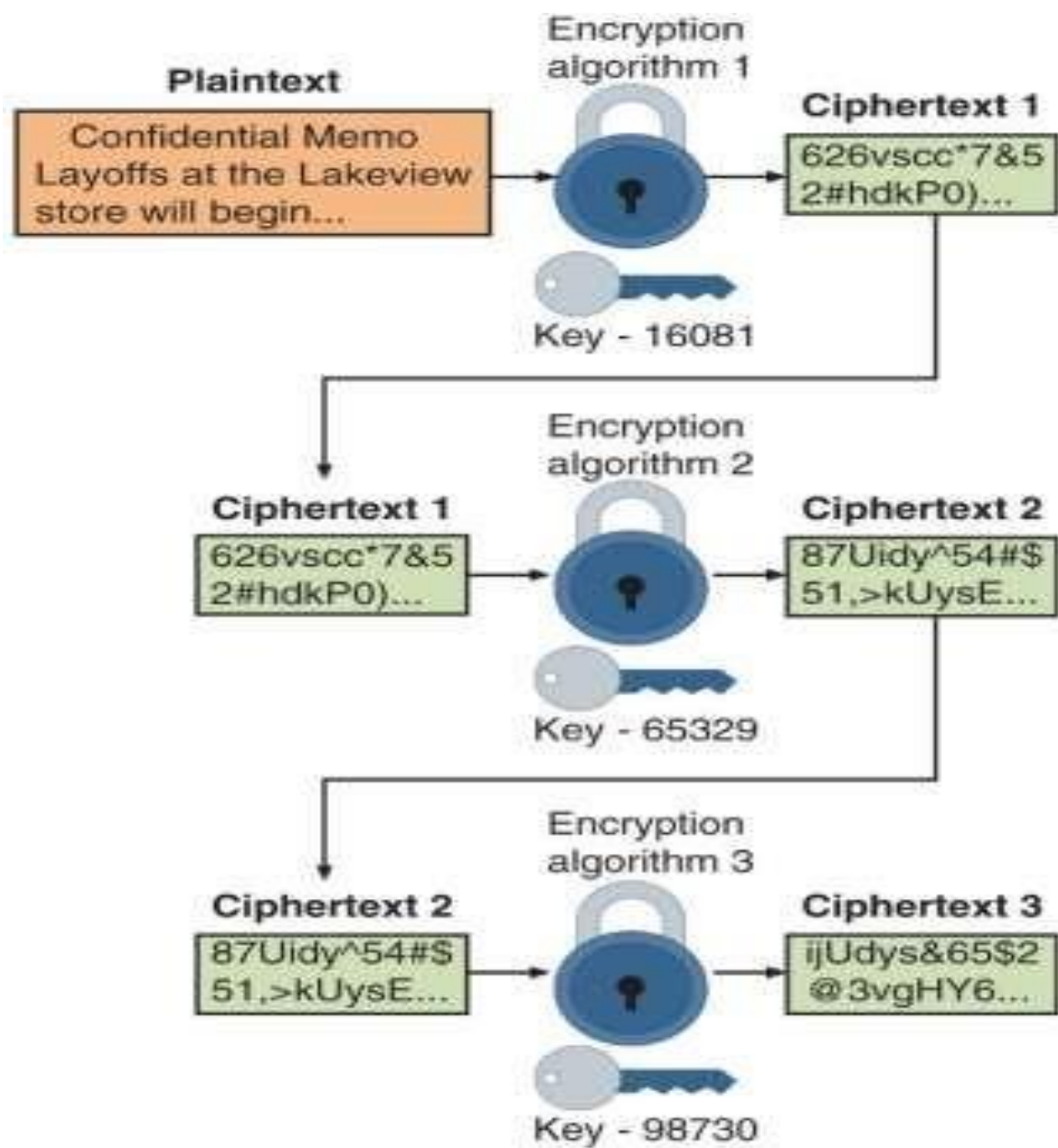


Figure 3-7 3DES

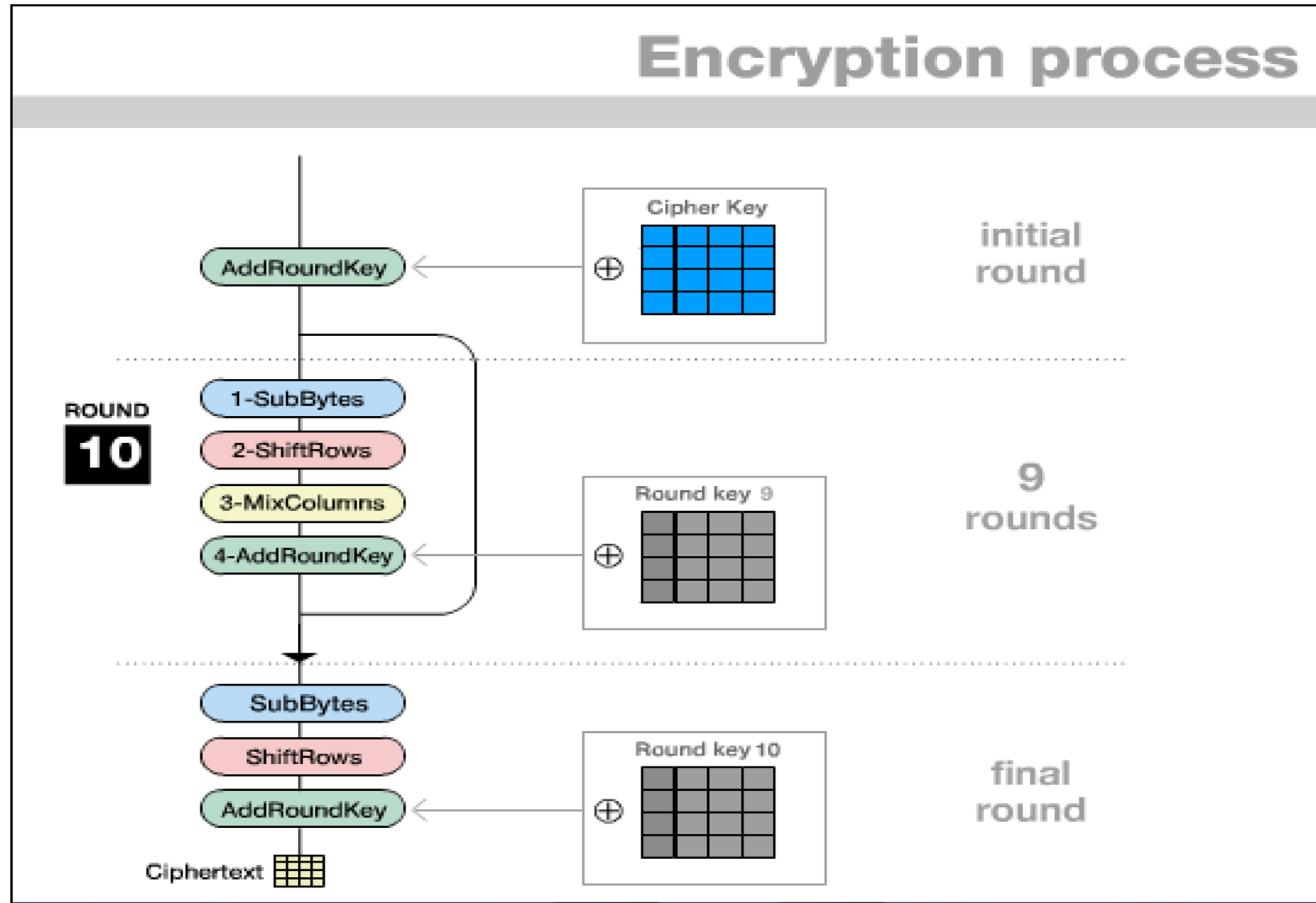
# **Advanced Encryption Standard (AES)**

Approved by the NIST in late 2000 as a replacement for DES.

Official standard for U.S. Government.

Considered secure has not been cracked.

# Animation of AES Algorithm



# Other Algorithms

Several other symmetric cryptographic algorithms are also used:

Rivest Cipher (RC) family from RC1 to RC6

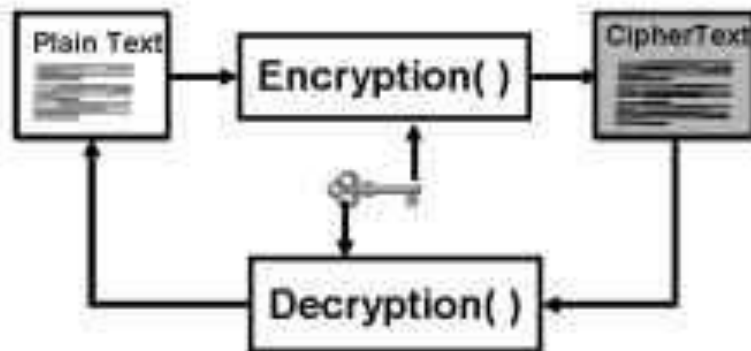
International Data Encryption Algorithm (IDEA)

Blowfish

Twofish

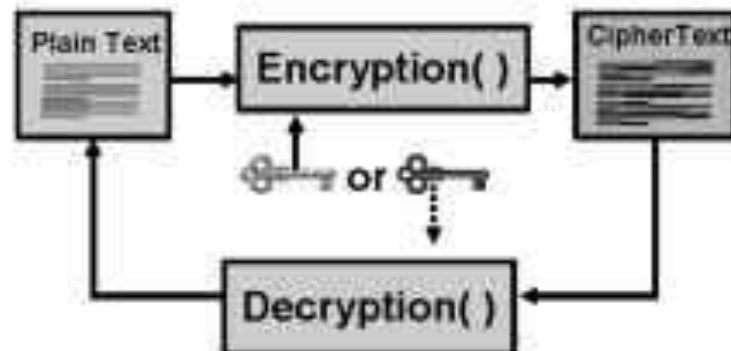
# Symmetric vs. Asymmetric Encryption Algorithms

## Symmetric



- Secret key cryptography
- Encryption and decryption use the same key
- Typically used to encrypt the content of a message
- Examples: DES, 3DES, AES

## Asymmetric



- Public key cryptography
- Encryption and decryption use different keys
- Typically used in digital certification and key management
- Example: RSA

# Asymmetric Cryptographic Algorithms

# Asymmetric Cryptographic Algorithms

## **Asymmetric cryptographic algorithms**

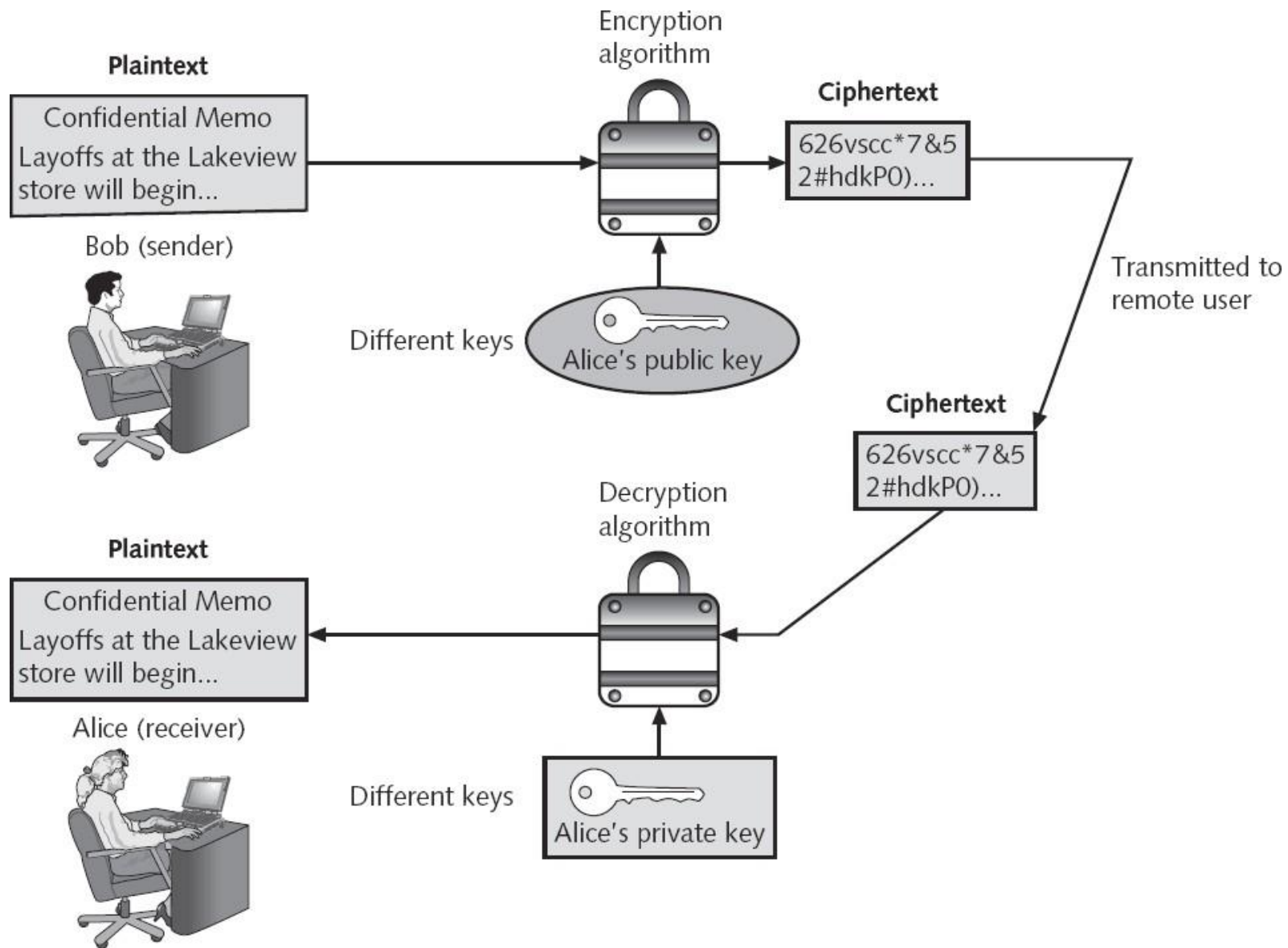
Also known as **public key cryptography**

Uses two keys instead of one

- The **public key** is known to everyone and can be freely distributed
- The **private key** is known only to the receiver of the message

Asymmetric cryptography can also be used to create a **digital signature**





**Figure 11-12** Asymmetric cryptography

# Digital Signature

Verify the sender

Prove the integrity of the message.

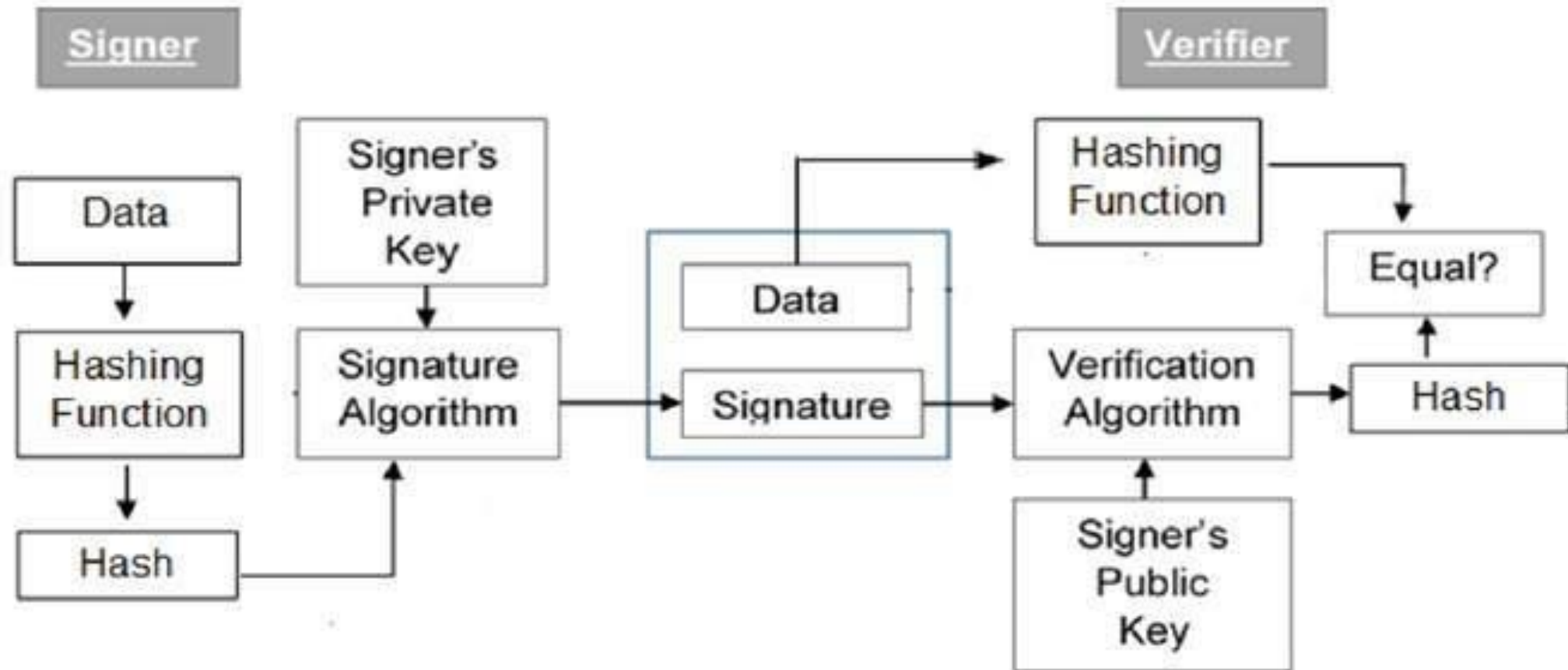
Digital signatures are the public-key primitives of message authentication.

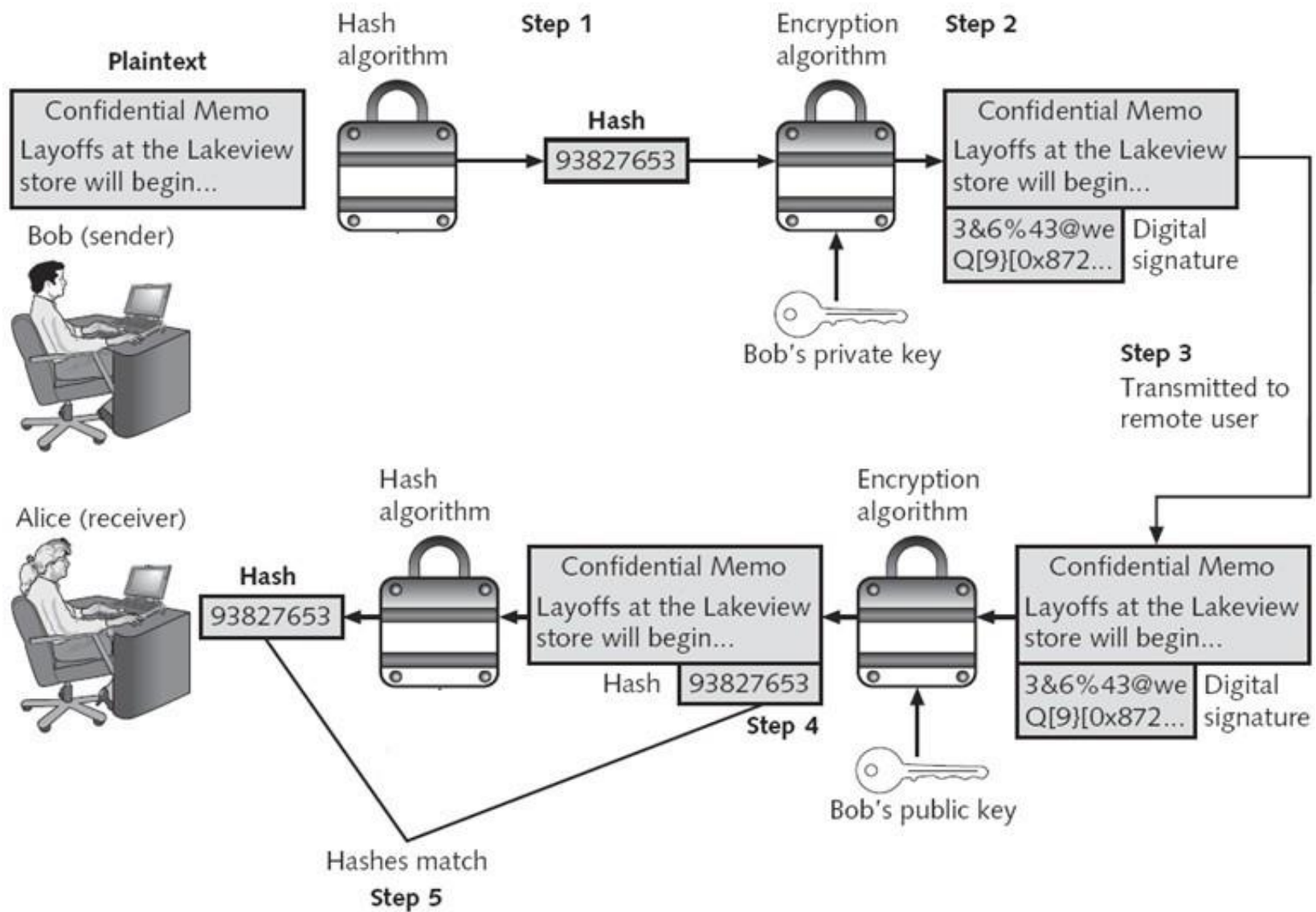
it is common to use handwritten signatures on handwritten or typed messages.

A digital signature does not encrypt the message, it only signs it...

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

# Model of Digital Signature





**Figure 11-13** Digital signatures

# Information Protections by Asymmetric Cryptography

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	Yes
Non-repudiation	Yes

**Table 11-6** Information protections by asymmetric cryptography

# RSA( (Rivest–Shamir–Adleman)

The most common asymmetric cryptography algorithm

RSA makes the public and private keys by multiplying two large prime numbers  $p$  and  $q$

To compute their product ( $n=pq$ )

It is very difficult to **factor** the number  $n$  to find  $p$  and  $q$

Finding the private key from the public key would require a factoring operation

RSA is complex and slow, but secure

100 times slower than DES

# Diffie-Hellman

A key exchange algorithm, not an encryption algorithm.

Allows two users to share a secret key securely over a public network.

Once the key has been shared

Then both parties can use it to encrypt and decrypt messages using symmetric cryptography

# HTTPS

Secure Web Pages typically use RSA, Diffie-Hellman, and a symmetric algorithm like RC4

RSA is used to send the private key for the symmetric encryption





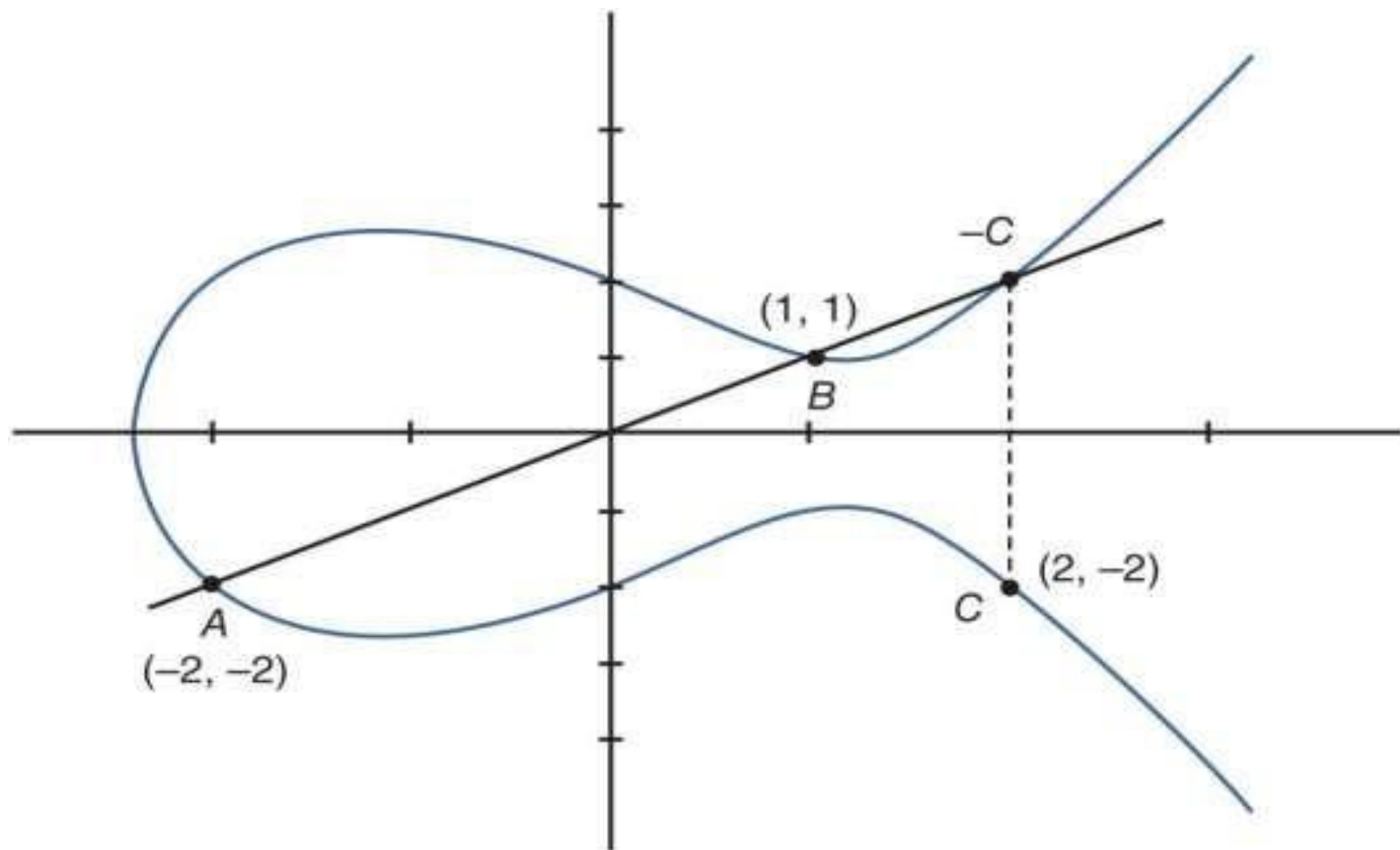
# Elliptic Curve Cryptography

An elliptic curve is a function drawn on an X-Y axis as a gently curved line.

By adding the values of two points on the curve, you can arrive at a third point on the curve.

The public aspect of an elliptic curve cryptosystem is that users share an elliptic curve and one point on the curve

Not common, but may one day replace RSA



**Figure 3-9** Elliptic curve cryptography (ECC)

# Using Cryptography on Files and Disks

# Encrypting Files: PGP and GPG

## **Pretty Good Privacy (PGP)**

One of the most widely used asymmetric cryptography system for files and e-mail messages on Windows systems

## **GNU Privacy Guard (GPG)**

A similar open-source program

PGP and GPG use both asymmetric and symmetric cryptography

# Encrypting Files: Encrypting File System (EFS)

Part of Windows.

Uses the Windows NTFS file system.

Because EFS is tightly integrated with the file system, file encryption and decryption are transparent to the user.

EFS encrypts the data as it is written to disk

On Macs, **Filevault** encrypts a user's home folder.

# Whole Disk Encryption

## **Windows BitLocker**

A hardware-enabled data encryption feature

Can encrypt the entire Windows volume

Includes Windows system files as well as all user files

Encrypts the entire system volume, including the Windows Registry and any temporary files that might hold confidential information

## **True Crypt**

Open-source, free, and can encrypt folders or files

# Trusted Platform Module (TPM)

- A chip on the motherboard of the computer that provides cryptographic services
- If the computer does not support hardware-based TPM then the encryption keys for securing the data on the hard drive can be stored by BitLocker on a USB flash drive

# Cold Boot Attack

Can defeat all currently available whole disk encryption techniques.

