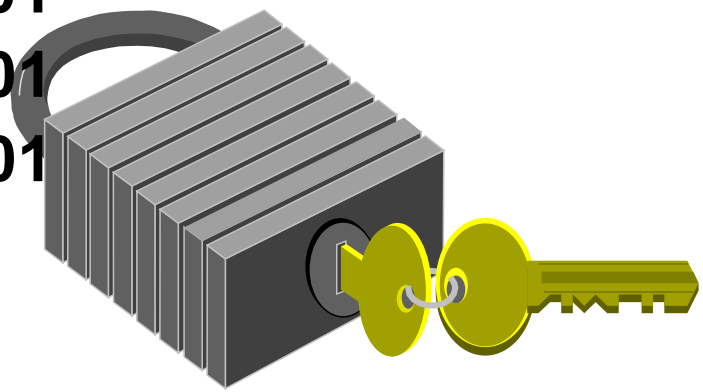
Encryption and Cryptography

0010100101110011
1001010010110011
0010111001001011



Using Encryption a message in its original form (plaintext) is encrypted into an unintelligible form (ciphertext) by a set of procedures known as an encryption algorithm and a variable, called a key; and the ciphertext is transformed (decrypted) back into plaintext using the encryption algorithm and a key. Encryption forms the basis of many technological solutions to computer and communications security problems.

Plan for the Lecture

- Definitions
- Types of Encryption
- History
- Classical Encryption Techniques
- Uses of Encryption
- Encryption in the OSI Model
- Security of Encryption Algorithms

Definition

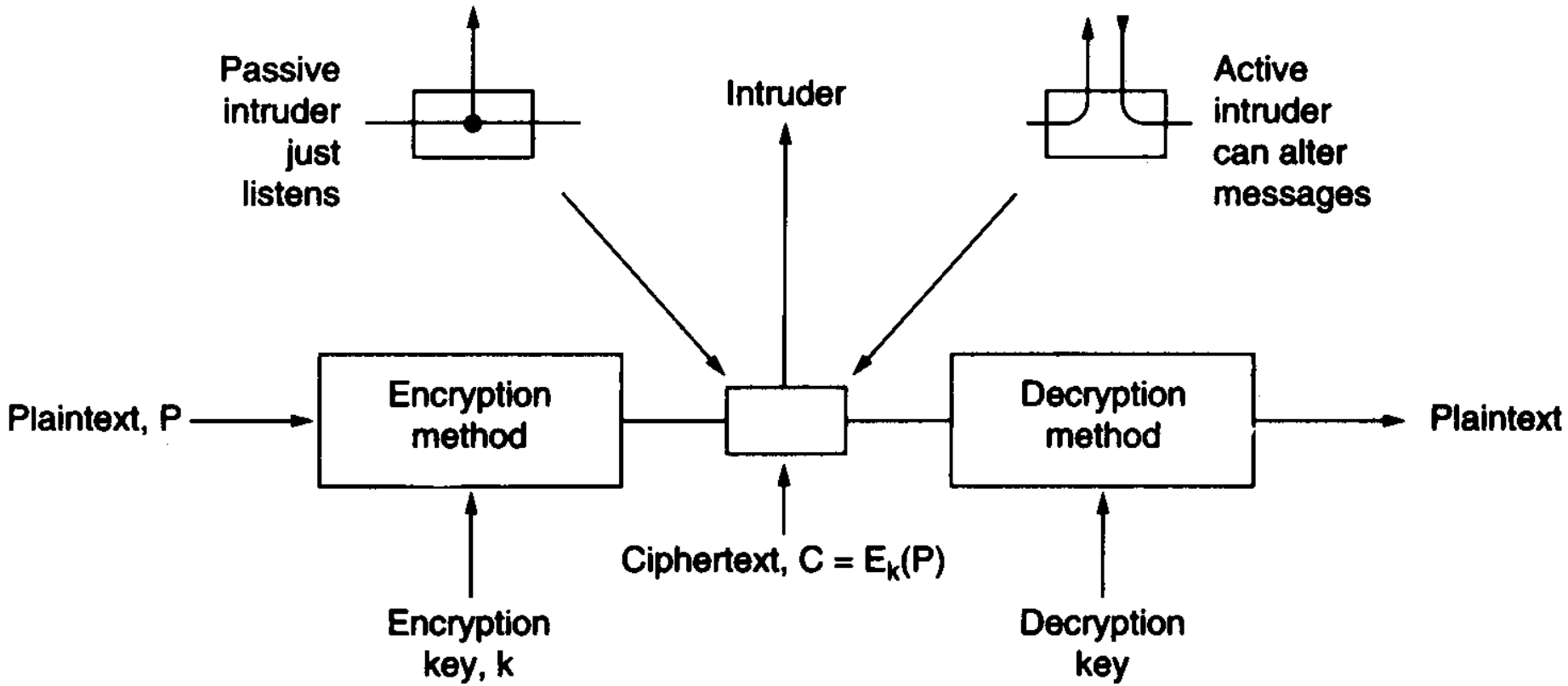
- Encryption normally works in the following way:

“ A message in its original form (plaintext) is encrypted into an unintelligible form (ciphertext) by a set of procedures known as an encryption algorithm and a variable, called a key; and the ciphertext is transformed (decrypted) back into plaintext using the encryption algorithm and a key.”

Definitions - Crypto-speak

- **Cryptography** is the study of secret (crypto-) writing (-graphy)
- Cryptography deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications
- The practitioner of Cryptography is called **Cryptographer**

Definitions



Why Cryptography?

- Concerned with developing algorithms which may be used to:
  - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  - Verify the correctness of a message to the recipient (authentication)
  - Forms the basis of many technological solutions to computer and communications security problems

Definitions

- In cryptographic terminology, the message is called **plaintext** or **cleartext**.
- Encoding the contents of the message in such a way that hides its contents from outsiders is called **encryption**.
- A method of encryption and decryption is called a cipher - The name cipher originates from the Hebrew word "Saphar," meaning "to number."
- The encrypted message is called the **ciphertext**.
- The process of retrieving the plaintext from the ciphertext is called **decryption**.
- Encryption and decryption usually make use of a **key**, and the coding method is such that decryption can be performed only by knowing the proper key.

Cryptography is Mathematical

- Encryption $C = E_K(P)$
- Decryption $P = E_K^{-1}(C)$
- E_K is chosen from a family of transformations known as a cryptographic system.
- The parameter that selects the individual transformation is called the key K, selected from a keyspace *K*

Cryptography is Mathematical

- A cryptographic system is a single parameter family of invertible transformations
  - E_K ; K in K : P $\rightarrow$ C
  - with the inverse algorithm E_K^{-1} ; K in *K* : C $\rightarrow$ P
  - such that the inverse is unique
- Usually we assume the cryptographic system is public, and only the key is secret information

Encryption is a form of Coding

- **Code -** an method for transforming an intelligible message into an unintelligible one using a code-book.
- A code is a pre-arranged word, sentence, or paragraph replacement system. Foreign languages are just like secret code, where the English word "hi" is represented as the word “Hola” in Spanish, or some other word in another language.
- Most codes have a code book for encoding and decoding.
- An important difference between coding and encryption?

Cryptanalaysis

- The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key is called **Cryptanalysis.**
- Also called “code breaking” sometimes.
- Whereas people who do cryptography are cryptographers, and practitioners of cryptanalysis are **cryptanalysts.**

Cryptology

- Cryptology is the branch of mathematics that studies the mathematical foundations of cryptographic methods.
- Cryptology comes from the Greek words Kryptos, meaning hidden, and Graphen, meaning to write. Cryptology is actually the study of codes and ciphers.
- Cryptology = both cryptography and cryptanalysis

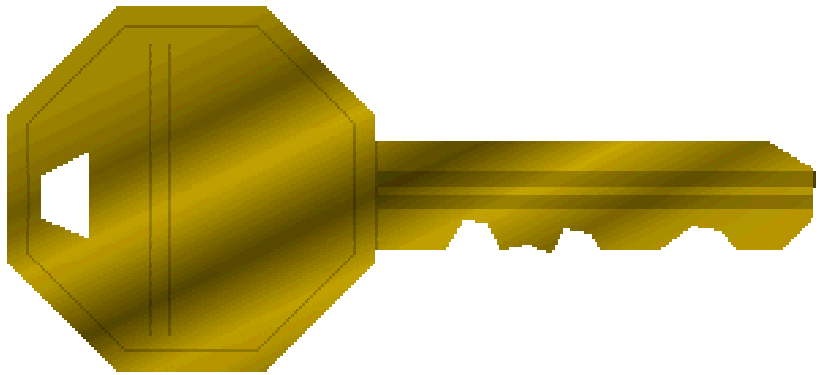
Algorithm Secrecy

- Some cryptographic methods rely on the secrecy of the algorithms; such algorithms are only of historical interest and are not adequate for real-world needs.
- **Kerchoff's Principle:** If the strength of your new cryptosystems relies on the fact that the attacker does not know the algorithm's inner workings,you are sunk.

Security through Obscurity Does Not Work !!!

The Key

- All modern algorithms use a key to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.
- The key used for decryption can be different from the encryption key, but for most algorithms they are the same.



Encryption Algorithm Types

- There are two classes of key-based algorithms:
  - **Symmetric (or secret-key)**
  - **Asymmetric (or public-key) algorithms**
- The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

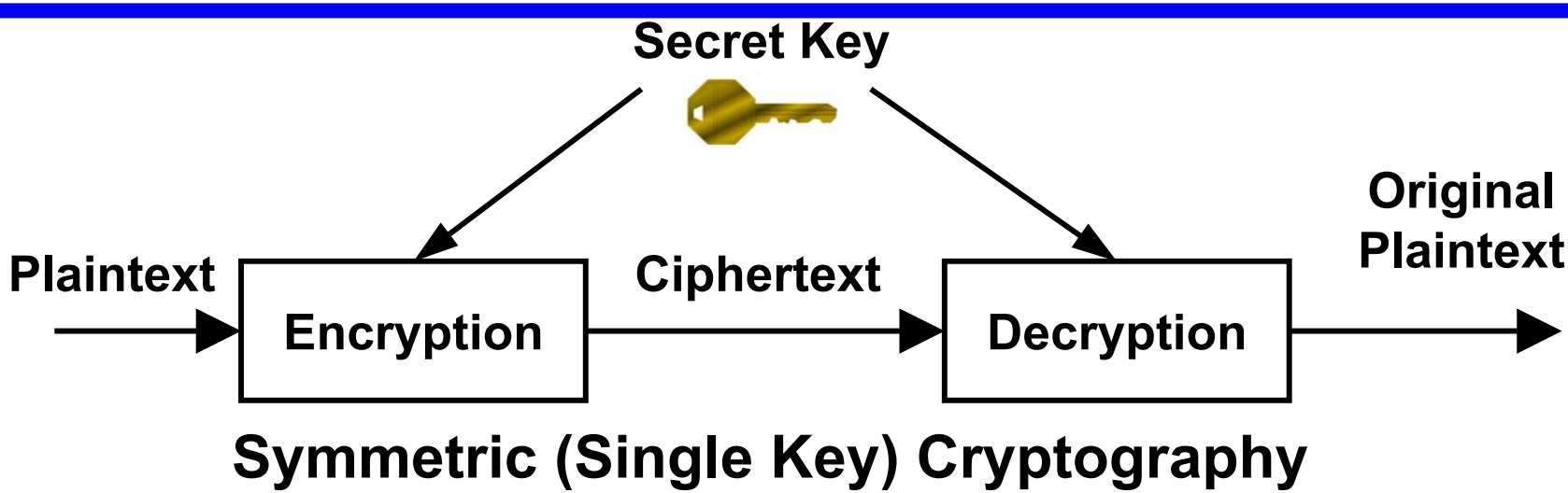
Symmetric Algorithms

- Symmetric algorithms can be divided into two categories: (1) stream ciphers and (2) block ciphers.
- **Stream ciphers** can encrypt a single bit/byte of plaintext at a time, whereas …
- **Block ciphers** take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

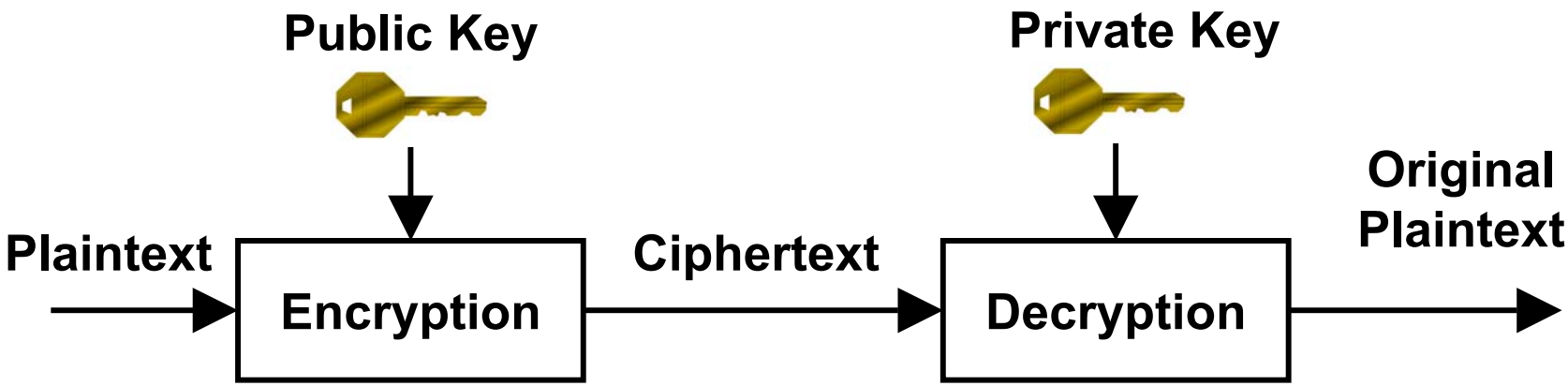
Asymmetric Algorithms

- Asymmetric ciphers (also called public-key algorithms or generally public-key cryptography) permit the encryption key to be public (it can even be published in a newspaper), allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message.
- The encryption key is also called the Public Key and the decryption key the Private Key or Secret Key.

Comparison of Symmetric and Asymmetric Encryption



Symmetric (Single Key) Cryptography



Asymmetric (Two Key) Cryptography

Types of Cryptographic Algorithms

- **Block** – processes information to be encrypted in blocks of 32/84/128 bits
- **Stream** – processes information one bit or one character at a time
- **Symmetric** – uses same key for encryption and decryption
- **Asymmetric** – uses one key for encryption and another totally different key for decryption
- **Secret Key** – usually refers to single key algorithms where the key must be kept secret
- **Public Key** – refers to asymmetric algorithms where one of the keys is public and does not need to be kept secret

Modes of Use

- What is a mode? A mode combines:
  - Basic Encryption Algorithm
  - Some Feedback
  - Some Simple Operation
- The security is a function of the underlying cipher and not the mode.
- The cipher mode should not compromise the security of the underlying algorithm.
- Benefits of modes: Patterns, Efficiency, Fault Tolerance.
- Examples: ECB, CBC, OFB, CFB, etc.

Crypto Algorithms are Time Consuming

- Modern cryptographic algorithms cannot really be executed by humans.
- Strong cryptographic algorithms are designed to be executed by computers or specialized hardware devices.
- In most applications, cryptography is done in computer software, and numerous cryptographic software packages are available.

Symmetric Algorithms are Faster

- Generally, symmetric algorithms are much faster to execute on a computer than asymmetric ones.
- In practice they are often used together, so that a public-key algorithm is used to encrypt a randomly generated encryption key, and the random key is used to encrypt the actual message using a symmetric algorithm.

Encryption Algorithms vs. Other Encoding Algorithms

- Encryption vs. Error Detection/Correction.
- Encryption vs. Compression.

Cryptography Through History

- Cryptography has a history of at least 4000 years.
- Ancient Egyptians enciphered some of their hieroglyphic writing on monuments.
- Ancient Hebrews enciphered certain words in the scriptures.
- 2000 years ago Julius Caesar used a simple substitution cipher, now known as the Caesar cipher.
- Roger Bacon in the middle ages described several methods in 1200s.

Cryptography Through History

- Geoffrey Chaucer included several ciphers in his works (e.g. Canterbury Tales).
- Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s.
- Blaise de Vigenère published a book on cryptology in 1585, & described the polyalphabetic substitution cipher.
- Increasing use, especially in diplomacy & war over centuries.

Muslim Contributions To Cryptography

- Ground breaking research by Dr. Ibrahim A. Al-Kadi, Associate Professor, Electrical Engineering Department, College of Engineering, King Saud University, SA.
- Old manuscripts show that the origin of cryptology, and the Arab contributions to it, are older and more extensive than previously thought.
- The word ‘cipher’ in European languages comes from the Arabic word sifr.

Muslim Cryptographers

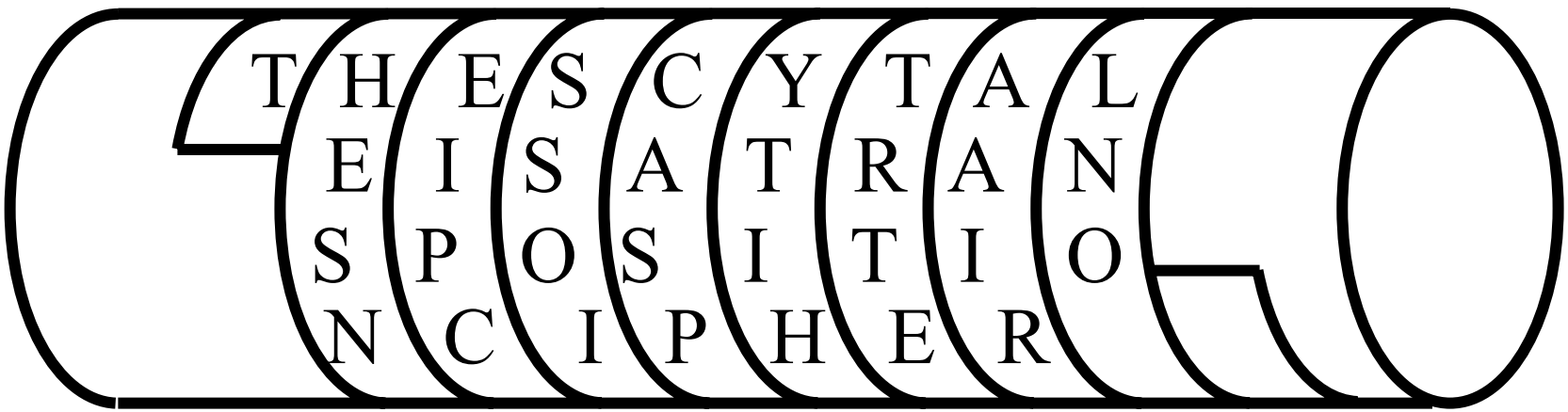
- Al-Kindi
- Ibn Adlaan
- Ibn Duraihim

History - Scytale Cipher

- The Spartans enciphered and concealed a message by using a scytale, a special stick and belt.
- The encipherer would wrap the belt around the stick and write a message on it.
- The belt was then unwound from the stick and sent to another person.
- Using a stick of similar size, the decipherer would wrap the belt around the stick to watch the secret message appear.
- If a stick of the wrong size appeared the message would be scrambled.
- Try this with 2 or 3 pencils bound together to make a stick, a long strip of paper, and another pencil for writing.

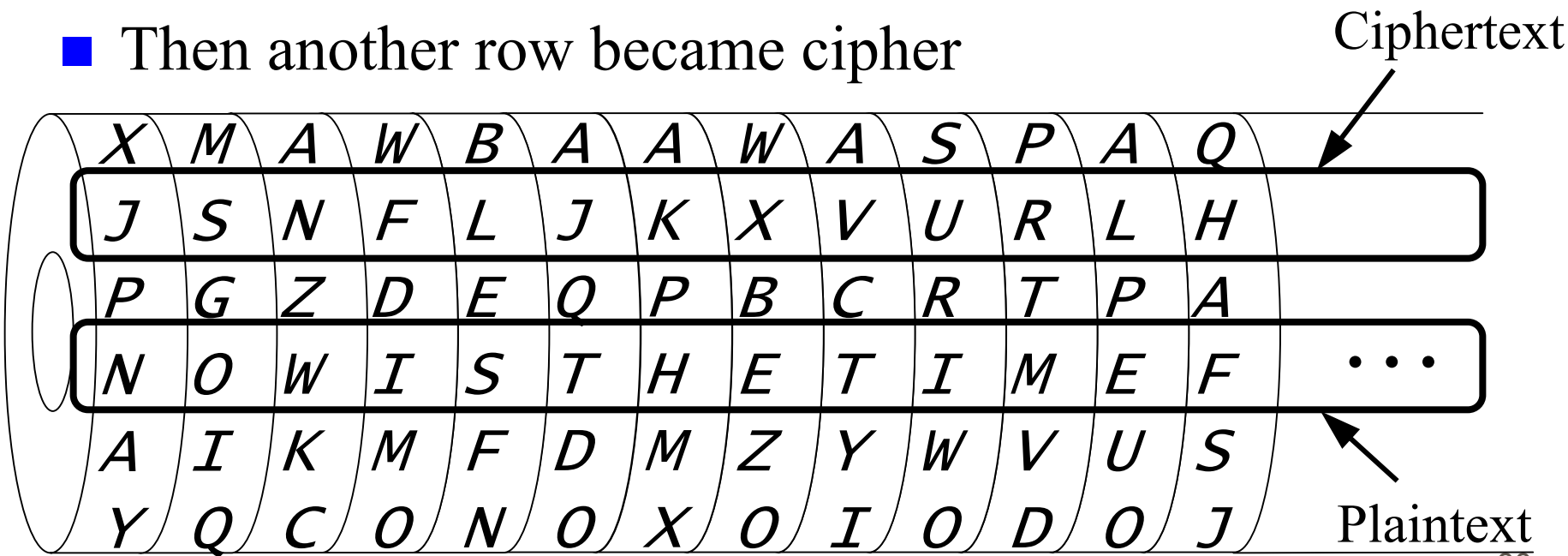
History - Scytale Cipher

- An early Greek transposition cipher a strip of paper was wound round a staff message written along staff in rows, then paper removed leaving a strip of seemingly random letters
- Not very secure as key was width of paper & staff



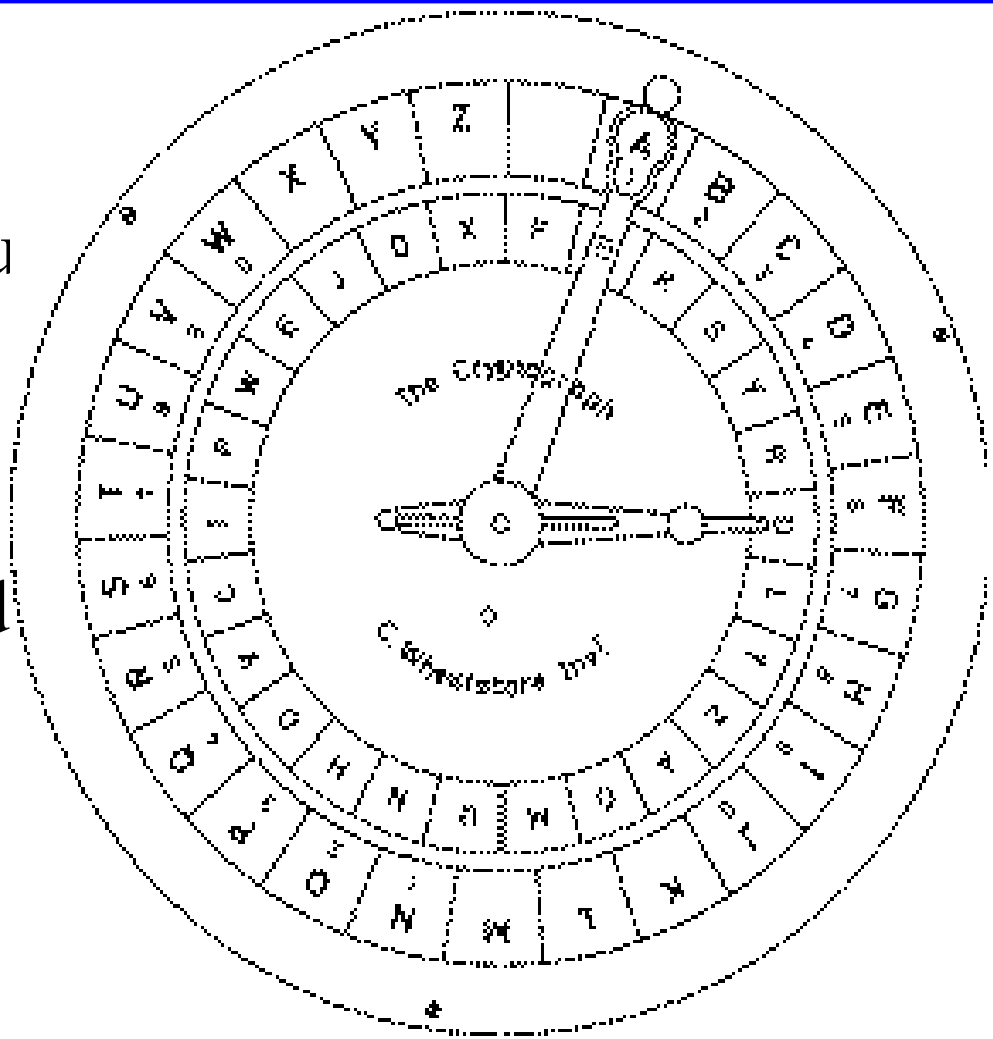
Machine Ciphers

- Jefferson cylinder, developed in 1790s, comprised 36 disks, each with a random alphabet
- Order of disks was key
- Message was set
- Then another row became cipher



Machine Ciphers

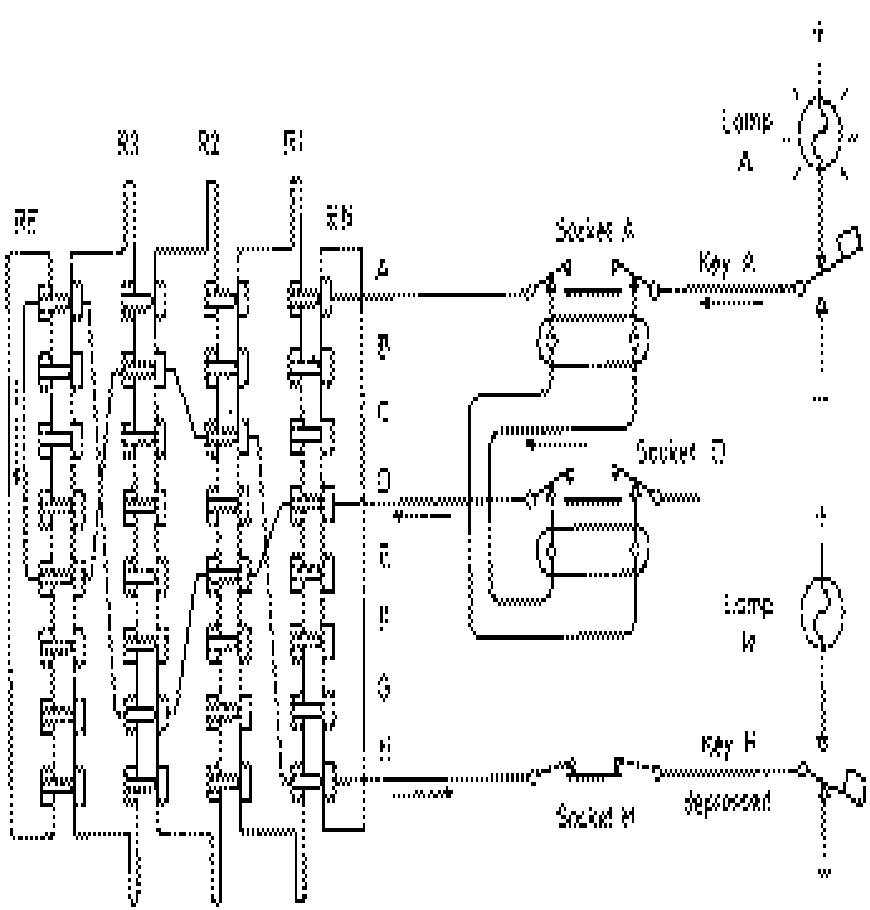
- Wheatstone disc, originally invented by Wadsworth in 1817, bu developed by Wheatstone in 1860's, comprised two concentric wheels used to generate a polyalphabetic cipher

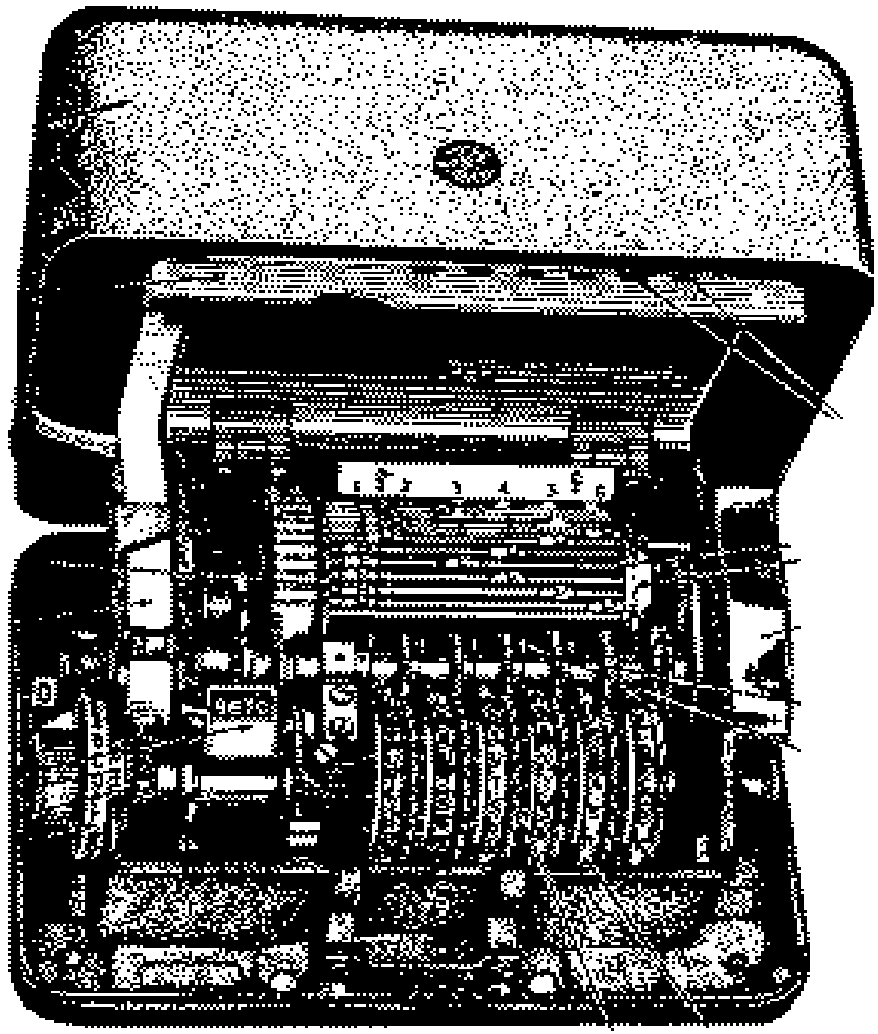


Enigma

- Enigma Rotor machine, one of a very important class of cipher machines, heavily used during 2nd world war.
- Comprised a series of rotor wheels with internal cross-connections, providing a substitution using a continuously changing alphabet.

Figure - Enigma





History - Caesar Cipher

- Julius Caesar used a simple alphabet (letter) substitution, offset by 3 letters.
- Taking the word “cipher" you would move ahead in the alphabet 3 letters to get “FLSKHU”.
  - c = 3 → 3+3 = 6 → F
  - i = 9 → 9+3 = 12 → L
  - p = 16 → 16+3 = 19 → S
  - h = 8 → 8+3 = 11 → K
  - e = 5 → 5+3 = 8 → H
  - r = 18 → 18+3 = 21 → U
- This worked for a while, until more people learned to read and studied his secret cipher.

History - Manual on Cryptology

- Gabriel de Lavinde made cryptology a more formally understood science when he published his first **Manual on Cryptology** in 1379.
- A variety of codes and mechanical devices were developed over the next few centuries to encode, decode, encipher, and decipher messages.

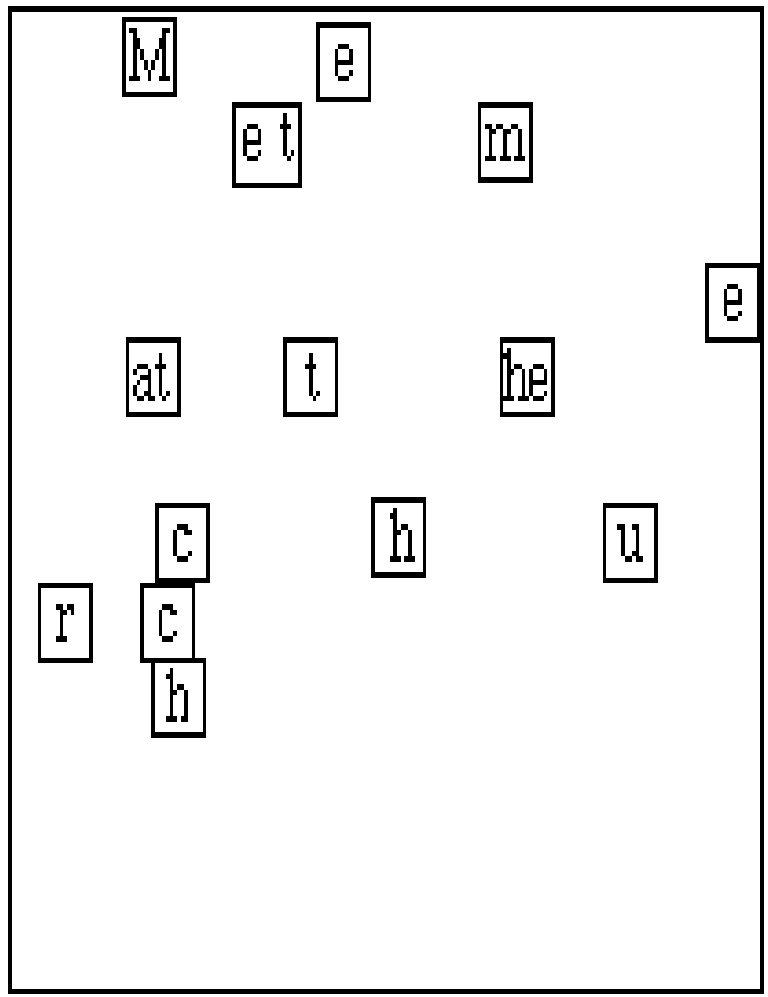
History - The Grille

- In the 1600's Cardinal Richelieu invented the grille.
- He created a card with holes in it and used it to write a secret message.
- When he was done he removed the card and wrote a letter to fill in the blanks and make the message look like a normal letter.
- The grille proved to be difficult to solve unless the decoder had the card which created the encrypted message.

History - The Grille

Dear Mr. S. Pye,
I would like to extend my thanks
to you and your company for your
gracious donation to our charitable
foundation last year. The monies
from your donation have been
used to create a scholarship fund
for special needs and outstand
citizenship students in our district

With Thanks,
Mr. Dunham



History - The Rosetta Stone

- The Rosetta Stone (black basalt), found in Egypt in 1799, had a message encrypted on its surface in three different languages! Greek, Egyptian, and Hieroglyphics messages all said the same thing.
- Once the Greek and Egyptian languages were found to have the same message the Hieroglyphics language was deciphered by referencing each letter to a symbol!

History - Morse Code

- Morse Code, developed by Samuel Morse in 1832, is not really a code at all.
- It is a way of enciphering (cipher) letters of the alphabet into long and short sounds.
- The invention of the telegraph, along with Morse code, helped people to communicate over long distances.
- Morse code can be used in any language and takes only 1 to 10 hours of instruction/practice to learn!
- The first Morse code sent by telegraph was “What hath God wrought?”, in 1844.

Morse Code

Letter	Sound
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	––··

History

- The little known native Indian language of the Navajo was used by the US in WWII as a simple word substitution code.
- There were 65 letters and numbers that were used to encipher a single word prior to the use of the Navajo language.
- The Navajo language was much faster and accurate compared to earlier ciphers and was heavily used in the battle of Iwo-jima.

History

- The Germans, responsible for much of the cipher science today, developed complex ciphers near the end of WWII.
- They enciphered messages and sent them at high rates of speed across radio wave bands in Morse code.
- To the unexpecting it sounded like static in the background.
- One gentleman tried to better understand the static and listened to it over and over again.
- The last time he played his recording he forgot to wind his phonograph.
- The static played at a very slow speed and was soon recognized as a pattern, Morse code!

History

- The Germans in WWII used codes but also employed other types of secret writings.
- One suspected spy was found to have large numbers of keys in his motel room.
- After inspecting the keys it was found that some of the keys were modified to unscrew at the top to show a plastic nib.
- The keys contained special chemicals for invisible ink!
- However, codes and secret ink messages were very easily captured and decoded.

Concealment Messages

- Some of the more fun secret writings are concealment messages like invisible inks made out of potato juice, lemon juice, and other types of juices and sugars!
- Deciphering and decoding messages take a lot of time and be very frustrating. But with experience, strategies, and most of all, luck, you'll be able to crack lots of codes and ciphers.

Cryptography vs. Steganography

- What is steganography?
- In an ideal world we would all be able to openly send encrypted email or files to each other with no fear of reprisals. However there are often cases when this is not possible, either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography can come into play.

Cryptography vs. Steganography

- Steganography simply takes one piece of information and hides it within another.
- Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them.
- An image of the space shuttle landing might contain a private letter to a friend.
- A recording of a short sentence might contain your company's plans for a secret new product.
- Steganography can also be used to place a hidden “trademark” in images, music, and software, a technique referred to as watermarking.

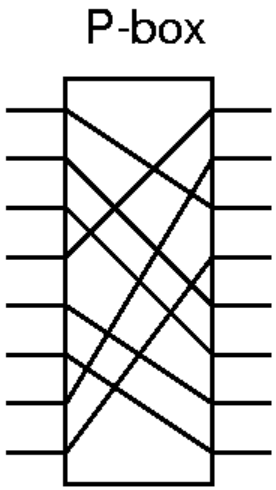
To Learn More About Steganography

- http://members.tripod.com/steganography/stego/info.htm

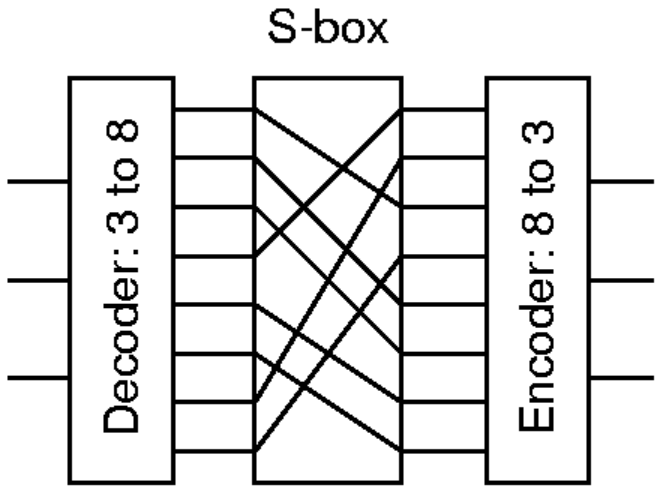
Classical Cryptographic Techniques

- Three Eras of Cryptography:
  - Classical
  - Traditional
  - Modern
- We have two basic components of classical ciphers: substitution and transposition.
- **Substitution:** In substitution ciphers letters are replaced by other letters.
- **Transposition:** In transposition ciphers the letters are arranged in a different order.

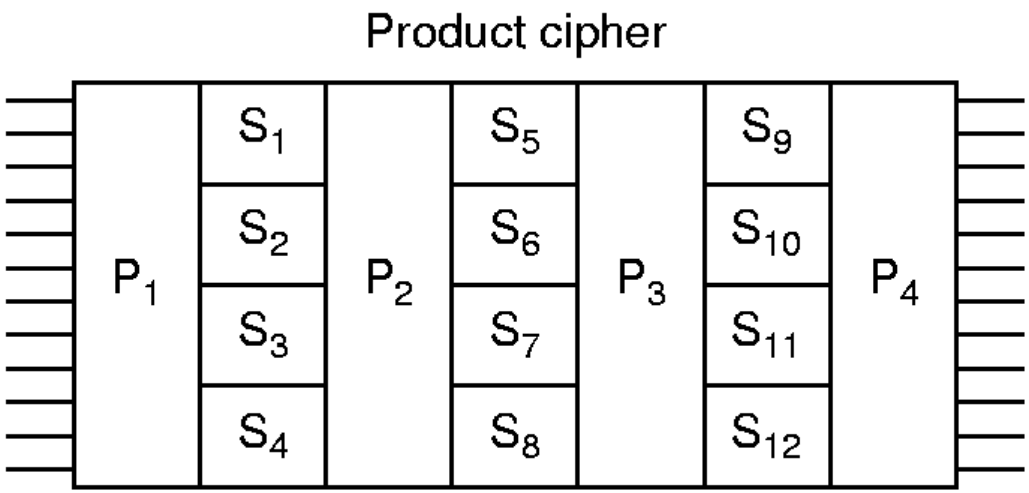
Substitution and Transposition



(a)



(b)



(c)

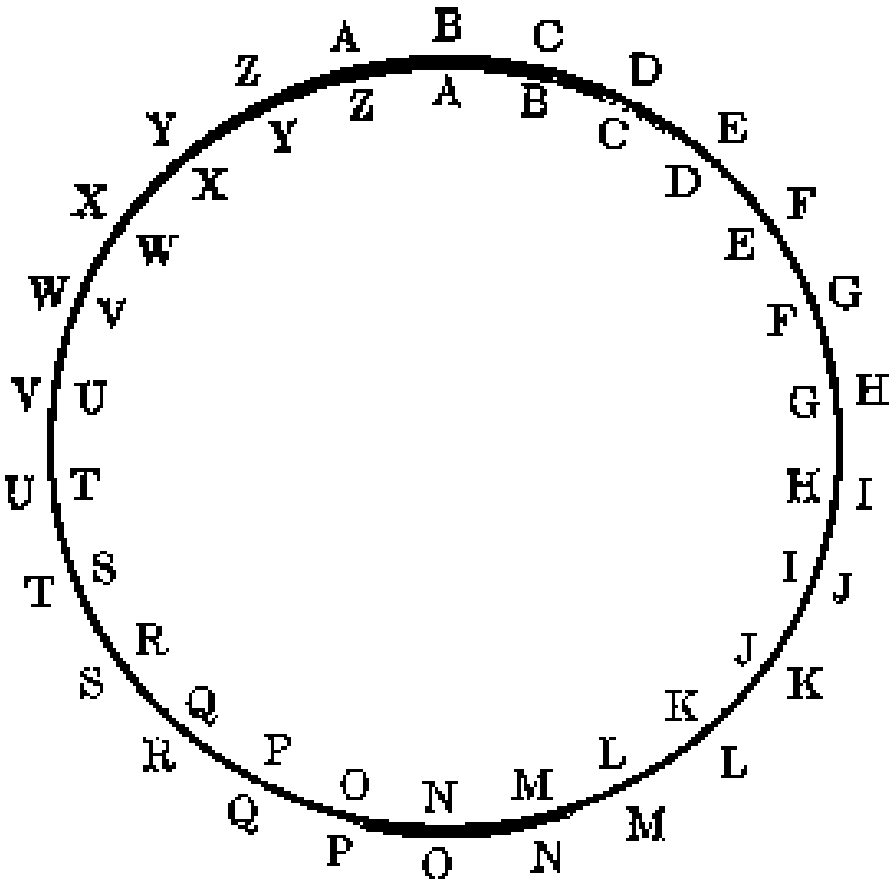
Monoalphabetic and Polyalphabetic Ciphers

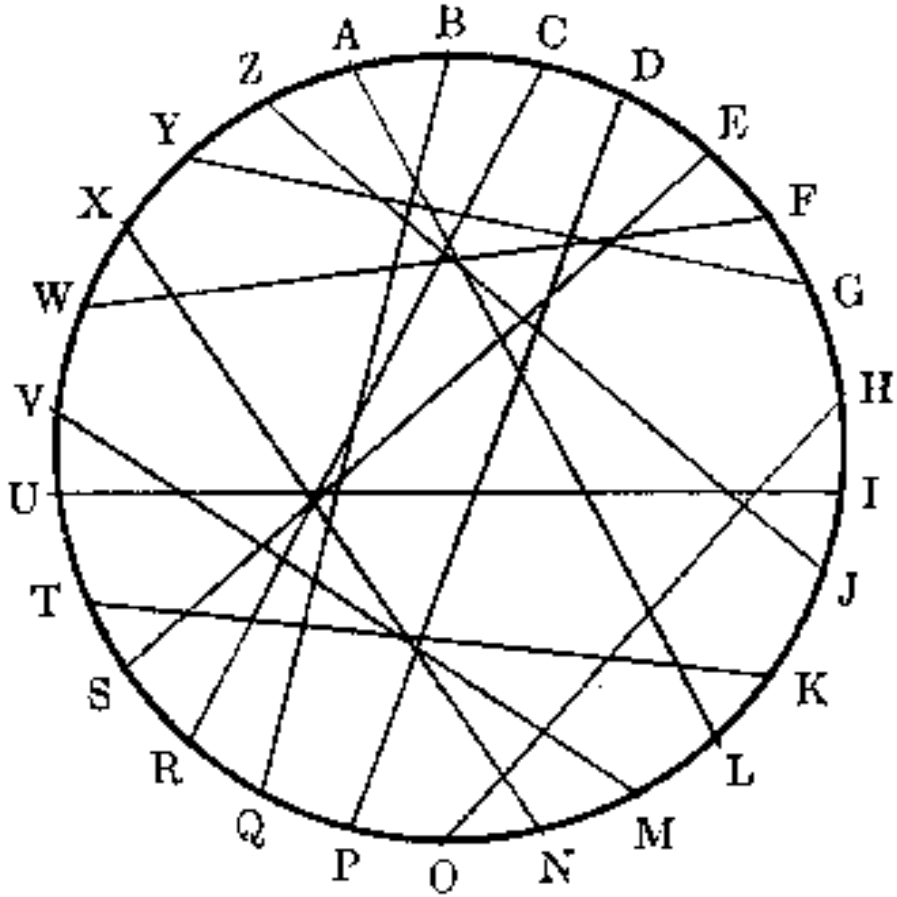
- **Monoalphabetic -** only one substitution/ transposition is used.
- **Polyalphabetic -** where several substitutions/ transpositions are used.
- Several such ciphers may be concatenated together to form a **Product Cipher.**

Caesar Cipher - A Monoalphabetic Substitution Cipher

- Replace each letter of message by a letter a fixed distance away e.g. use the 3rd letter on
- Reputedly used by Julius Caesar, e.g.
  - L FDPH L VDZ L FRQTXHUHG
  - I CAME I SAW I CONQUERED
- i.e. mapping is
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - DEFGHIJKLMNOPQRSTUVWXYZABC
- Can describe this cipher as:
  - Encryption $E_k : i \rightarrow i + k \bmod 26$
  - Decryption $D_k : i \rightarrow i - k \bmod 26$

Caesar Cipher Key

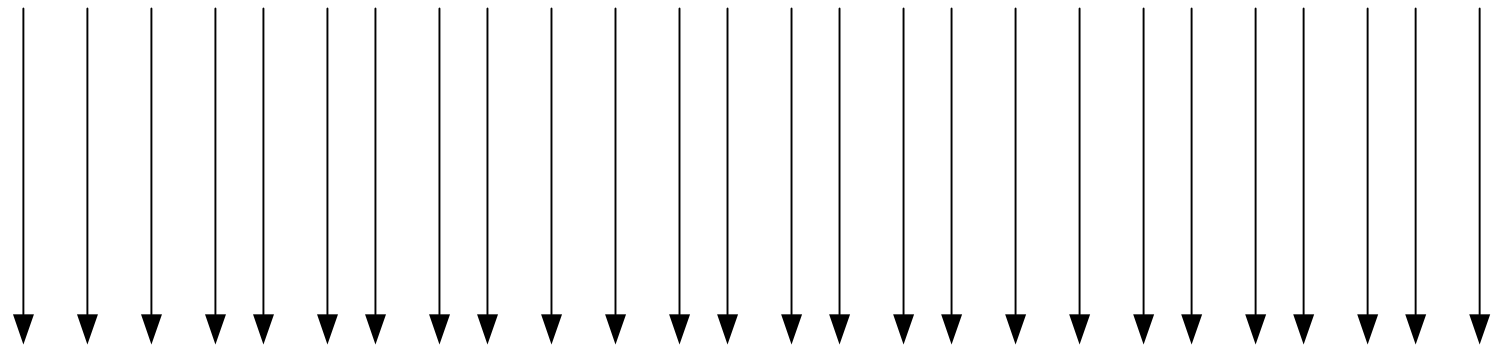




A Simple Substitution Cipher

Plaintext:

abcdefghijklmnopqrstuvwxyz



QIAYMWFUBKPDGJZSOCVLXNETRH

Ciphertext:

Frequency-based Cryptanalytic Attacks

- Cryptanalyst knows the letter-frequency distribution of the language.
- Cryptanalyst constructs the letter frequency table of the cipher-text.
- Cryptanalyst tries to find letter pairs with the same frequency distribution in the plain text and cipher text.
- Also uses the frequencies of di-grams and tri-grams.
- Finally a little bit of trial and error.

Frequency Distribution of Letters in Standard English

A	8.167	J	0.153	S	6.327
B	1.492	K	0.772	T	9.056
C	2.782	L	4.025	U	2.758
D	4.253	M	2.406	V	0.978
E	12.702	N	6.749	W	2.360
F	2.228	O	7.507	X	0.150
G	2.015	P	1.929	Y	1.974
H	6.094	Q	0.095	Z	0.074
I	6.966	R	5.987		

Polyalphabetic Substitution Cipher

- **Polyalphabetic** Substitution - several substitutions are used.
- Used to hide the statistics of the plain-text.

Polyalphabetic Substitution Example

Suppose that a polyalphabetic cipher of period 3 is being used, with the three monoalphabetic ciphers M1, M2, M3 as defined below. To encrypt a message, the first 3 letters of the plaintext are enciphered according to ciphers M1, M2, M3 respectively, with the process being repeated for each subsequent block of 3 plaintext letters.

	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
M1:	K	D	N	H	P	A	W	X	C	Z	I	M	Q	J	B	Y	E	T	U	G	V	R	F	O	S	L
M2:	P	A	G	U	K	H	J	B	Y	D	S	O	E	M	Q	N	W	F	Z	I	T	C	V	L	X	R
M3:	J	M	F	Z	R	N	L	D	O	W	G	I	A	K	E	S	U	C	Q	V	H	Y	X	T	P	B

Plaintext

now is the time for every good man

Ciphertext

JCQ CZ VXK VCER AQC PCRTX LBQZ QPK

Note:

The two o's in good have been enciphered as different letters. Also the three letters "X" in the ciphertext represent different letters in the plaintext.

Transposition Ciphers

- Transposition or permutation ciphers hide the message contents by rearranging the order of the letters.
- Scytale Cipher is an example of a transposition cipher.
- How does a cryptanalyst know that a transposition cipher has been used?
- Single transposition vs. double transposition

Transposition Cipher Example (1)

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

← Weights to be used for double transposition

Plaintext

pleasetransferonemilliondollarstomyswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANTESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Transposition Cipher Example (2)

Key → S H O E S

Weights to be used for double transposition → 1 3 5 4 2

Plaintext

paymebysundayorsufferthecons
equences

Ciphertext

PBDSROUSENRECQEZAYAUT
NEZMUOFEECZYSYFHSNZ

p	a	y	m	e
b	y	s	u	n
d	a	y	o	r
s	u	f	f	e
r	t	h	e	c
o	n	s	e	q
u	e	n	c	e
s	z	z	z	z

Types of Encryption Systems

- There are two types of encryption algorithms:
  - Symmetric or Private Key systems
  - Asymmetric or Public Key systems

Symmetric or Private Key Systems

- A Private-Key (or secret-key, or single-key) encryption algorithm is one where the sender and the recipient share a common, or closely related, key.
- "Symmetric" means it uses the same key for encryption as for decryption. As with all symmetric ciphers, the sender must transmit the key to the recipient via some secure and tamperproof channel, otherwise the recipient won't be able to decrypt the ciphertext.
- All traditional encryption algorithms are private-key.

One Time Pad - OTP

- A one-time pad is a very simple yet completely unbreakable symmetric cipher.
- A one-time pad involves sheets of paper with random numbers on them: These numbers are used to transform the message; each number or sequence of numbers is used only once.
- The recipient of the message has an identical pad to use to decrypt the message. One-time pads have been proven to be foolproof-without having a copy of the pad.
- Supposedly, mathematicians can prove that a one-time pad is impossible to break.

What is a One-Time Pad?

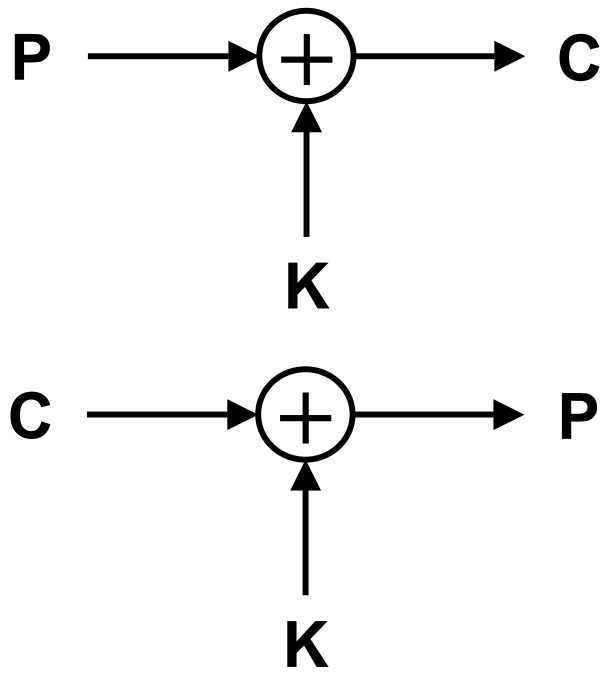
- The key for a one-time pad cipher is a string of random bits, usually generated by a cryptographically strong pseudo-random number generator (CSPRNG).
- It is better to generate the key using the natural randomness of quantum mechanical events (such as those detected by a Geiger counter), since quantum events are believed by many to be the only source of truly random information in the universe.
- One-time pads that use CSPRNGs are open to attacks which attempt to compute part or all of the key.

What is a One-Time Pad?

- With a one-time pad, there are as many bits in the key as in the plaintext.
- This is the primary drawback of a one-time pad, but it is also the source of its perfect security.
- It is essential that no portion of the key ever be reused for another encryption (hence the name "one-time pad"), otherwise cryptanalysis can break the cipher.

One Time Pad Algorithm

- The cipher itself is exceedingly simple. To encrypt plaintext, P, with a key, K, producing ciphertext, C, simply compute the bitwise exclusive-or of the key and the plaintext:
  - C = K *XOR* P
- To decrypt ciphertext, C, the recipient computes
  - P = K *XOR* C
- It's that simple, and it's perfectly secure, as long as the key is random and is not compromised.



Why are One-Time Pads Perfectly Secure?

- If the key is truly random, an xor-based one-time pad is perfectly secure against ciphertext-only cryptanalysis.
- This means an attacker can't compute the plaintext from the ciphertext without knowledge of the key, even via a brute force search of the space of all keys!
- Trying all possible keys doesn't help you at all, because all possible plaintexts are equally likely decryptions of the ciphertext.

Why are One-Time Pads Perfectly Secure?

- This result is true regardless of how few bits the key has or how much you know about the structure of the plaintext.
- To see this, suppose you intercept a very small, 8-bit, ciphertext. You know it is either the ASCII character 'S' or the ASCII character 'A' encrypted with a one-time pad. You also know that if it's 'S', the enemy will attack by sea, and if it's 'A', the enemy will attack by air. That's a lot to know. All you are missing is the key, a silly little 8-bit one-time pad.

Why are One-Time Pads Perfectly Secure?

- You assign your crack staff of cryptanalysts to try all 256 8-bit one-time pads. This is a brute force search of the keyspace.
- The results of the brute force search of the keyspace is that your staff finds one 8-bit key that decrypts the ciphertext to 'S' and one that decrypts it to 'A'. And you still don't know which one is the actual plaintext.
- This argument is easily generalized to keys (and plaintexts) of arbitrary length.

Cryptography Meets Computers

- The invention of computers in the 20th century revolutionized cryptology.
- IBM corporation created a code, Data Encryption Standard (DES), that has not been broken to this day.
- Thousands of complex codes and ciphers have been programmed into computers so that computers can algorithmically unscramble secret messages and encrypted files.

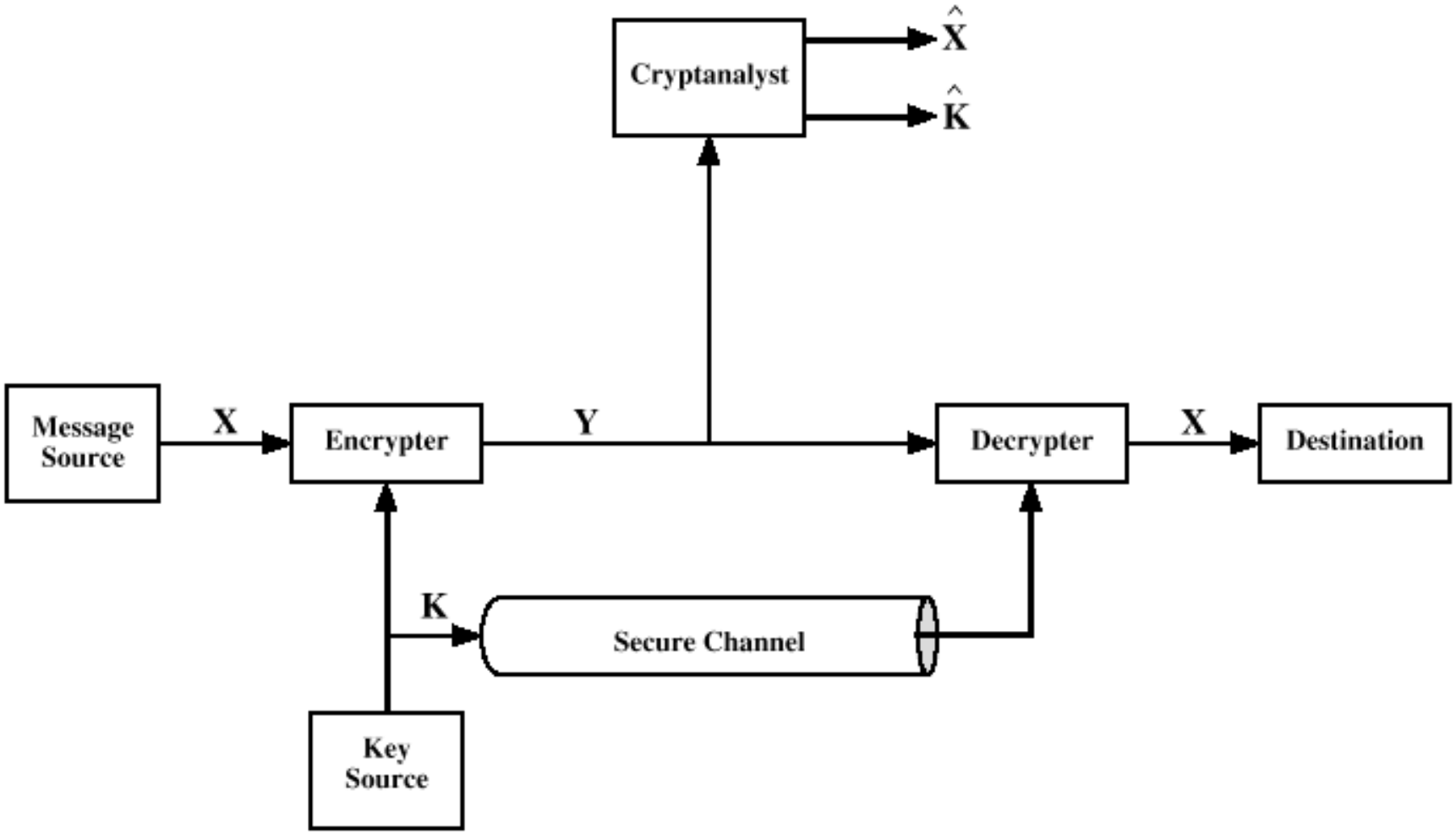
Example Symmetric Encryption Algorithm - DES

- The most well known symmetric system is the Data Encryption Standard (DES).
- Data Encrypt Standard (DES) is a private key system adopted by the U.S. government as a standard “very secure” method of encryption.

Private Key Problems

- Keys must be exchanged before transmission with any recipient or potential recipient of your message.
- So, to exchange keys you need a secure method of transmission, but essentially what you've done is create a need for another secure method of transmission.
- Secondly the parties are not protected against each other, if one of the parties leaks the keys it could easily blame the other party for the compromise.

Private Key Encryption



Public Key Encryption

- To overcome the drawbacks of private key systems, a number of mathematicians have invented public key systems.
- Unknown until about 30 years ago, public key systems were developed from some very subtle insights about the mathematics of large numbers and how they relate to the power of computers.

Public Key Encryption

- Public key means that anyone can publish his or her method of encryption, publish a key for his or her messages, and only the recipient can read the messages.
- This works because of what is known in math as a trapdoor problem.

Trapdoor Problem

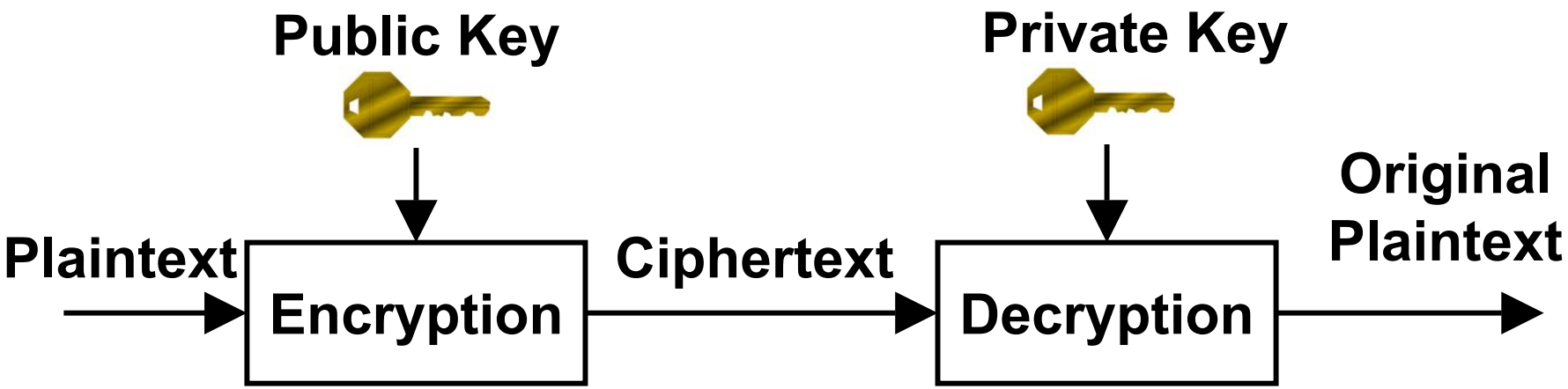
- A trapdoor is a mathematical formula that is easy to work forward but very hard to work backward. In general it is easy to multiply two very large numbers together, but it is very difficult to take a very large number and find its two prime factors. Public key algorithms depend on a person publishing a large public key and others being unable to factor this public key into its component parts. Because the creator of the key knows the factors of his or her large number, he or she can use those factors to decode messages created by others using his or her public key. Those who only know the public key will be unable to discover the private key, because of the difficulty of factoring the large number.

Public Key Encryption Systems

- In public key systems there is a public key, which may be known to many people and a secret key, which is unique and known only to the sender. Because a different key is used on each side of the process, public key systems are also known as 'asymmetric systems'. The distribution of keys for public key systems is generally much easier because it is not normally necessary to keep the public key secret. The private key, on the other hand, must remain secret or else security is compromised.

Public Key Encryption

- Key Pairs (Public and Private).
- Publish one key, keep the other secret.
- Anyone who wants to send you a message encrypts it using your public key.
- To read a message you decrypt it with the private key.



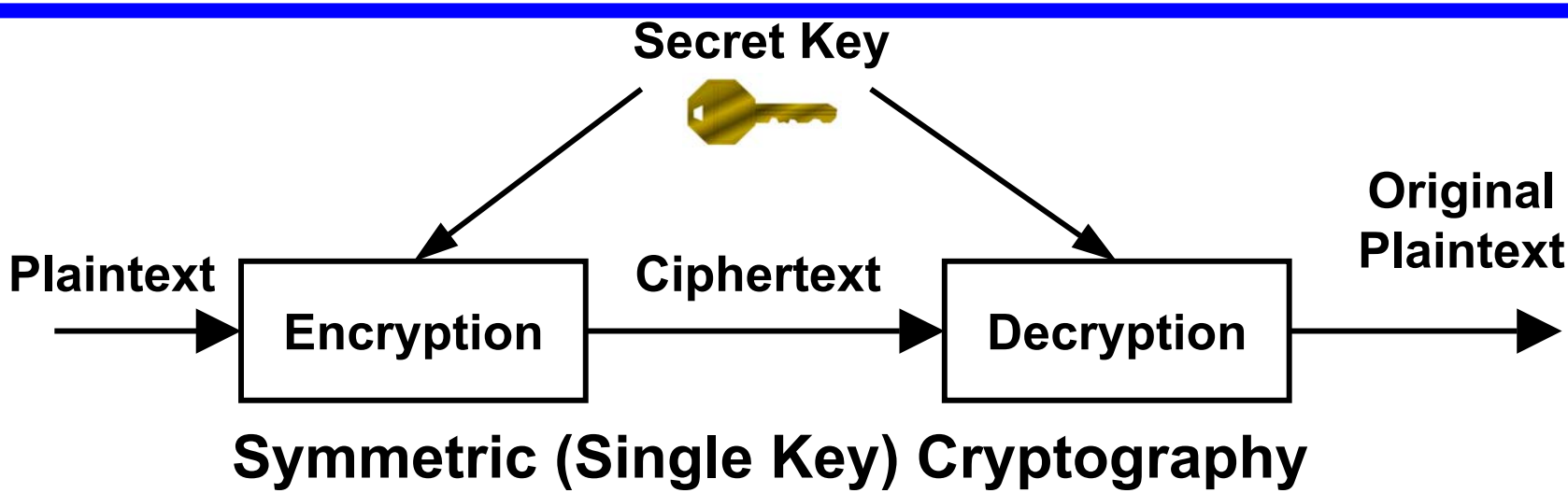
Public Key Encryption

- A good public key algorithm:
  - Infeasible to derive one key from the other
  - Keys are interchangeable
- Simplifies (but does not solve) key distribution problem
- Public key is slower than secret key algorithms
  - RSA is about 1000-5000 times slower than DES
  - Public key encryption is sometimes used to encrypt a secret key algorithm's session key

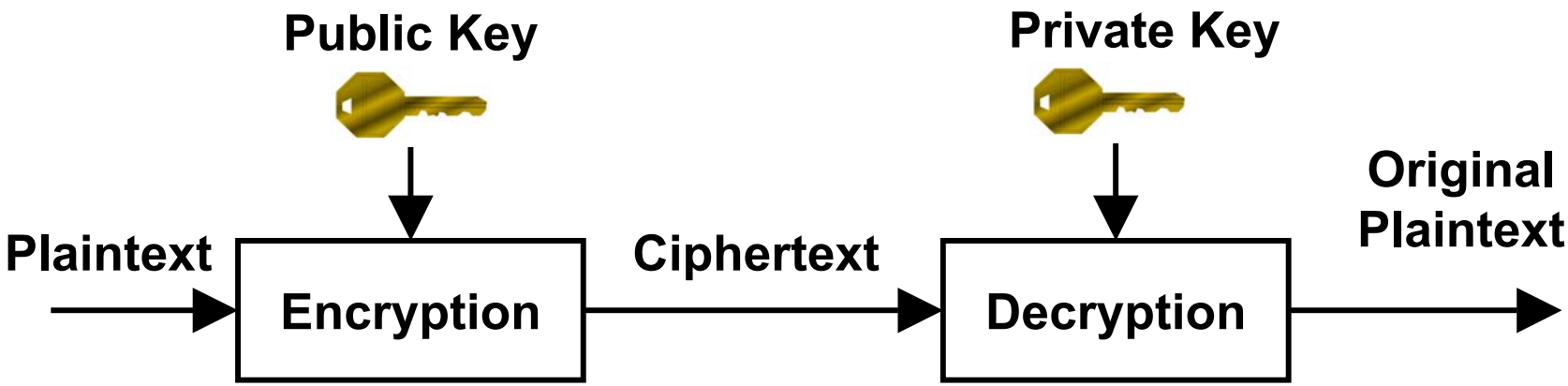
RSA

- The best known public key system is RSA, named after its authors, Rivest, Shamir and Adelman.
- It has recently been brought to light that an RSA-like algorithm was discovered several years before the RSA guys by some official of the British Military Intelligence Cryptography Wing

Comparison of SK and PK Cryptography



Symmetric (Single Key) Cryptography



Asymmetric (Two Key) Cryptography

Comparison of SK and PK Cryptography

DISTINCT FEATURES	SECRET KEY	PUBLIC KEY
NUMBER OF KEYS	Single key.	Pair of keys.
TYPES OF KEYS	Key is secret.	One key is private, and one key is public.
LENGTH OF KEYS	40-200 bits	512-2048 bits
RELATIVE SPEEDS	Faster.	Slower.

Uses of Encryption

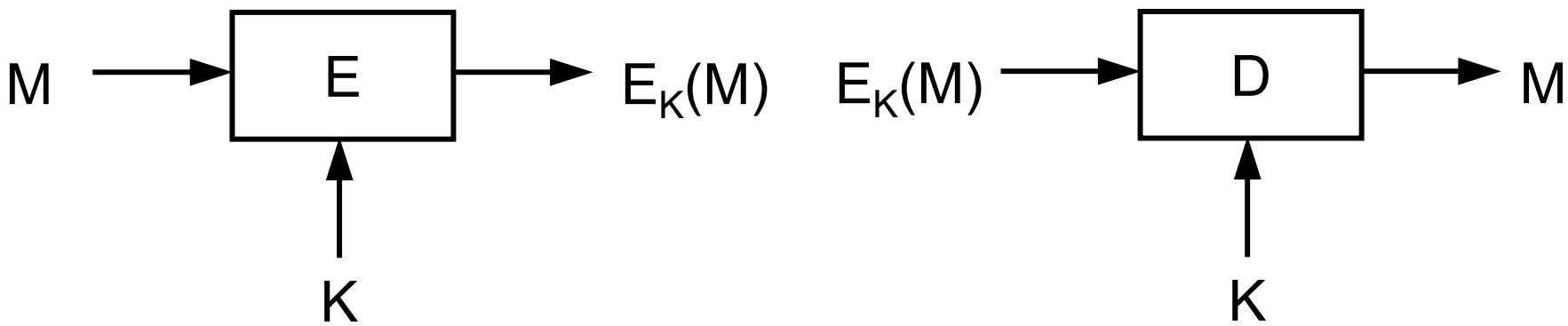
- Protecting data from prying eyes is not the only security issue in networking.
- One can imagine at least four security services:
  - Protecting data from being read by unauthorized persons
  - Verifying the sender of each message (authentication)
  - Preventing unauthorized persons from inserting or deleting messages
  - Making it possible for users to send signed documents electronically
- Encryption can be used to achieve all these goals.

Uses of Encryption

- Encryption may be used for:
  - Confidentiality
  - Error Detection
  - User Authentication
  - Message Authentication
  - Proof of Origin

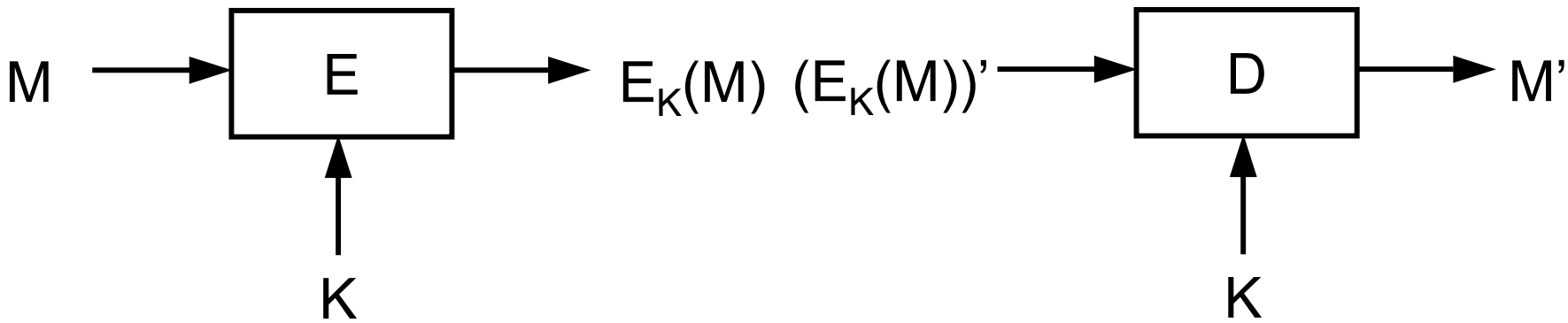
Confidentiality - Secrecy

- Confidentiality - encrypted data cannot normally be understood by anyone other than the sender or the receiver.
- How?



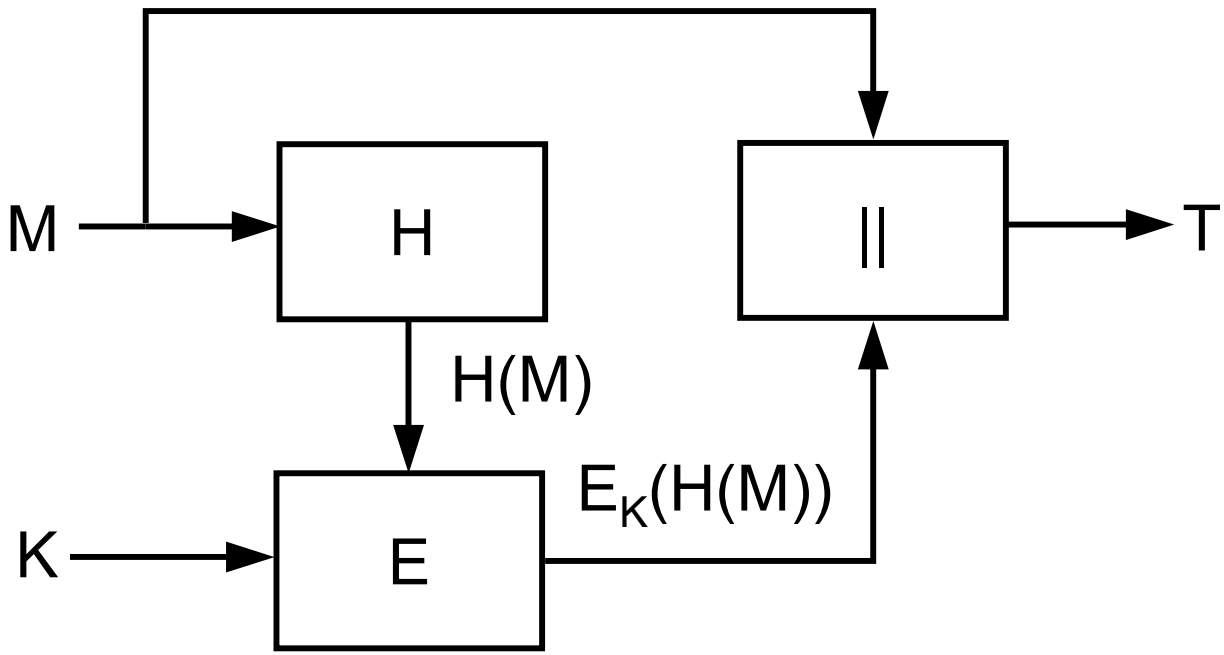
Error Detection

- Error Detection - checking that the contents of a message have not accidentally changed.
- How?



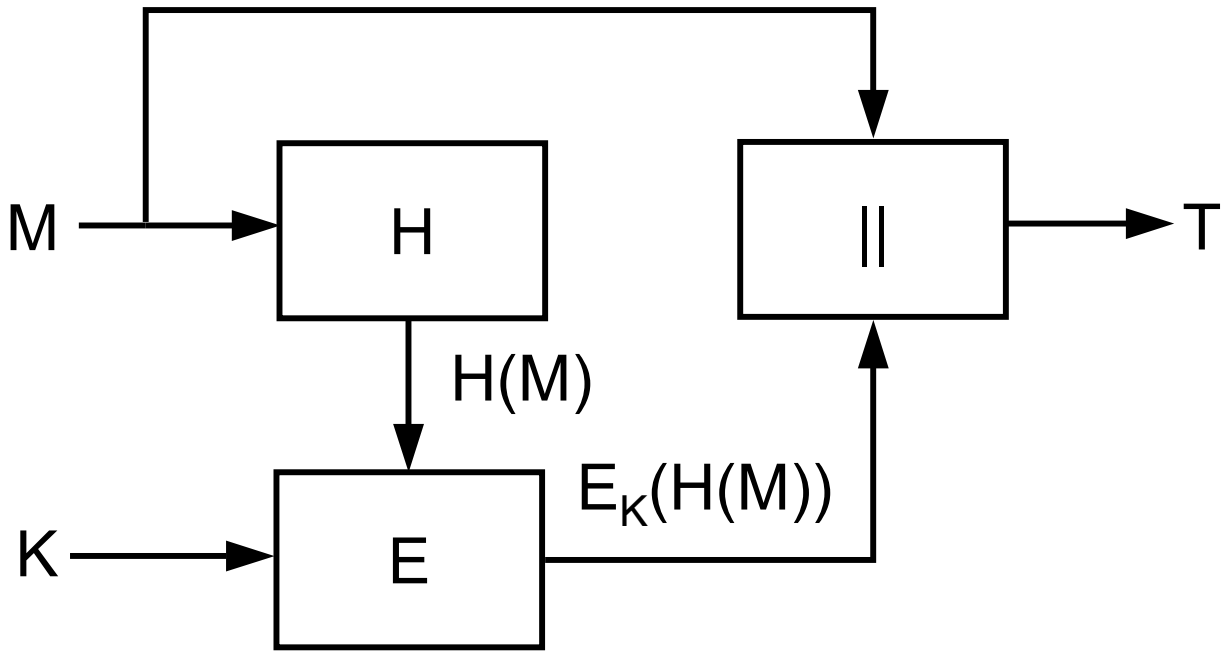
User Authentication

- User authentication - verification by the receiver that the sender is the genuine author and not somebody else.
- How?



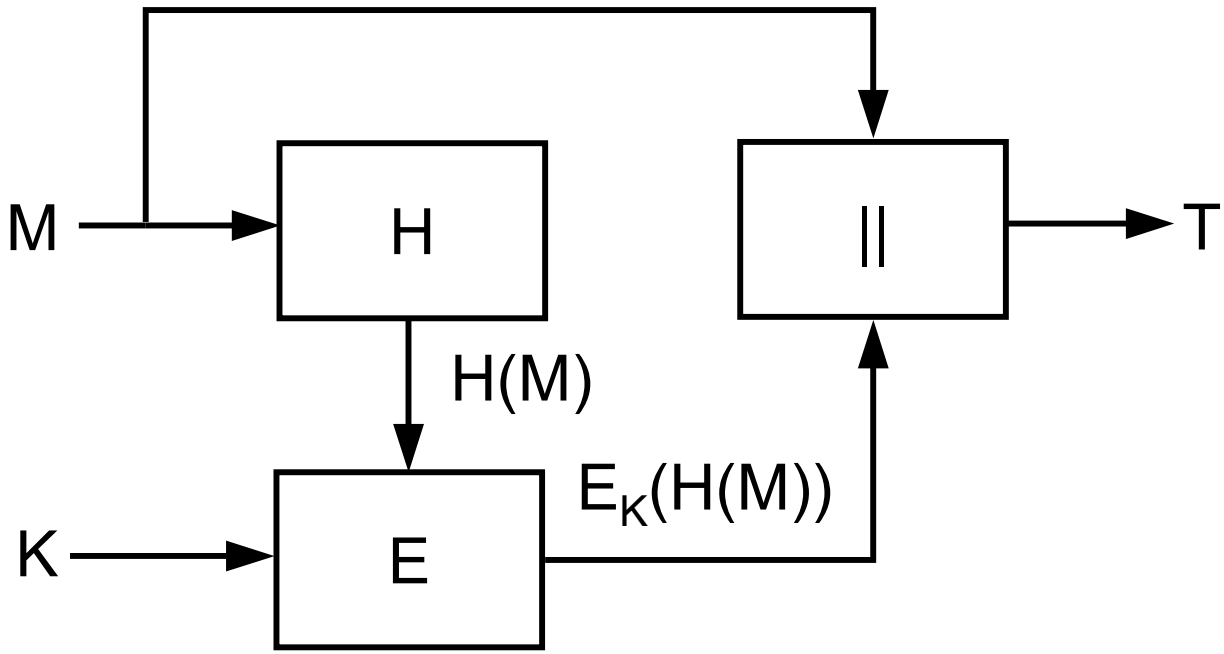
Message Authentication

- Message authentication - verification that messages have not been lost or tampered with.
- How?



Proof of Origin

- Proof or origin - proving to a third party that the message came from the stated sender.
- How?



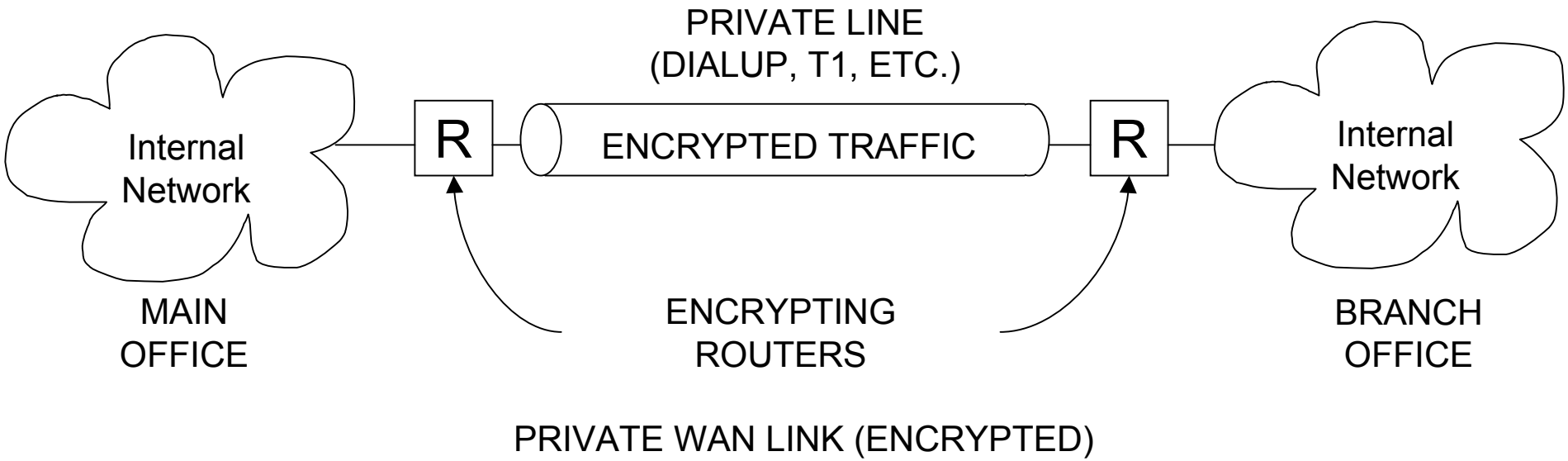
Location of Encryption in OSI Model

- The location of encryption in the OSI model has been so controversial that all mention of the subject was omitted from the initial standard.
- In theory, encryption can be done in any layer, but in practice three layers seem the most suitable: physical, transport, and presentation.

Encryption at the Physical Layer

- When encryption is done on the physical layer, an encryption unit is inserted between each computer and the physical medium.
- Every bit leaving the computer is encrypted and every bit entering a computer is decrypted. This scheme is called link encryption.
- It is simple , but relatively inflexible.
- Examples:
  - PPP-ECP
  - WEP

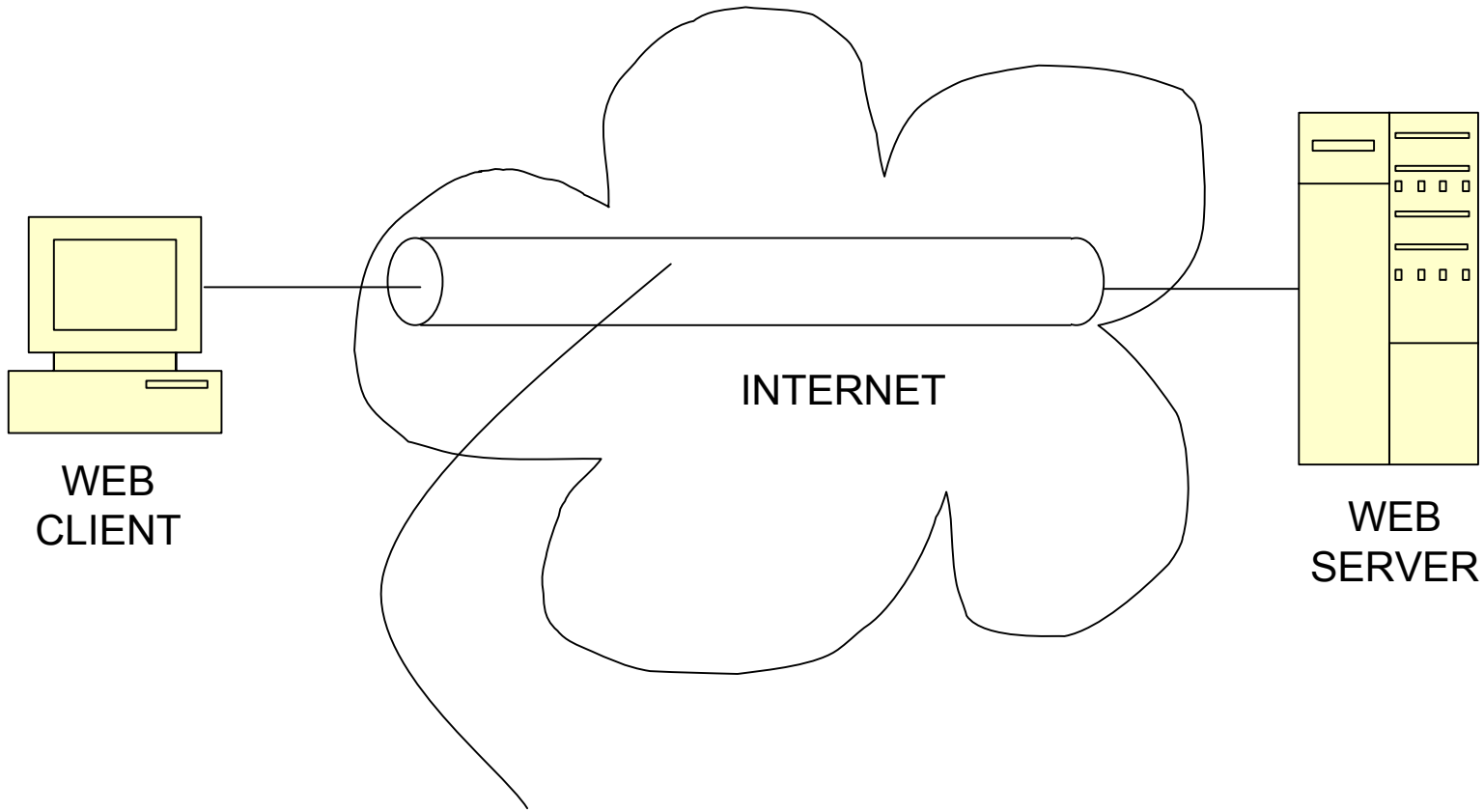
Link Encryption



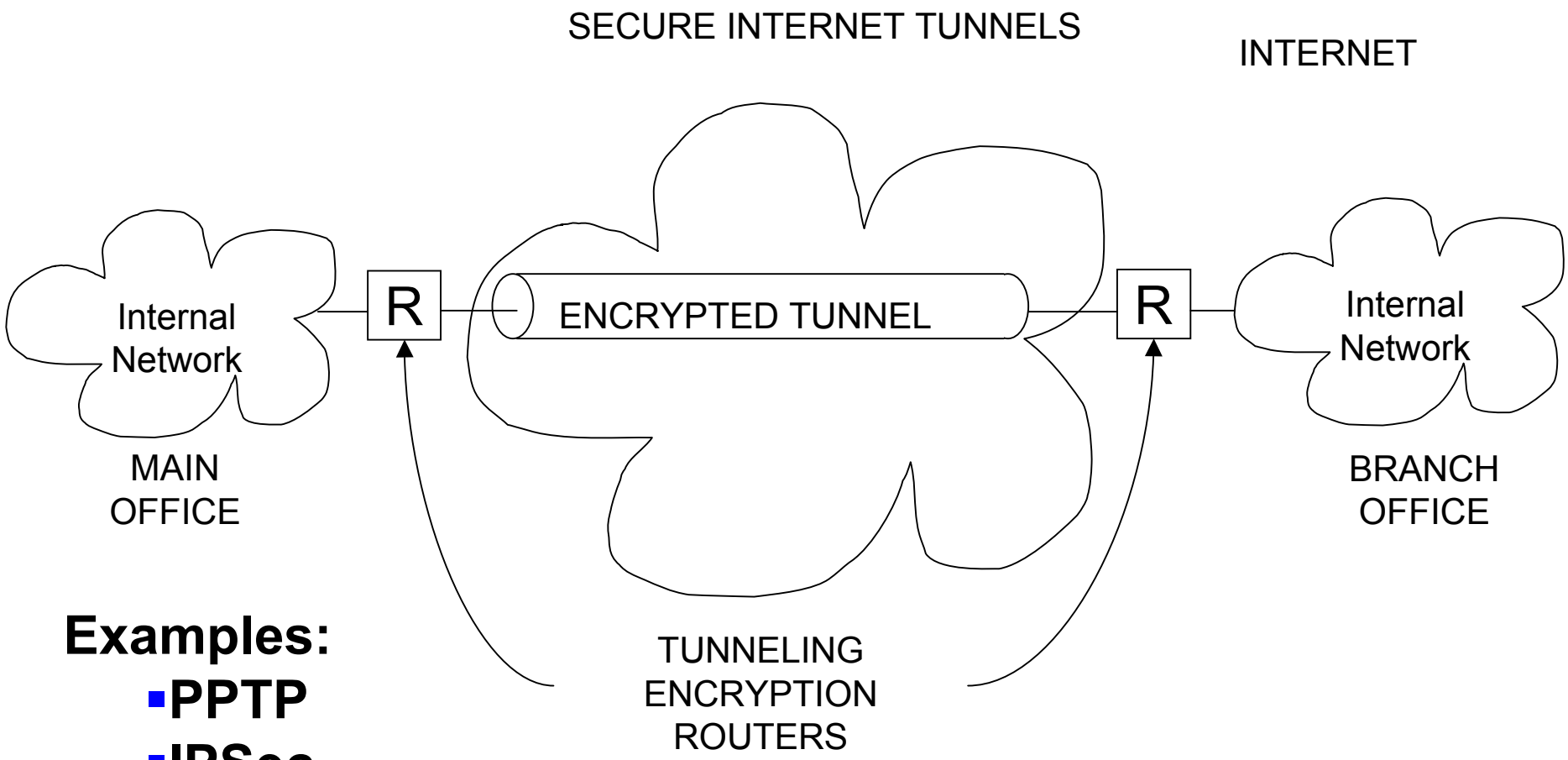
Encryption at the Transport Layer

- When encryption is done in the transport layer, the entire session is encrypted.
- A more sophisticated approach is to put it in the presentation layer, so that only those data structures or fields requiring encryption must suffer the overhead of it.
- Examples:
  - TLS (SSL)
  - IPSec (Transport Mode)

Session Encryption



Secure Internet Tunnels



Examples:

- **PPTP**
- **IPSec**

Cryptanalysis and Attacks on Cryptosystems

- Cryptanalysis is the art of deciphering encrypted communications without knowing the proper keys.
- There are many cryptanalytic techniques. Some of the more important ones for a system implementers are described herein.

Ciphertext-only Attack

- This is the situation where the attacker does not know anything about the contents of the message, and must work from ciphertext only.
- In practice it is quite often possible to make guesses about the plaintext, as many types of messages have fixed format headers.
- Even ordinary letters and documents begin in a very predictable way.
- It may also be possible to guess that some ciphertext block contains a common word.

Known-plaintext Attack

- The attacker knows or can guess the plaintext for some parts of the ciphertext.
- The task is to decrypt the rest of the ciphertext blocks using this information.
- This may be done by determining the key used to encrypt the data, or via some shortcut.

Chosen-plaintext Attack

- The attacker is able to have any text he likes encrypted with the unknown key.
- The task is to determine the key used for encryption.
- Some encryption methods, particularly RSA, are extremely vulnerable to chosen-plaintext attacks.
- When such algorithms are used, extreme care must be taken to design the entire system so that an attacker can never have chosen plaintext encrypted.

Others

- There are many other cryptographic attacks and cryptanalysis techniques.
- However, these are probably the most important ones for a practical system designer.
- Anyone contemplating to design a new encryption algorithm should have a much deeper understanding of these issues.
- One place to start looking for information is the excellent book Applied Cryptography by Bruce Schneier.

Unconditional and Computational Security

- Two fundamentally different ways ciphers may be secure:
- **Unconditional security**
  - No matter how much computer power is available, the cipher cannot be broken
- **Computational security**
  - Given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

Strength of Cryptographic Algorithms

- Good cryptographic systems should always be designed so that they are as difficult to break as possible.
- It is possible to build systems that cannot be broken in practice (though this cannot usually be proved).
- This does not significantly increase system implementation effort; however, some care and expertise is required. There is no excuse for a system designer to leave the system breakable.
- Any mechanisms that can be used to circumvent security must be made explicit, documented, and brought into the attention of the end users.

Strength of Cryptographic Algorithms

- In theory, any cryptographic method with a key can be broken by trying all possible keys in sequence. If using **brute force** to try all keys is the only option, the required computing power increases exponentially with the length of the key. A 32 bit key takes 2^32 (about 10^9) steps. This is something any amateur can do on his/her home computer. A system with 40 bit keys (e.g. US-exportable version of RC4) takes 2^40 steps - this kind of computing power is available in most universities and even smallish companies.

Strength of Cryptographic Algorithms

- A system with 56 bit keys (such as DES) takes a substantial effort, but is quite easily breakable with special hardware. The cost of the special hardware is substantial but easily within reach of organized criminals, major companies, and governments.
- Keys with 64 bits are probably breakable now by major governments, and will be within reach of organized criminals, major companies, and lesser governments in a few years.
- Keys with 80 bits may become breakable in future.
- Keys with 128 bits will probably remain unbreakable by brute force for the foreseeable future.
- Even larger keys are possible; in the end we will encounter a limit where the energy consumed by the computation, using the minimum energy of a quantum mechanic operation for the energy of one step, will exceed the energy of the mass of the sun or even of the universe.

Strength of Cryptographic Algorithms

- However, key length is not the only relevant issue.
- Many ciphers can be broken without trying all possible keys.
- In general, it is very difficult to design ciphers that could not be broken more effectively using other methods.
- Designing your own ciphers may be fun, but it is not recommended in real applications unless you are a true expert and know exactly what you are doing.

Strength of Cryptographic Algorithms

- One should generally be very wary of unpublished or secret algorithms. Quite often the designer is then not sure of the security of the algorithm, or its security depends on the secrecy of the algorithm.
- Generally, no algorithm that depends on the secrecy of the algorithm is secure. Particularly in software, anyone can hire someone to disassemble and reverse-engineer the algorithm.
- Experience has shown that a vast majority of secret algorithms that have become public knowledge later have been pitifully weak in reality.

Why PKC Requires Longer Keys than SKC

- The key lengths used in public-key cryptography are usually much longer than those used in symmetric ciphers.
- There the problem is not that of guessing the right key, but deriving the matching secret key from the public key.
- In the case of RSA, this is equivalent to factoring a large integer that has two large prime factors.

Why PKC Requires Longer Keys than SKC

- To give some idea of the complexity, for the RSA cryptosystem, a 256 bit modulus is easily factored by ordinary people.
- 384 bit keys can be broken by university research groups or companies.
- 512 bits is within reach of major governments. Keys with 768 bits are probably not secure in the long term.
- Keys with 1024 bits and more should be safe for now unless major algorithmic advances are made in factoring; keys of 2048 bits are considered by many to be secure for decades.

Conventional vs Public-Key vs ECC Key Sizes

Conventional	Public-key	ECC
(40 bits)	—	—
56 bits	(400 bits)	—
64 bits	512 bits	—
80 bits	768 bits	—
90 bits	1024 bits	160 bits
112 bits	1792 bits	195 bits
120 bits	2048 bits	210 bits
128 bits	2304 bits	256 bits

Key Sizes and Algorithms (cont'd)

- 512 bit public key vs 40 bit conventional key is a good balance for weak security
- Recommendations for public keys:
  - Use 512-bit keys only for micropayments/smart cards
  - Use 1K bit key for short-term use (1 year expiry)
  - Use 1.5K bit key for longer-term use
  - Use 2K bit key for certification authorities (keys become more valuable further up the hierarchy), long-term contract signing, long-term secrets
  - The same holds for equivalent-level conventional and ECC keys

Strength of Cryptographic Algorithms

- It should be emphasized that **the strength of a cryptographic system is usually equal to its weakest point**.
- No aspect of the system design should be overlooked, from the choice algorithms to the key distribution and usage policies.

Crypto is Becoming Ubiquitous

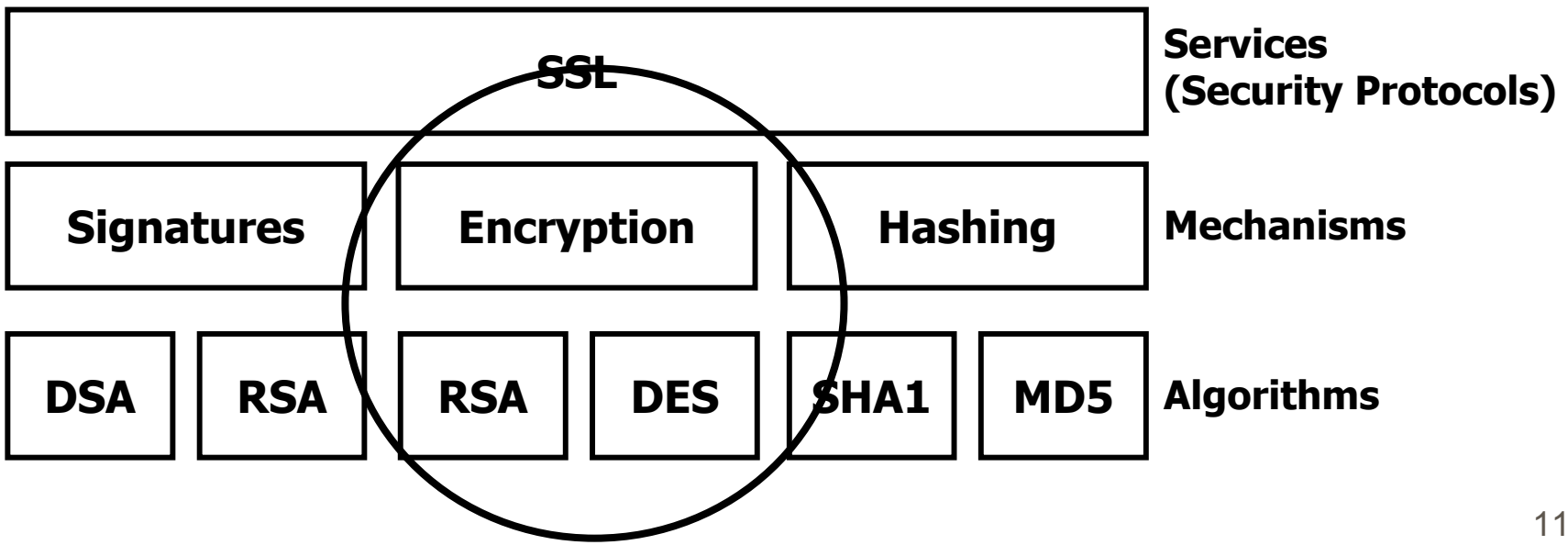
- Crypto is not just for internet e-mail. You will find it in:
- – Cellular phones
- – Cable/Sat TV broadcasts
- – radio modems
- – Smart cards
- – DVD
- – Garage door openers

Cryptography and Patents

- Many of the Public Key algorithms are patented.
- RSA is patented.
- Patent is granted by US Patent Office in the USA. Other countries have some procedure too.
- Patent is valid for 17 years, after it is issued not when it is filed
- Patent vs. Public Domain.

Cryptography is Not Security

- Encryption is a key enabling technology to implement computer security
- But Encryption is to security what bricks are to buildings



References

- Cryptography - Theory and Practice by Douglas Stinson
  CRC Press
  Boca Raton, 1995
- Applied Cryptography by Bruce Schneier
  Second Edition
  John Wiley & Sons, Inc.
  New York, c. 1996
- Handbook of Applied Cryptography by Alfred J. Menezes and others, Available freely on the web
- RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1
  RSA Laboratories, 2000
  RSA Security Inc.
  Available at http://www.rsadsi.com
- Internet Cryptography by Richard E. Smith
  Low Priced Edition, Pearson Education Asia
  Addison Wesley Longman 1997