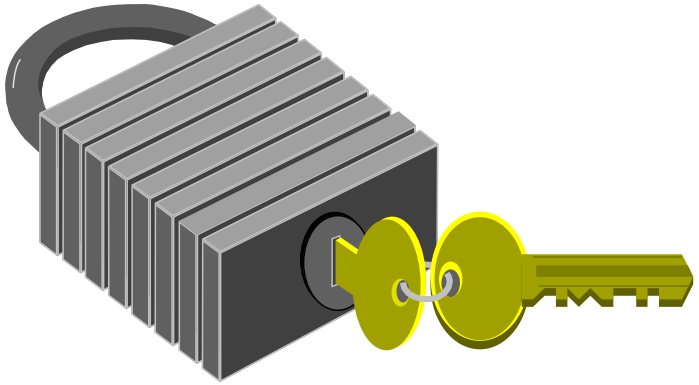
Encryption and Cryptography



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.

Plan for the Lecture

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

Concepts

- 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*

Cryptanalaysis

- The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key
- Also called codebreaking
- 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

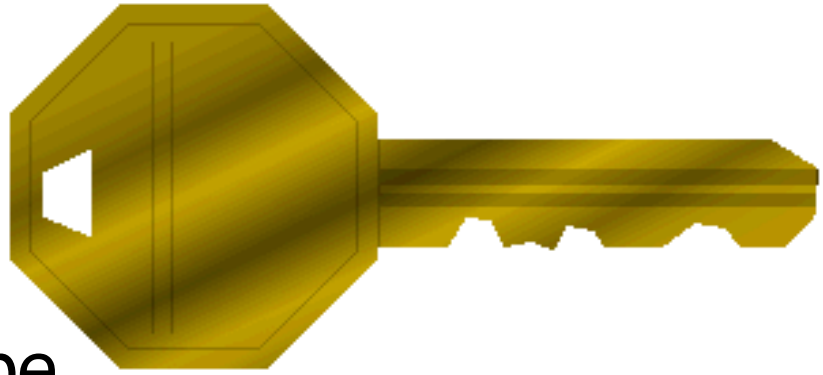
Algorithm Secrecy

- 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.

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 stream ciphers and block ciphers.
- Stream ciphers can encrypt a single bit 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.

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.

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 Ceasar used a simple substitution cipher, now known as the Caesar cipher
- Roger Bacon described several methods in 1200s

Cryptography Through History

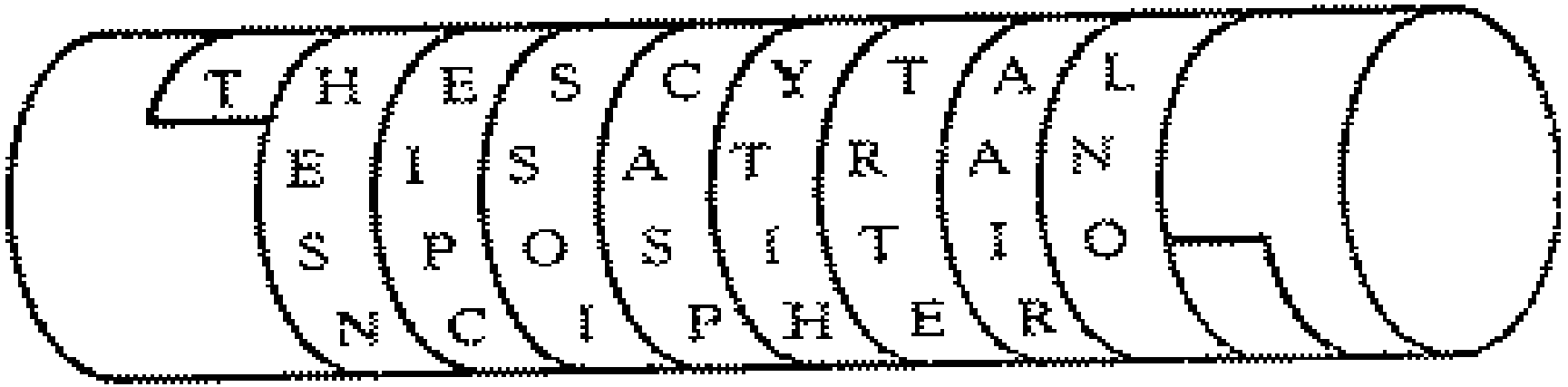
- Geoffrey Chaucer included several ciphers in his works
- Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s
- Blaise de Vigenère published a book on cryptology in 1585, & described the polyalphabetic substitution cipher
- increasing use, especially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

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.

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

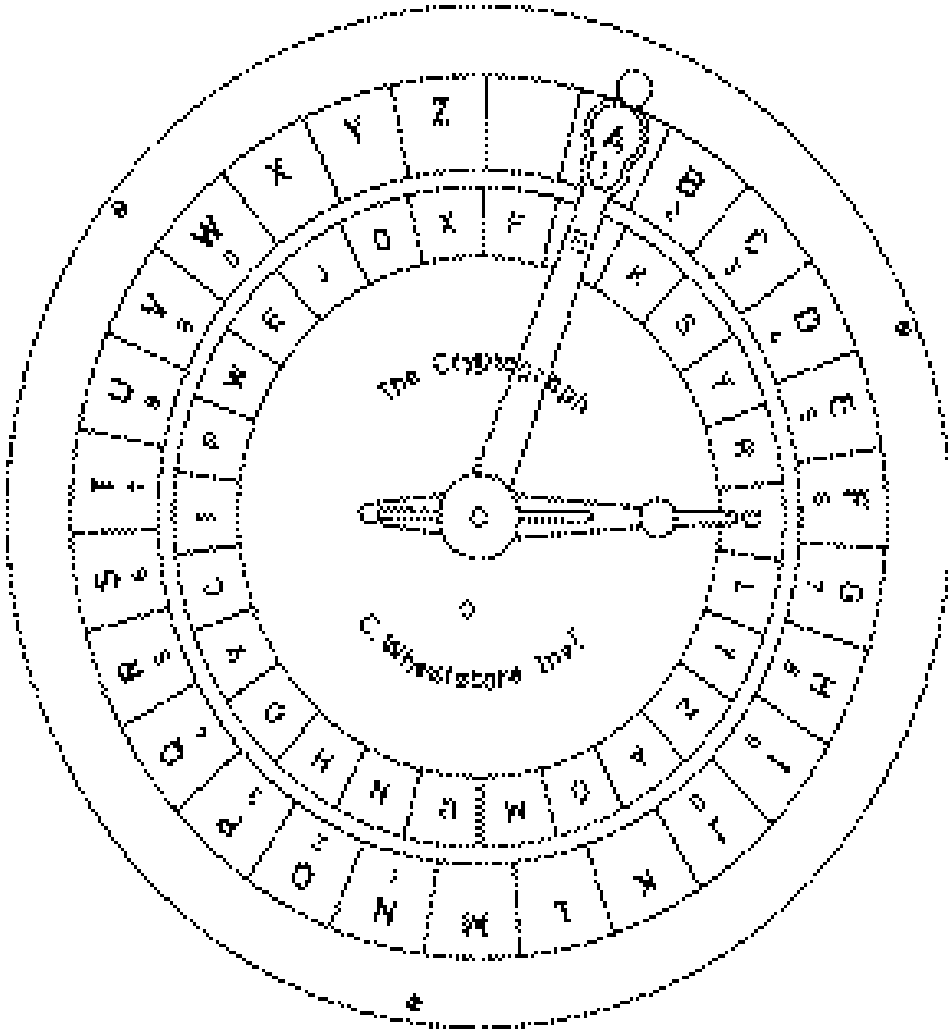


Machine Ciphers

- 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

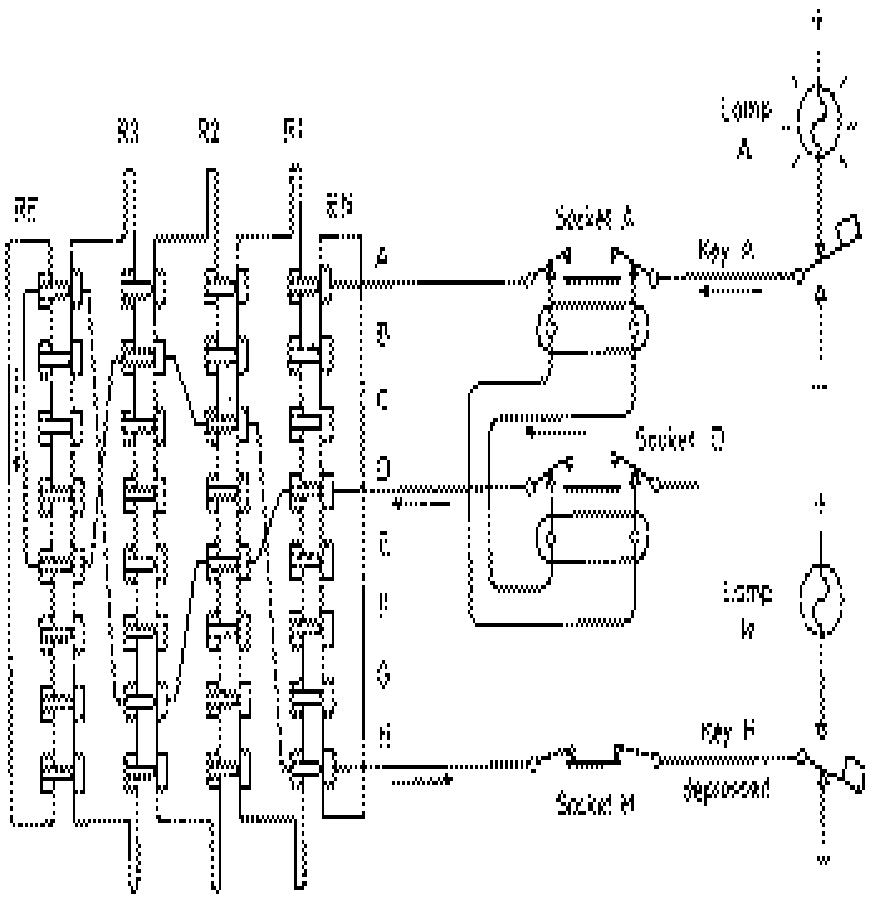
- Wheatstone disc, originally invented by Wadsworth in 1817, but developed by Wheatstone in 1860's, comprised two concentric wheels used to generate a polyalphabetic cipher

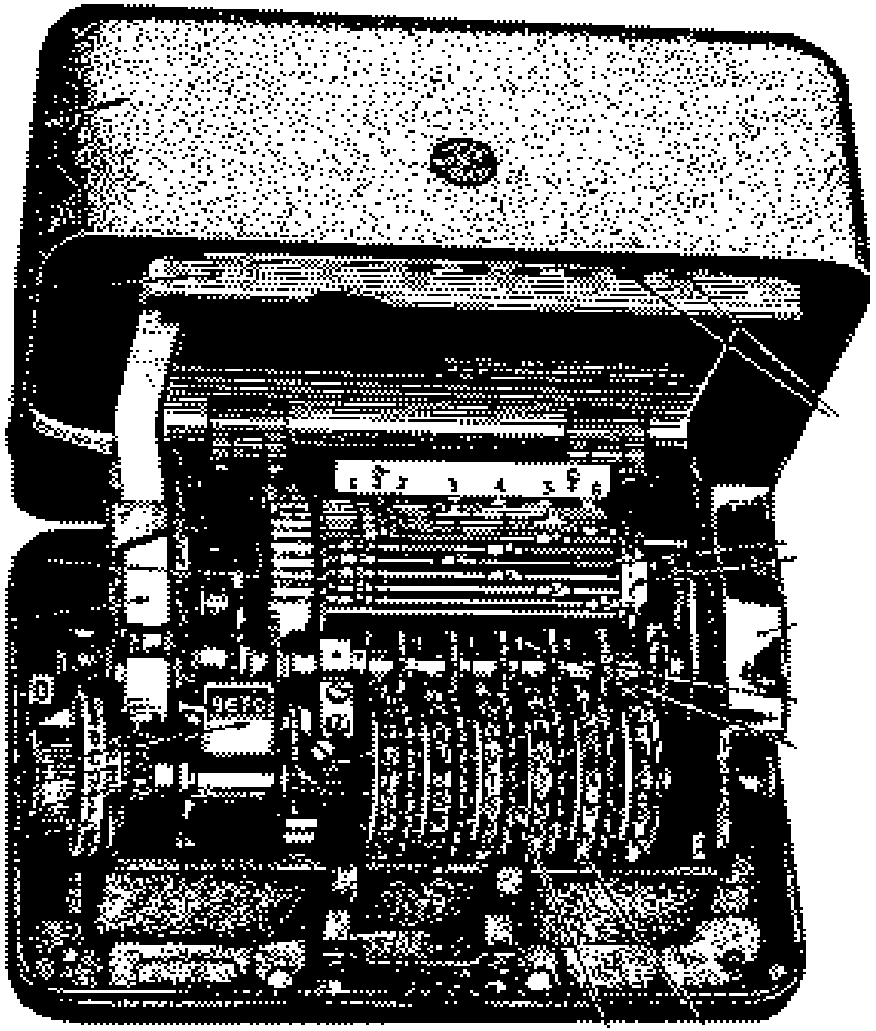


Enigma

- 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 "help" you would move ahead in the alphabet 3 letters to get "jgnr." 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.

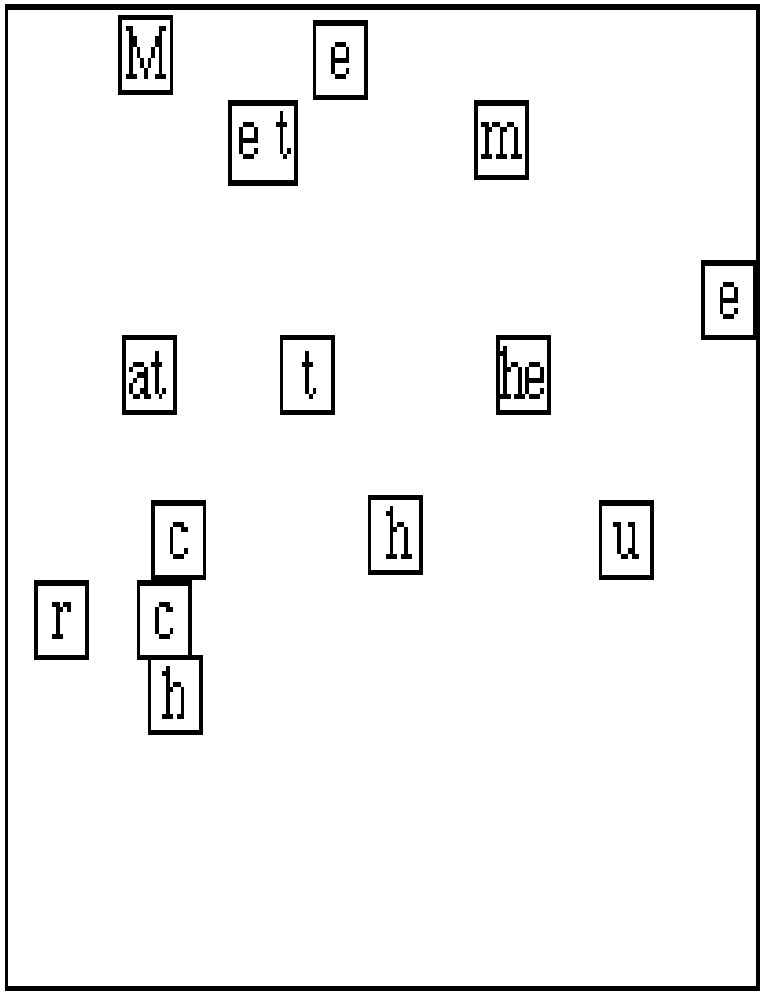
History - The Grille

- 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 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.

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!

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.

Classical Cryptographic Techniques

- 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

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 -> i + k mod 26
  - Decryption D_k : i -> i - k mod 26

A Simple Substitution Cipher

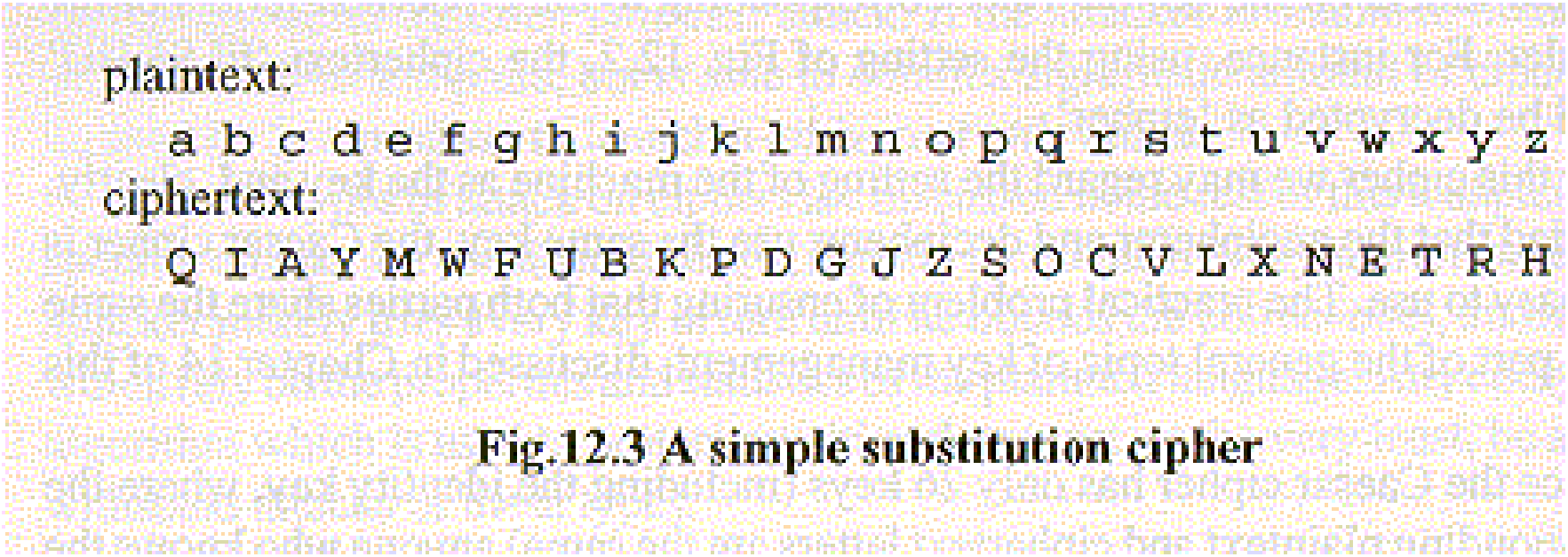


Fig.12.3 A simple substitution cipher

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

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		

Fig.12.4 Frequency distribution of letters in the English language

Polyalphabetic Substitution Cipher

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

Polyalphabetic Substitution Example

Example 4:

Suppose that a polyalphabetic cipher of period 3 is being used, with the 3 monoalphabetic ciphers M_1, M_2, M_3 defined below. To encrypt a message, the first 3 letters of the plaintext are enciphered according to ciphers M_1, M_2, M_3, 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
M_1:	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
M_2:	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
M_3:	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

For the plaintext message:

now is the time for every good man

the 1st, 4th, 7th ... letters are enciphered according to M_1, the 2nd, 5th, 8th ... letters according to M_2 and the remaining letters according to M_3. This yields the following ciphertext:

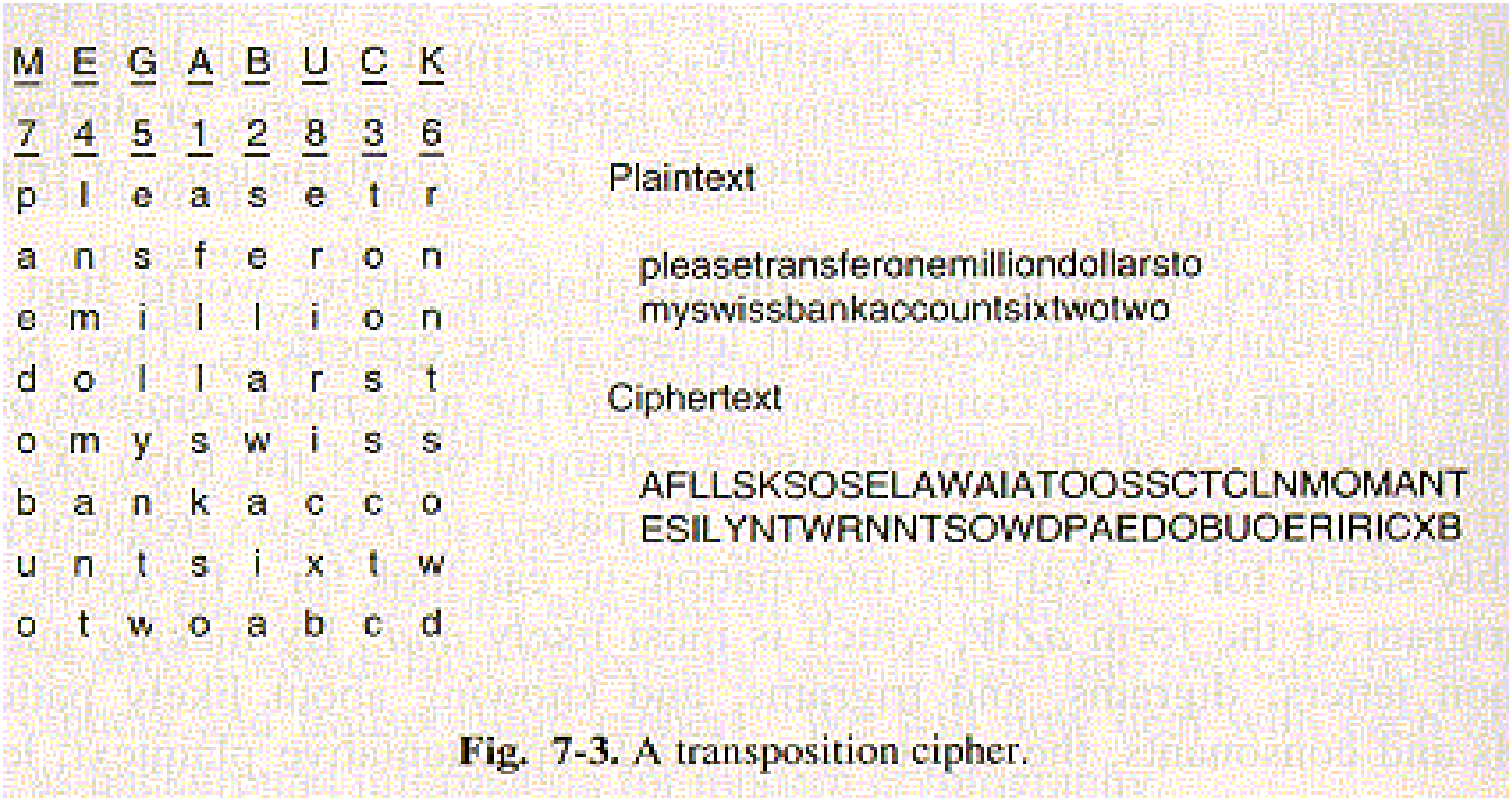
JQX CZ VXK VCER AQC PCRTX LBQZ QPK

Note, for instance, that the two letters 'o' in the word 'good' have been enciphered as different letters. Also the three letters 'X' in the ciphertext correspond to 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

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

Fig. 7-3. A transposition cipher.

Transposition Cipher Example (2)

Double Transposition Order for Enciphering:	1	3	5	4	2
Keyword:	**S**	**H**	**O**	**E**	**S**
	P	A	Y	M	E
	B	Y	S	U	N
Column 1: PGDSROUS	D	A	Y	O	R
Column 2: ENRECQEZ	S	U	F	F	E
Column 3: AYAUTNEZ	R	T	H	E	C
Column 4: MUOFEECZ	O	N	S	E	Q
Column 5: YSYFHSNZ	U	E	N	C	E
	S	Z	Z	Z	Z

One Time Pad

- 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.

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

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.

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
  - User Authentication
  - Message Authentication
  - Proof of Origin

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.

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.

Negotiated Secure Sessions

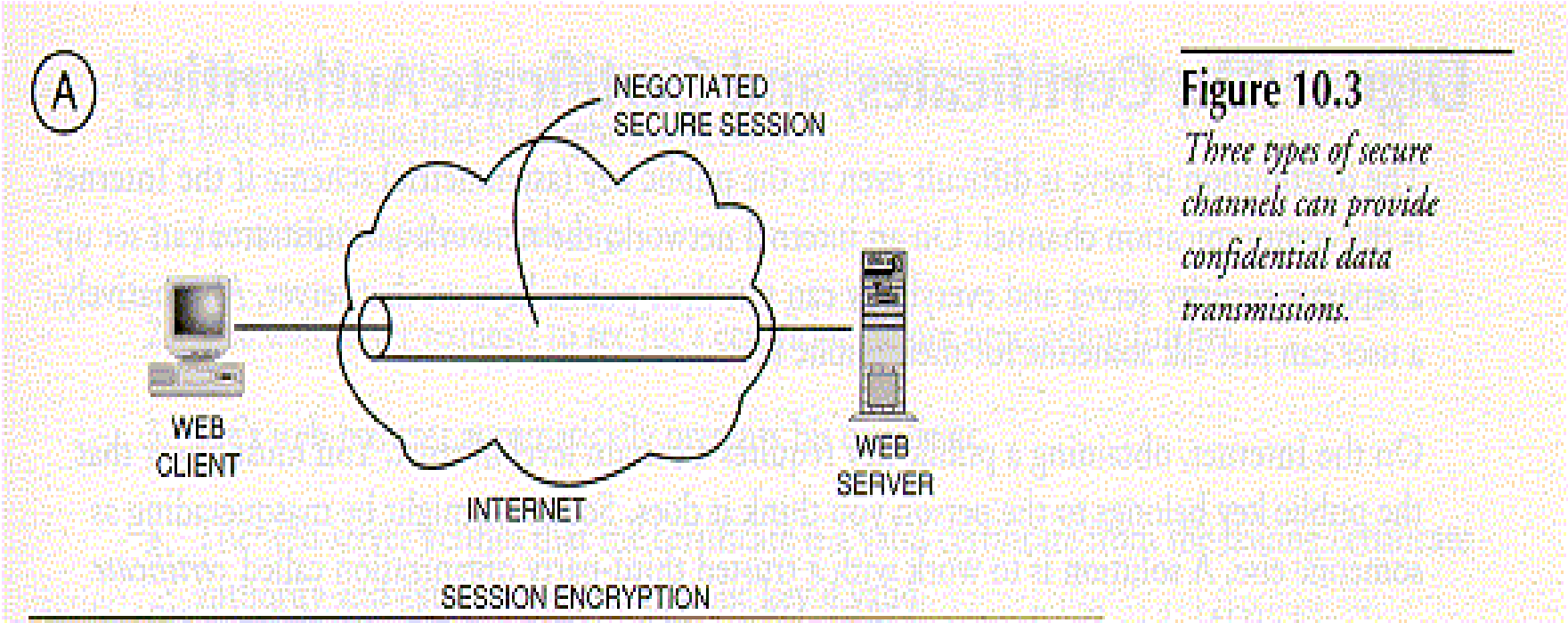
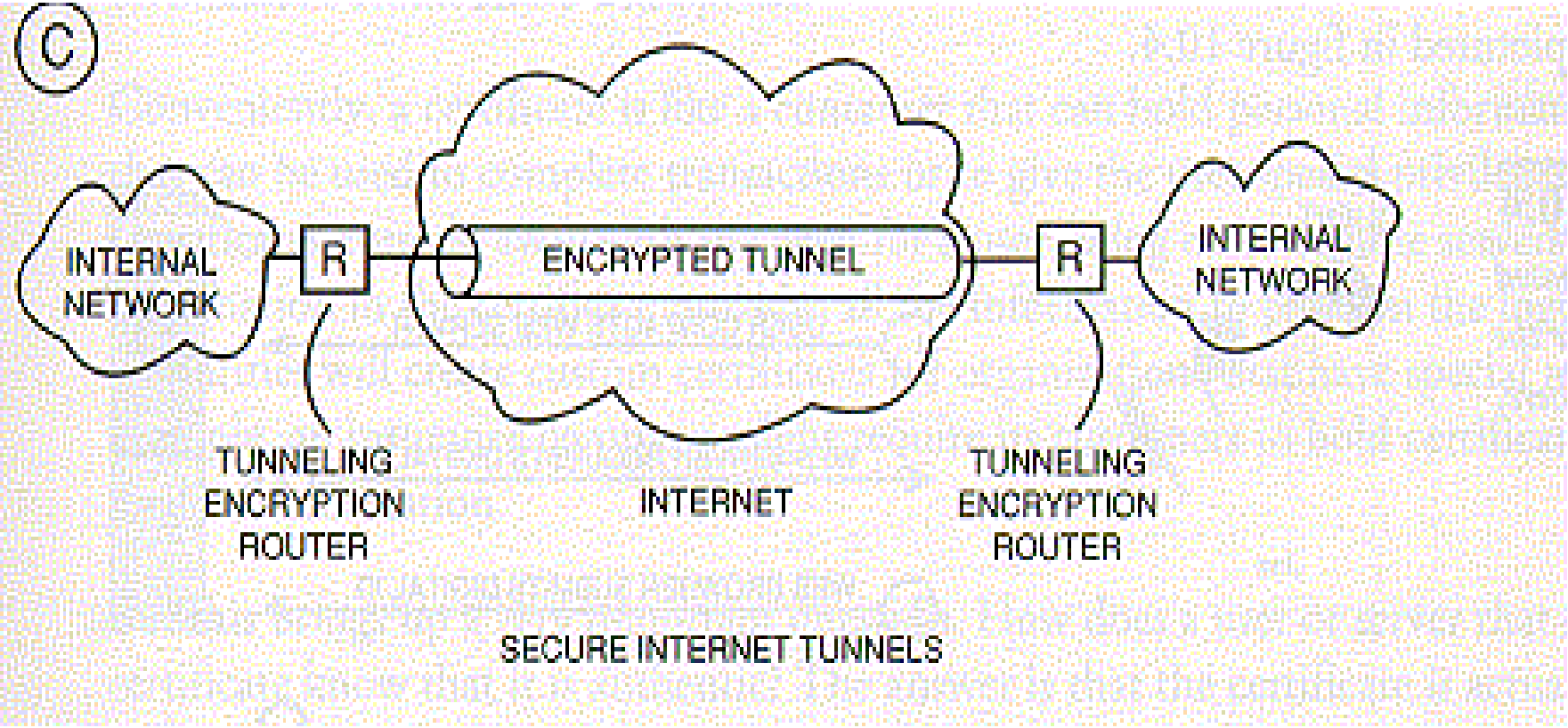


Figure 10.3
Three types of secure channels can provide confidential data transmissions.

Secure Internet Tunnels



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.

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.