DENNIS GUNAWAN

IF470 COMPUTER SECURITY

06 PHYSICAL DATA LOSS

UMN

UNIVERSITAS MULTIMEDIA NUSANTARA

REVIEW: ILLICIT DATA ACCESS

- Attack
  - Keylogging
- Threat
  - Illicit Data Access
- Harm
  - Data and Reputation

- Vulnerability
  - Physical Access
  - Misplaced Trust
  - Insiders
  - System Subversion
  - Weak Authentication

- Failed Countermeasure
  - Security through Obscurity
- Countermeasure
  - Physical Access Control
  - Strong Authentication
  - Trust / Least Privilege

COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO 6
  - Students are able to relate physical data loss to real case in their daily life (C3)

OUTLINE

- Threat
  - Loss of Data
  - Disaster
- Vulnerability
  - Physical Access
  - Unprotected Availability of Data
  - Unprotected Confidentiality of Data
- Countermeasure
  - Policy
  - Physical Security
  - Data Redundancy (Backup)
  - Encryption

INTRODUCTION

- Leave money unattended in a busy, public space
  - Likely to lose it
- Keep your money in your pocket
  - Pickpockets
- Leave your money at home behind a locked door
  - Burglars
- Other defenses
  - Alarms, guard dogs, and safes

- Theft is a simple crime
  - Simple to understand
  - Sometimes simple to perpetrate
  - Not always simple to prevent
- With a motive, an attacker will try diligently to overcome any defenses you mount

INTRODUCTION

- Theft of money or anything else can occur to anyone at any time
  - A thief may single out from a crowd one person who looks like an easy or likely target
  - Another thief may try every third person who walks alone down the street, regardless of the victim's appearance

- In some cases, the theft is simply to take the computer and resell the computer itself
  - Other times the thief will target a specific person's computer that contains valuable data

- We need to protect valuables at all times

LOSS OF DATA

- Nonmalicious loss
  - Sometimes we accidentally delete the wrong file
  - A system failure causes a file to become corrupted
  - We overwrite a good file with a bad one
  - We simply put the file somewhere and then cannot remember where or under what name

Data become unavailable

Denying access to or productive use of the data

LOSS OF DATA

- Theft
  - Loss combined with malicious intent
- Thief’s objective
  - The thief wants your data or merely the computer

The confidentiality of the data is now potentially in peril

Not only do you not have access to your data, someone else does

LOSS OF DATA

Harm

Ranging from **embarrassment** to **identity theft** to **failure of a responsibility** because of lacking data

DISASTER

- Natural or unpredictable disasters
  - Fires, floods, windstorms, explosions, sabotage, and riots
- Nonselective
  - Affect buildings, people, valuables, papers, and computers indiscriminately

Physical Damage

Destruction of hardware, leading to **loss of data and equipment**

PHYSICAL ACCESS

- An attacker with physical access can quickly and easily switch cables, install software, or add hardware
- Components are also getting smaller
- What qualifies as a "computer" is likewise becoming unclear
- The small size of such devices makes theft easier

UNPROTECTED AVAILABILITY OF DATA

- Protecting against data access loss has been a need since the inception of computing
- Early days of computing
  - Data storage was big and bulky
    - Rendered some protection against theft
  - Computing devices were far less reliable
    - Time between hardware-induced system failures was measured in hours, not months or years

- System administrators had to protect system data and shared programs against loss
  - Individual users were responsible for their own data
- Failure to protect data could mean that an entire computing session had been wasted on an expensive computer

UNPROTECTED CONFIDENTIALITY OF DATA

- The seriousness of the issue was not that a device containing data was stolen
  - It was the compromise of the confidentiality of data items

- A laptop may be stolen for a relatively small payoff as a computing device on the open market

- When the relatively inexpensive laptop was stolen, the far more valuable private data was also harmed

POLICY

- Organizations have to create security policies that achieve the desired effect
- Enforce security policies
- Ensure that all employees comply with security policy requirements

PHYSICAL SECURITY

- Business travelers
  - Laptop theft from hotel rooms or at airport check-in facilities or from unsupervised suitcases and briefcases
  - Prudent travelers carry their computers with them into restaurants and onboard planes
- Often deterrence is adequate protection
  - A locking cable for a laptop, secured to an immovable object will suffice for a short period in a low-threat environment

PHYSICAL SECURITY

- Computer equipment is sensitive to the heat of a car parked in the sun
- A static electric charge due to low humidity
- Water damage from a fire protection sprinkler system
- A power surge caused by an electrical storm
- Inadequate physical protection, as computers become small devices carried almost everywhere

DATA REDUNDANCY (BACKUP)

A copy of all or part of a file

to assist in reestablishing a lost file

- Periodic backups are usually performed automatically, often at night when system use is low
- Backup addresses the availability issue of being able to access data after a device has been lost, stolen, or broken

DATA REDUNDANCY (BACKUP)

Complete backup

- Everything on the system is copied
- Done at regular intervals depending on the criticality of the information or service provided by the system

Revolving backup

- The last several backups are kept
- Each time a backup is done, the oldest backup is replaced with the newest one
- 2 reasons
  - Avoid problems with corrupted media
  - Allow users or developers to retrieve old versions of a file

Selective backup

- Only files that have been changed (or created) since the last backup are saved
  - Fewer files must be copied
  - Done more quickly

DATA REDUNDANCY (BACKUP)

Offsite Backup

- Keeping a backup version separate from the actual system
  - Rent warehouse space some distance from the computing system
  - Far enough away that a crisis is not likely to affect the offsite location at the same time

- As a backup is completed, it is transported to the backup site

- If both secrecy and integrity are important, a bank vault, or even a secure storage place in another part of the same building, can be used

DATA REDUNDANCY (BACKUP)

Networked Storage

- Storage providers sell space in which you can store data
- Think of these services as big network-attached disk drives
- Choose a storage provider whose physical storage is not close to your processing
- You do not need to manage tapes or other media and physically transport them offsite

DATA REDUNDANCY (BACKUP)

Cloud Backup

- Cloud computing
  - A user's workstation is augmented with a seemingly infinite set of hardware on the Internet
- The user signs a contract with a cloud provider and uses the Internet effectively as an auxiliary device
- Risks
  - The user gives up significant control over data, which has implications for highly sensitive data
  - What if the cloud provider goes out of business?
  - What if the user defaults on the contract with the provider?

DATA REDUNDANCY (BACKUP)

Cloud Backup

- 3 significant advantages of this approach relate to availability
  - The cloud provider assumes responsibility for maintaining the content
    - Cloud computing can provide automatic redundancy that overcomes failing to perform backups at critical times
  - The user needs only an Internet connection to access a document
  - The cloud permits document sharing by a controlled list of people

DATA REDUNDANCY (BACKUP)

- It may be important to recover from a crisis and quickly resume computation
- The hard part is deciding where to put the equipment in order to begin a temporary operation

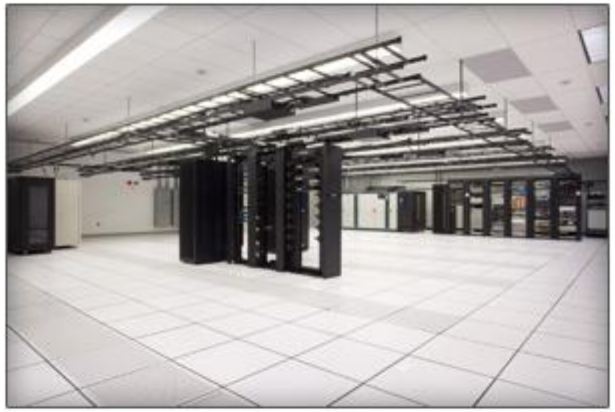
A bank might be able to tolerate a four-hour loss of computing facilities during a fire, but it could not tolerate a ten-month period to rebuild a destroyed facility, acquire new equipment, and resume operation.

DATA REDUNDANCY (BACKUP)

Cold Site

- A facility with power and cooling available, in which a computing system can be installed to begin immediate operation

- These sites usually come with cabling, fire prevention equipment, separate office space, telephone access, network connectivity, and other features

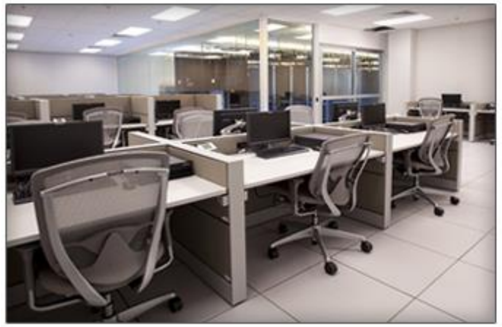


DATA REDUNDANCY (BACKUP)

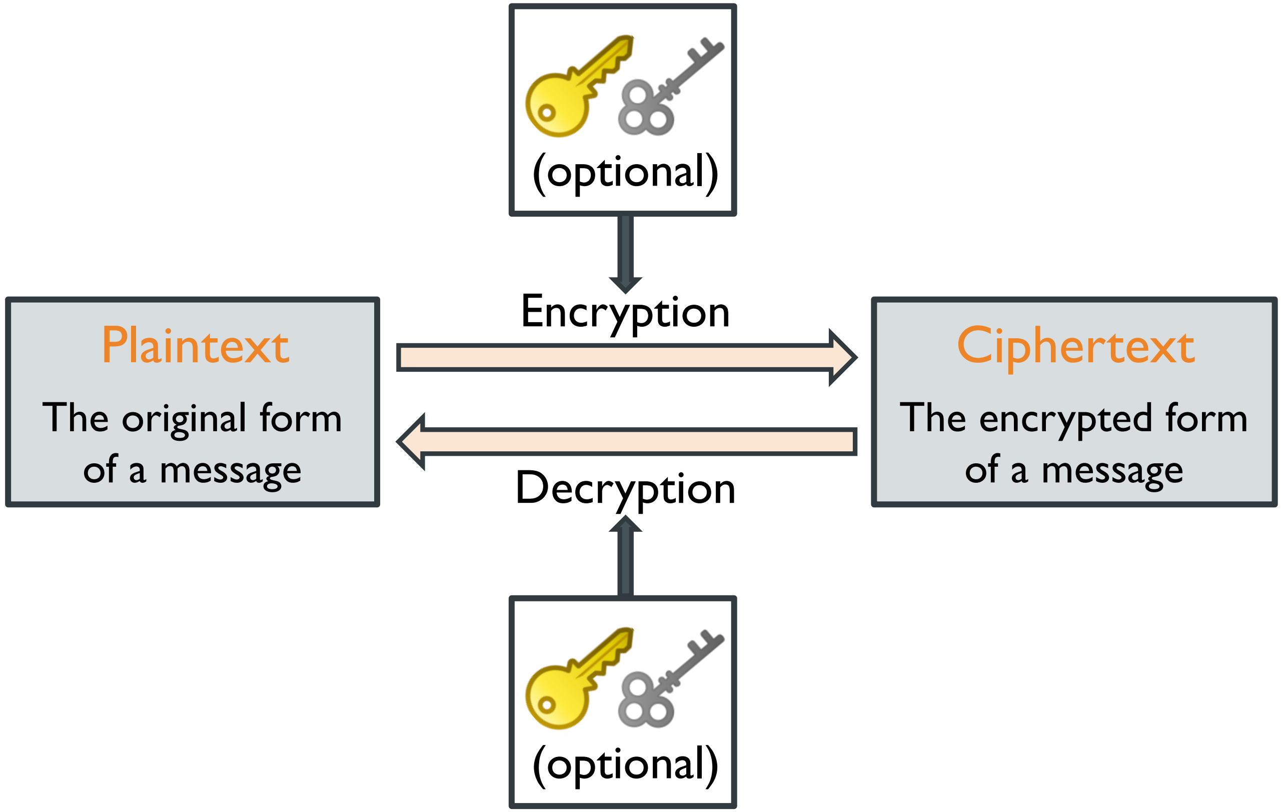
Hot Site

- A computer facility with an installed and ready-to-run computing system

- The system has peripherals, telecommunications lines, power supply, and even personnel ready to operate on short notice



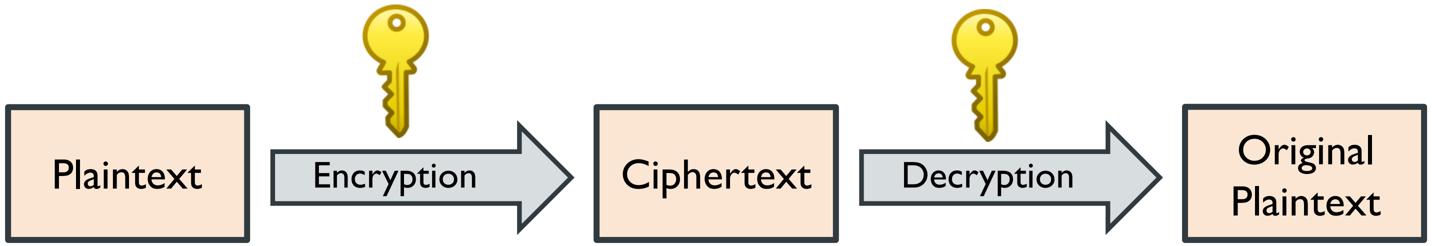
ENCRYPTION


(optional)
Encryption
Plaintext
The original form of a message
Ciphertext
The encrypted form of a message
Decryption
(optional)

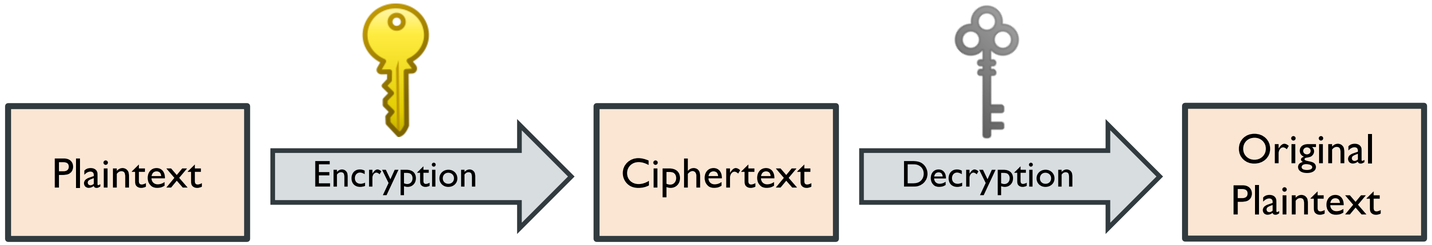
- Encryption
  - The process of encoding a message so that its meaning is not obvious
- Decryption
  - The process of transforming an encrypted message back into its normal, original form

ENCRYPTION

- **Symmetric Encryption**
  - The encryption and decryption keys are the same



- **Asymmetric Encryption**
  - Encryption and decryption keys come in pairs



ENCRYPTION

Cryptography

- The practice of using encryption to conceal text
- A cryptographer works on behalf of a legitimate sender or receiver

Cryptanalysis

- Breaking an encryption
- A cryptanalyst works on behalf of an unauthorized interceptor

It is risky to pronounce an algorithm secure just because it cannot be broken with current technology, or worse, that it has not been broken yet

ENCRYPTION: REPRESENTING CHARACTERS

- This representation allows us to consider performing arithmetic on the "letters" of a message

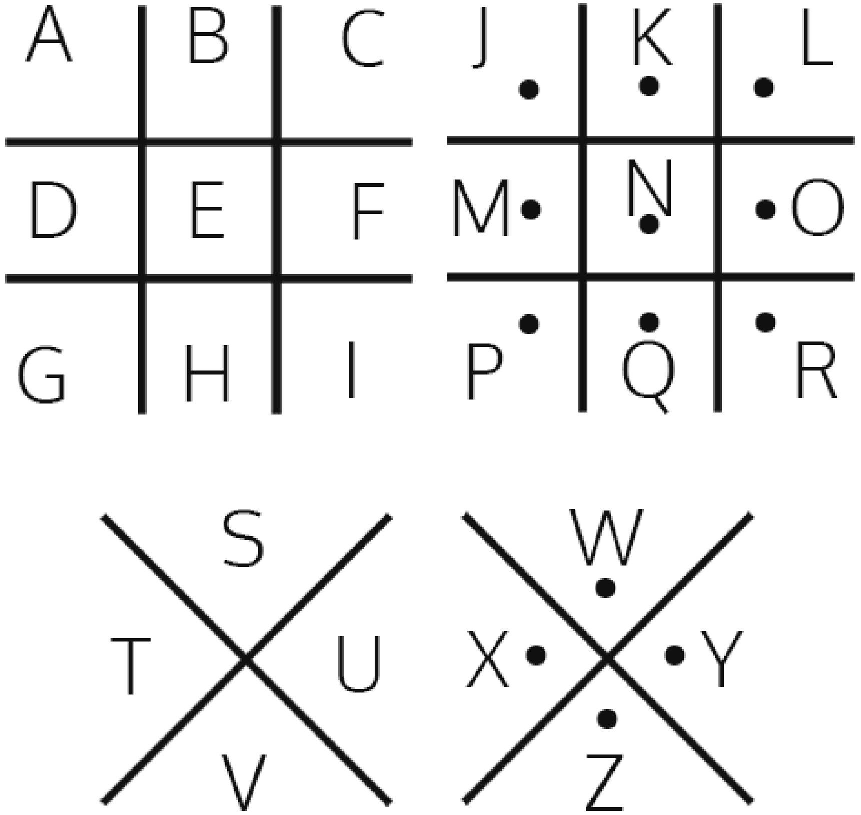
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Code	0	1	2	3	4	5	6	7	8	9	10	11	12

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

- Arithmetic is performed as if the alphabetic table were circular
  - Y + 3 = B
  - Every result of an arithmetic operation is between 0 and 25

SUBSTITUTION CIPHERS

One letter is exchanged for another



CAESAR CIPHER

Each letter is translated to the letter a fixed number of places after it in the alphabet

- Julius Caesar is said to have been the first to use this scheme
- Caesar used a shift of 3

$$\boxed{c_i = E(p_i) = p_i + 3}$$

CAESAR CIPHER

- A full translation chart of the Caesar cipher is shown here

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	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

- Using this encryption, the message TREATY IMPOSSIBLE would be encoded as

T	R	E	A	T	Y		I	M	P	O	S	S	I	B	L	E
w	u	h	d	w	b		l	p	s	r	v	v	l	e	o	h

CAESAR CIPHER

- During Caesar’s lifetime, the simplicity did not dramatically compromise the safety of the encryption
  - Anything written, even in plaintext, was rather well protected
  - Few people knew how to read!

- A secure encryption should not allow an interceptor to use a small piece of the ciphertext to predict the entire pattern of the encryption

OTHER SUBSTITUTIONS

- One way to scramble an alphabet is to use a key, a word that controls the permutation

- If the key is **word**, the sender or receiver first writes the alphabet and then writes the key under the first few letters of the alphabet

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
word
```

- The sender or receiver then fills in the remaining letters of the alphabet, in some easy-to-remember order, after the keyword

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
wordabcefghijklmnpqstuvxyz
```

OTHER SUBSTITUTIONS

- Duplicate letters in a keyword, such as the second s and o in **professional**, are dropped

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
profesinalbcdghjkmqtuvwxyz
```

- Since regularity helps an interceptor, a less regular rearrangement of the letters is desirable

- One possibility is to count by threes (or fives or sevens or nines) and rearrange the letters in that order
  - At the end of the alphabet, the pattern continues mod 26

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
adgjmpsvybehknqtwzcfilorux
```

CRYPTANALYSIS OF SUBSTITUTION CIPHERS

```
wklv phvvdjh lv qrw wrr kdug wr euhdn
```

- Short words
- Words having particular patterns
  - ‘sleeps’ is a word that follows the pattern ‘abccda’
- Words with repeated patterns
- Common initial and final letters
- Common prefixes and suffixes

- The frequency with which certain letters are used
  - In English, the letters E, T, O, and A occur far more often than J, Q, X, and Z
- The nature and context of the text being analyzed
  - In a medical article in which the term x-ray was used often, the letter x would have an uncommonly high frequency

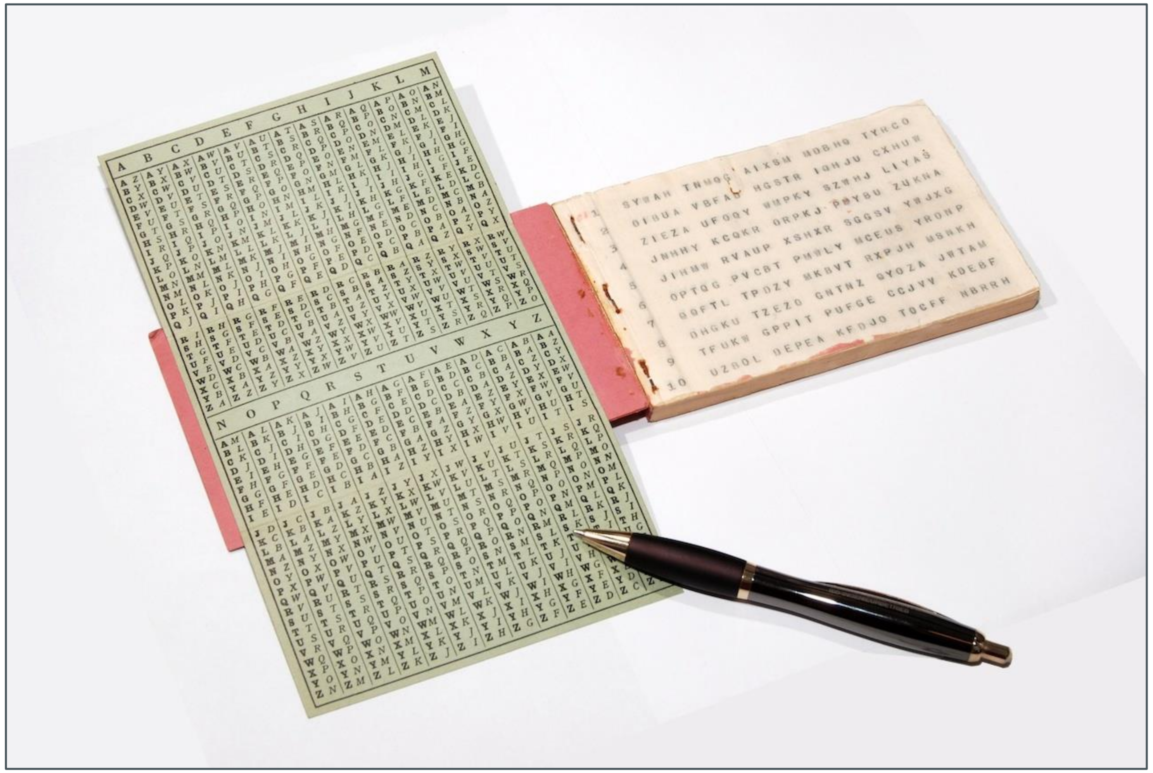
ONE-TIME PADS

1
2
3
4
5
6
SYWAH TNMOG AIXSM MDBHQ TYRCO
OIBUA VBFAD HGSTR IQHJU CXHUW
ZIEZA UFOQY WMPKY SZWHJ LIYAS
JNHHY KCQKR ORPKJ PMYBU ZUKNA
JIHMW RVAUP XSHXR SGGSV
OPTQG PVCBT PMWLY MCEU
KNK
UKIQU
IRCXH
NXSDP
ACUPC
PIYJG
TARFP

- A large, nonrepeating set of keys is written on sheets of paper, glued together into a pad

- If the keys are 20 characters long and a sender must transmit a message 300 characters in length, the sender would tear off the next 15 pages of keys

ONE-TIME PADS



- The sender would write the keys one at a time above the letters of the plaintext and encipher the plaintext with a prearranged chart (called a Vigenère tableau) that has all 26 letters in each column, in some scrambled order

- The sender would then destroy the used keys

- The receiver needs a pad identical to that of the sender

- The receiver takes the appropriate number of keys and deciphers the message

ONE-TIME PADS

- The one-time pad method has 2 problems
  - The need for absolute synchronization between sender and receiver
  - The need for an unlimited number of keys
    - Although generating a large number of random keys is no problem with a computer, printing, distributing, storing, and accounting for such keys are problems

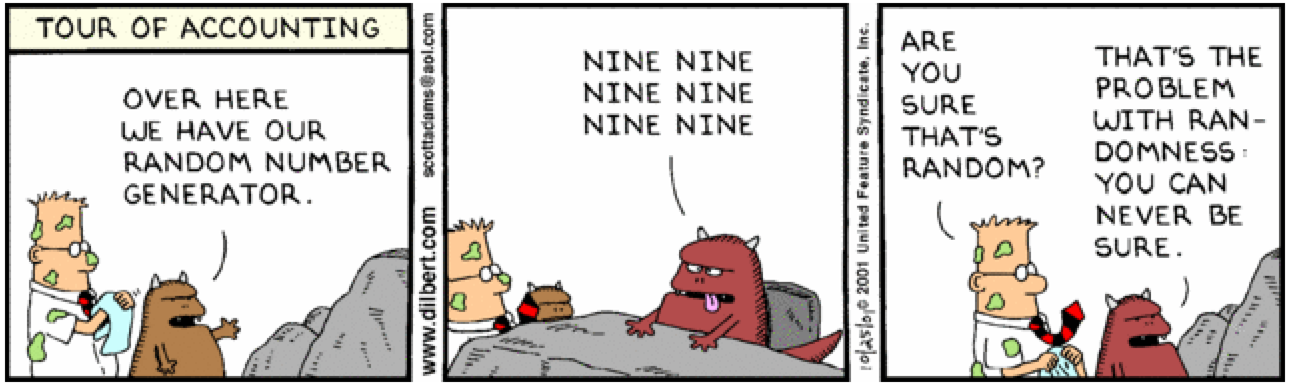
ONE-TIME PADS: LONG RANDOM NUMBER SEQUENCES

- A close approximation of a one-time pad for use on computers is a random number generator

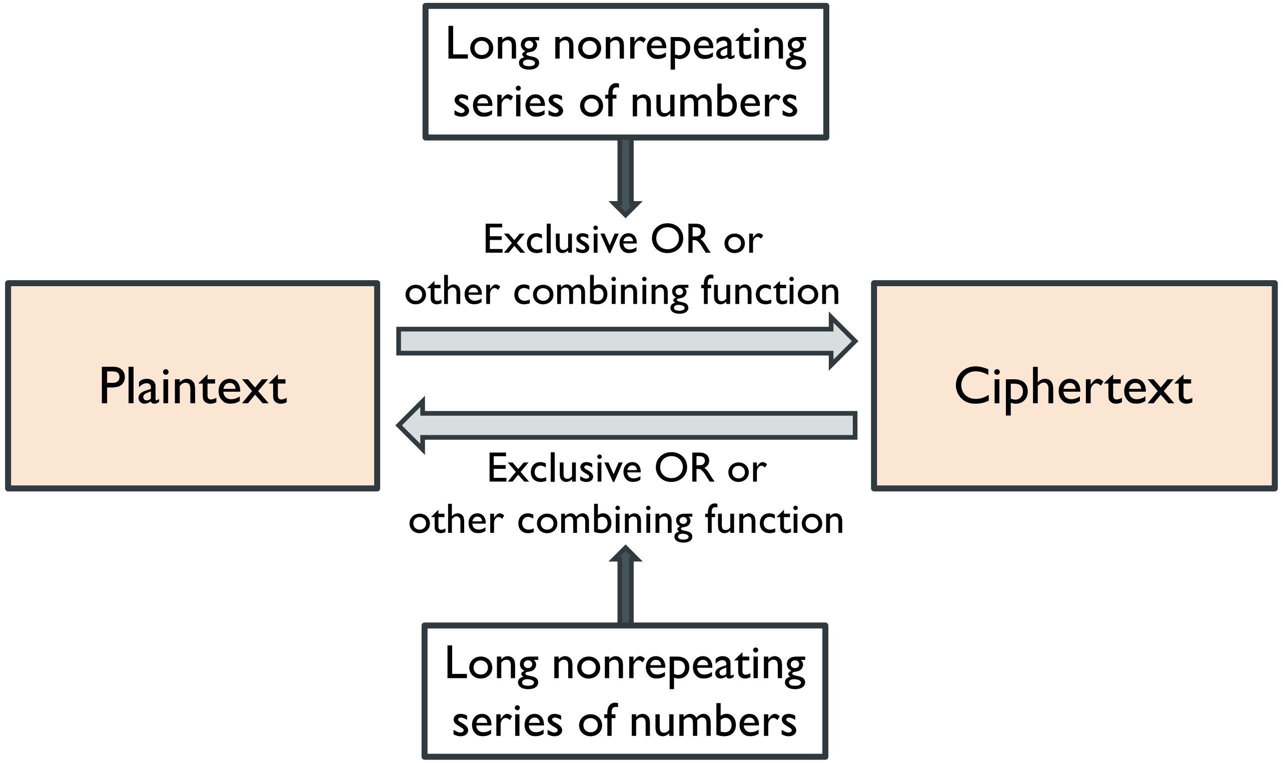
- In fact, computer random numbers are not random

- They really form a sequence with a very long period

- They go for a long time before repeating the sequence


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

ONE-TIME PADS:VERNAM CIPHER


Long nonrepeating series of numbers
Exclusive OR or other combining function
Plaintext
Ciphertext
Exclusive OR or other combining function
Long nonrepeating series of numbers

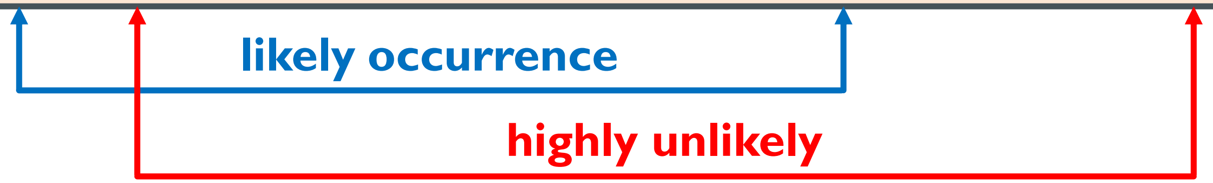
- The basic encryption involves an arbitrarily long nonrepeating sequence of numbers that are combined with the plaintext

- Immune to cryptanalytic attack
  - There is no pattern

ONE-TIME PADS:VERNAM CIPHER

- For instance, the message is VERNAM CIPHER

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
Scaled to <26 (mod 26)	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b



ONE-TIME PADS: BOOK CIPHERS

- Another source of supposedly "random" numbers is any book, piece of music, or other object of which the structure can be analyzed

- Both the sender and receiver need access to identical objects

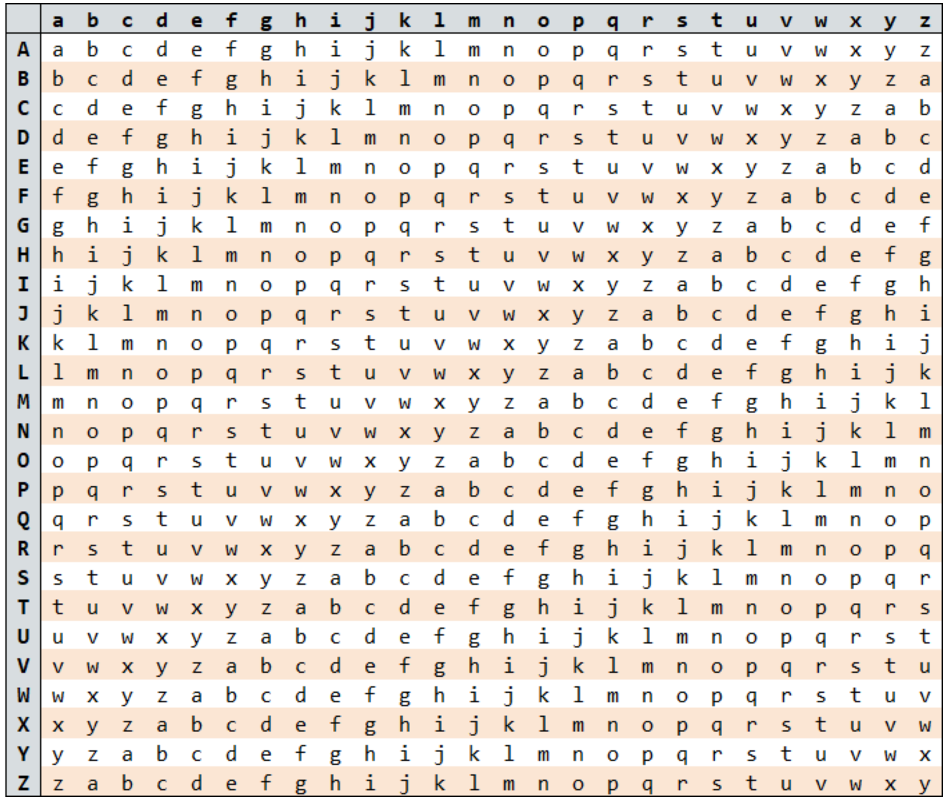
ONE-TIME PADS: BOOK CIPHERS

- A passage from Descartes’ meditation
  - *What of thinking? I am, I exist, that is certain*

- To encipher the message MACHINES CANNOT THINK by using the Descartes key, you would write the message under enough of the key and encode the message by selecting the substitution in row p_i, column k_i

```
iamie xistt hatis cert
MACHI NESCA NNOTT HINK
uaopm kmkvt unhbl jmed
```

- Vigenère tableau



	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

TRANSPOSITIONS / PERMUTATIONS

The letters of the message are rearranged

- Because a transposition reorders the symbols of a message, it is also known as a permutation

TRANSPOSITIONS: COLUMNAR TRANSPOSITIONS

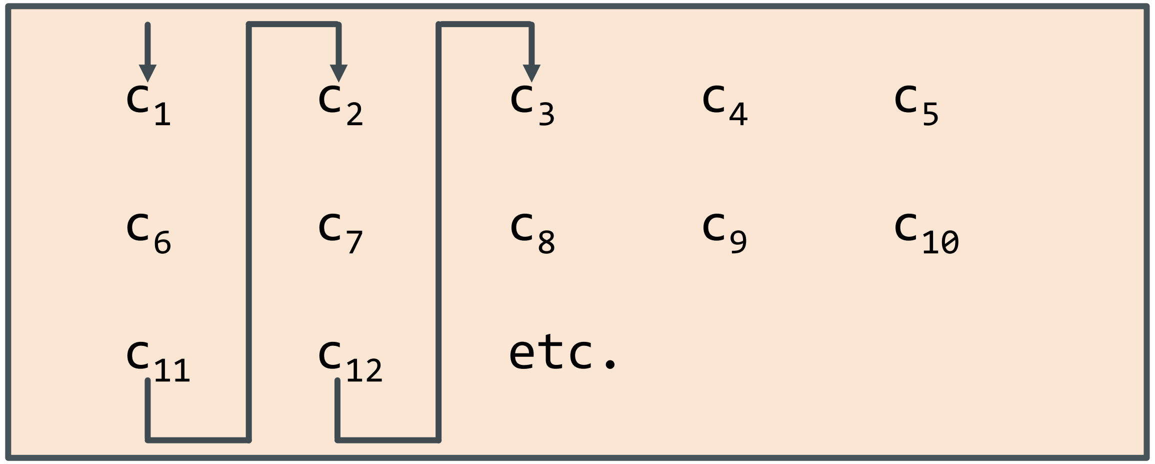
A rearrangement of

the characters of the plaintext

into columns

Five-column transposition

- The plaintext characters are written in rows of five and arranged one row after another
- You form the resulting ciphertext by reading down the columns



c_1 c_2 c_3 c_4 c_5

c_6 c_7 c_8 c_9 c_{10}

c_{11} c_{12} etc.

TRANSPOSITIONS: COLUMNAR TRANSPOSITIONS

- Suppose you want to write the plaintext message THIS IS A MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS

- We arrange the letters in 5 columns as

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

- The resulting ciphertext would then be read down the column as

```
tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns
```

- If the message length is not a multiple of the length of a row, the last columns will be one or more letters short
  - When this happens, we sometimes use an infrequent letter such as X to fill in any short columns

DIGRAMS & TRIGRAMS

- The frequency of appearance of letter groups can be used to match up plaintext letters that have been separated in a ciphertext
- The infrequent combinations can occur in acronyms, in foreign words or names, or across word boundaries

- 10 most common digrams and trigrams in English (shown in descending order of frequency)

Digrams	Trigrams
EN	ENT
RE	ION
ER	AND
NT	ING
TH	IVE
ON	TIO
IN	FOR
TE	OUR
AN	THI
OR	ONE

CRYPTANALYSIS OF A TRANSPOSITION CIPHER

- The first step in analyzing the transposition is computing the letter frequencies
  - If we find that all letters appear with their normal frequencies, we can infer that a transposition has been performed
- The trick then is to break it into columns
  - We must do an exhaustive comparison of strings of ciphertext
- For each window position, ask 2 questions
  - Do common digrams appear?
  - Do most of the digrams look reasonable?

```
t s s o h o a
n i w h a a s o l r s t o ...
```

```
  t s s o h o a
n i w h a a s o l r s t o ...
```

```
    t s s o h o a
n i w h a a s o l r s t o ...
```

```
      t s s o h o a
n i w h a a s o l r s t o ...
```

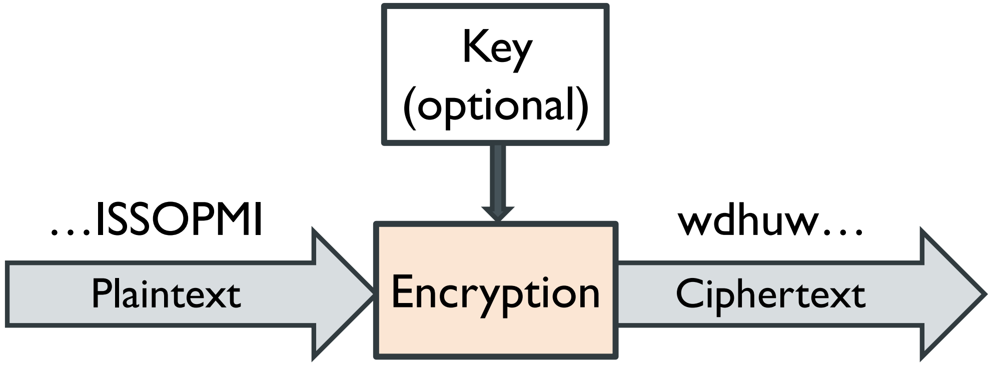
COMBINATIONS OF APPROACHES

- You could combine various approaches to encryption to strengthen the overall security of your system
- A combination of 2 ciphers is called a product cipher
- Just because you apply 2 ciphers does not necessarily mean the result is any stronger than, or even as strong as, either individual cipher
- 2 encryptions can sometimes interact, leaving you with less protection than you might expect

STREAM & BLOCK CIPHERS

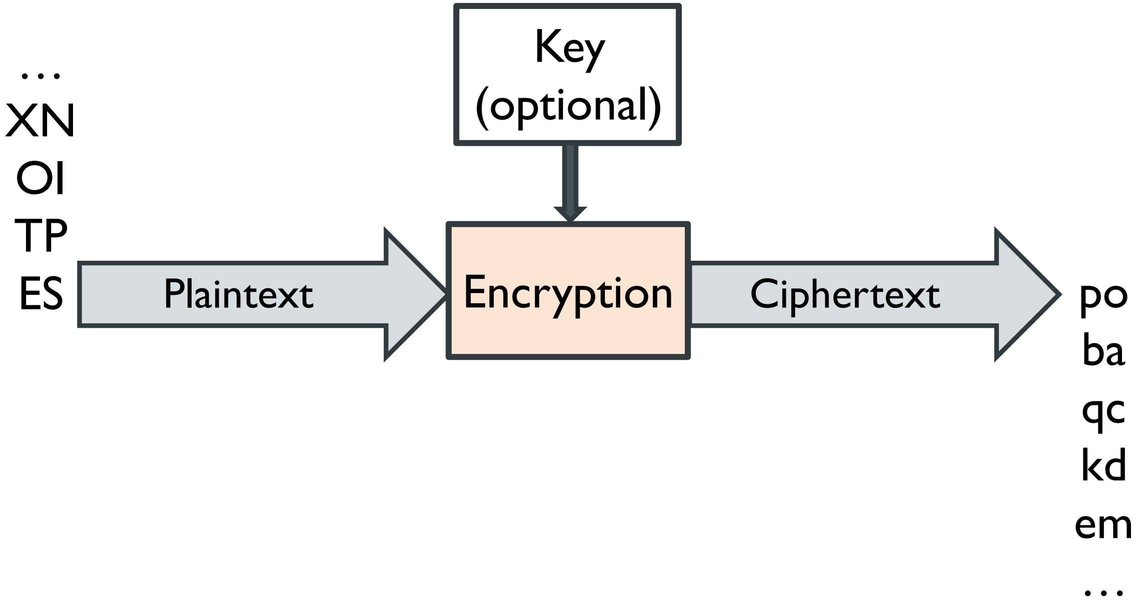
Stream Ciphers

- Convert one symbol of plaintext immediately into a symbol of ciphertext



Block Ciphers

- Encrypt a group of plaintext symbols as a single block and produce blocks of ciphertext



CONFUSION & DIFFUSION

Confusion

- Take the information from the plaintext and transform it so that the interceptor cannot readily recognize the message
- An algorithm providing good confusion has a complex functional relationship between the plaintext / key pair and the ciphertext
- The goal of substitution is confusion
  - Caesar cipher is not good for providing confusion
  - A one-time pad provides good confusion

Diffusion

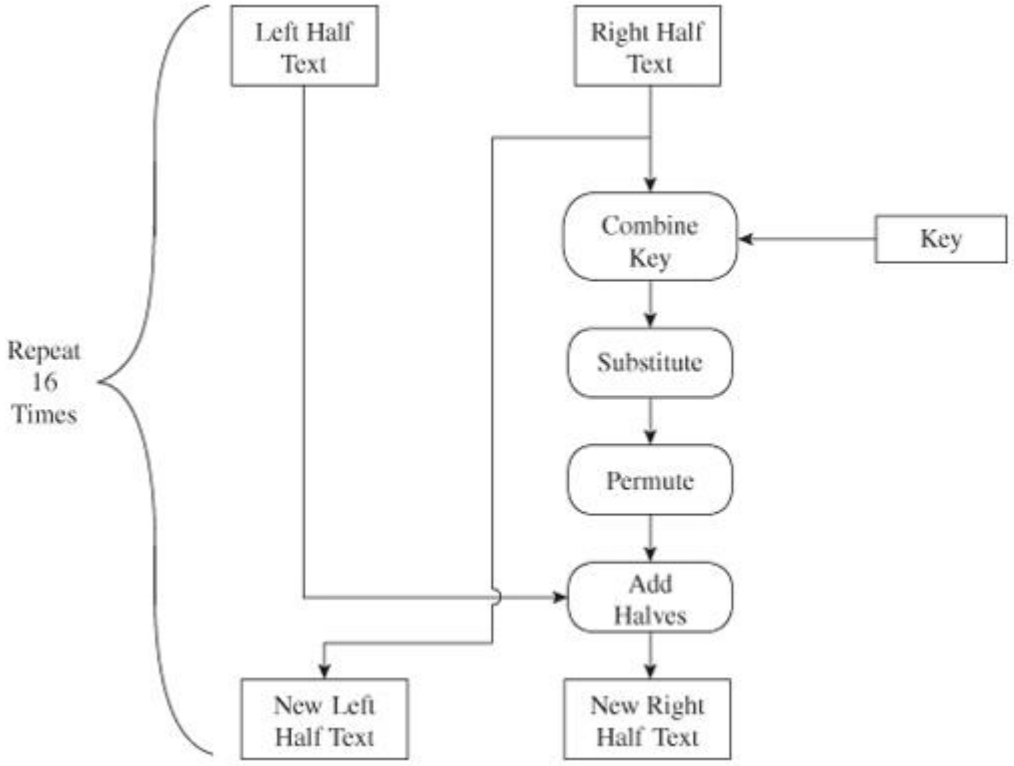
- Spread the information from the plaintext over the entire ciphertext so that changes in the plaintext affect many parts of the ciphertext
- Good diffusion means that the interceptor needs access to much of the ciphertext to be able to infer the algorithm
- With transposition, the cryptographer aims for diffusion

PROPERTIES OF "COMMERCIAL GRADE" OR "TRUSTWORTHY" ENCRYPTION SYSTEMS

- It is based on sound mathematics
  - Not just invented
  - Derived from solid principles
- It has been analyzed by competent experts and found to be sound
  - Review by critical outside experts
- It has stood the "test of time"
  - The flaws in many algorithms are discovered relatively soon after their release
  - People continue to review
  - A long period of successful use and analysis is not a guarantee of a good algorithm

DATA ENCRYPTION STANDARD (DES)

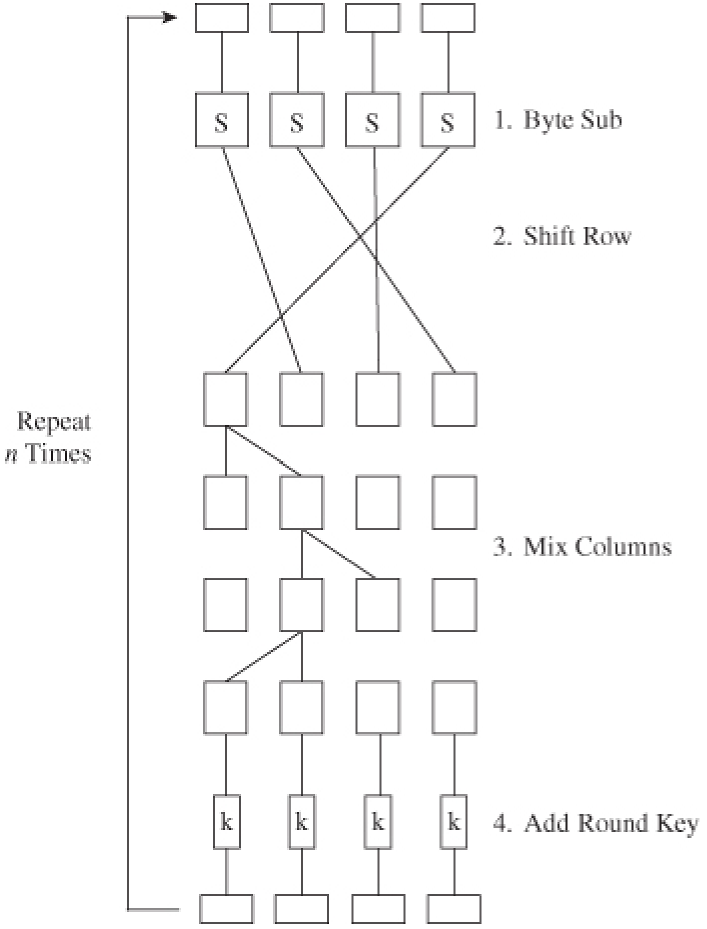
- Combination of 2 fundamental building blocks of encryption
  - Substitution provides the confusion
  - Transposition provides the diffusion
- Its adequacy has recently been questioned



ADVANCED ENCRYPTION STANDARD (AES)

- It primarily uses substitution, transposition, and the shift, exclusive OR, and addition operations

- There are 10, 12, or 14 rounds for keys of 128, 192, and 256 bits, respectively



DISK ENCRYPTION

What is
Security & Privacy
FileVault
FileVault secures the data on your disk by encrypting its contents automatically
Click the lock to make changes.
BitLocker Drive Encryption
Windows (C:) BitLocker on
Full Disk Encryption (FDE)?

- Several commercially available tools can take an entire disk and encrypt it

REFERENCES

- Pfleeger, Charles P. and Shari Lawrence Pfleeger (2012), *Analyzing Computer Security*, 1st Edition, Prentice Hall.

NEXT WEEK: BUFFER OVERFLOW

- Harm
  - Destruction of Code and Data
- Vulnerability
  - Off-by-One Error
  - Integer Overflow
  - Unterminated Null-Terminated String
  - Parameter Length and Number
  - Unsafe Utility Programs

- Countermeasure
  - Programmer Bounds Checking
  - Programming Language Support
  - Stack Protection / Tamper Detection
  - Hardware Protection of Executable Space
  - General Access Control

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE

Vision

To become an **outstanding** undergraduate Computer Science program that produces **international-minded** graduates who are **competent** in software engineering and have **entrepreneurial spirit** and **noble character**.

INFORMATIKA UMN UNIVERSITAS MULTIMEDIA NUSANTARA

Mission

1. To conduct studies with the best technology and curriculum, supported by professional lecturer
2. To conduct research in Informatics to promote science and technology
3. To deliver science-and-technology-based society services to implement science and technology