Bachelor of Computer Science

SCS2214 - Information System Security

Handout 1 - Introduction

Kasun de Zoysa
kasun@ucsc.cmb.ac.lk

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

What do we mean by "secure"?

- At one time Bank robbery was common. Now its very rare. What has changed or been implemented to provide this security?
  - Sophisticated alarms
  - Criminal investigation techniques (DNA testing)
  - Change in "assets" (cash was/is inherently insecure)
  - Improvements in communication and transportation
- Risk becomes so high that it is no longer beneficial.

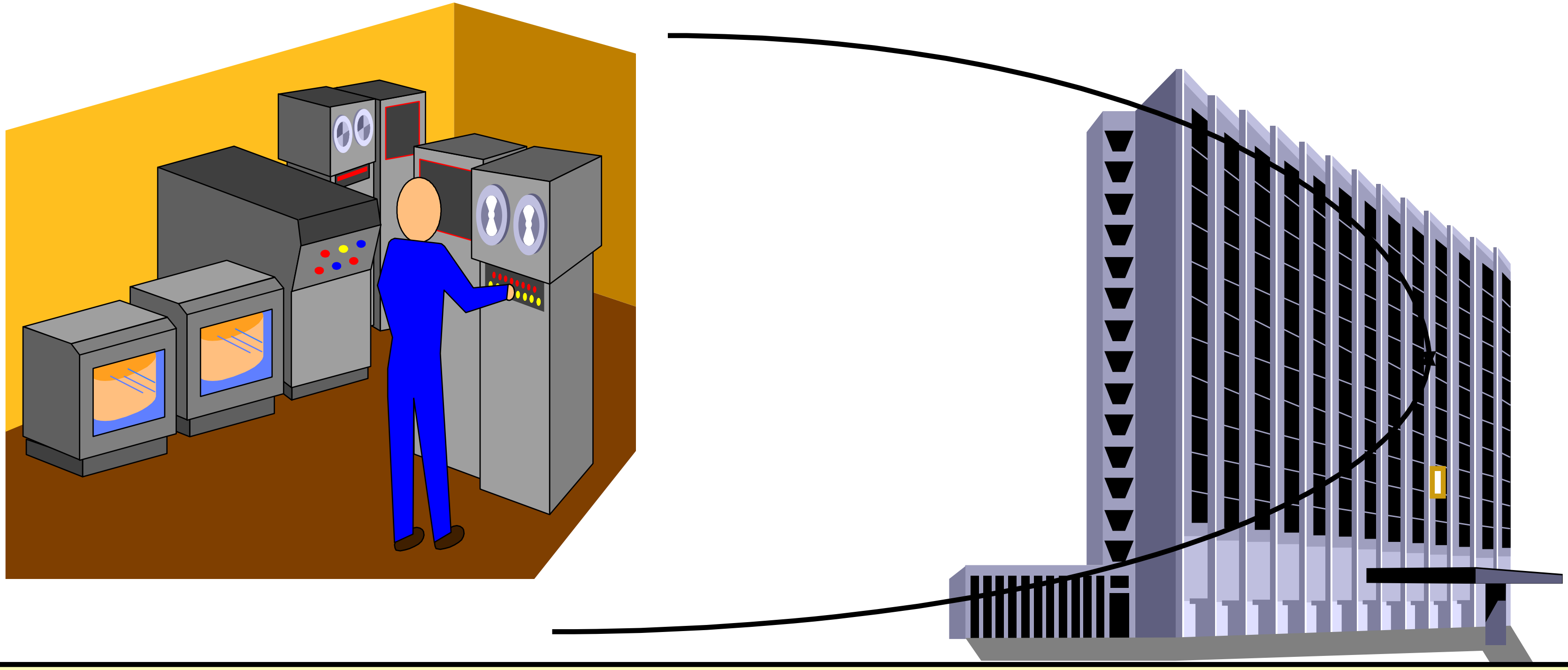
Security is all about protecting valuables

- In our case the “valuables” are computer related assets instead of money
  - Though these days money is so electronic that one can argue that the protection of money is a subset of computer asset security
- Information seems to be the currency of the 21st century.

Money vs. Information

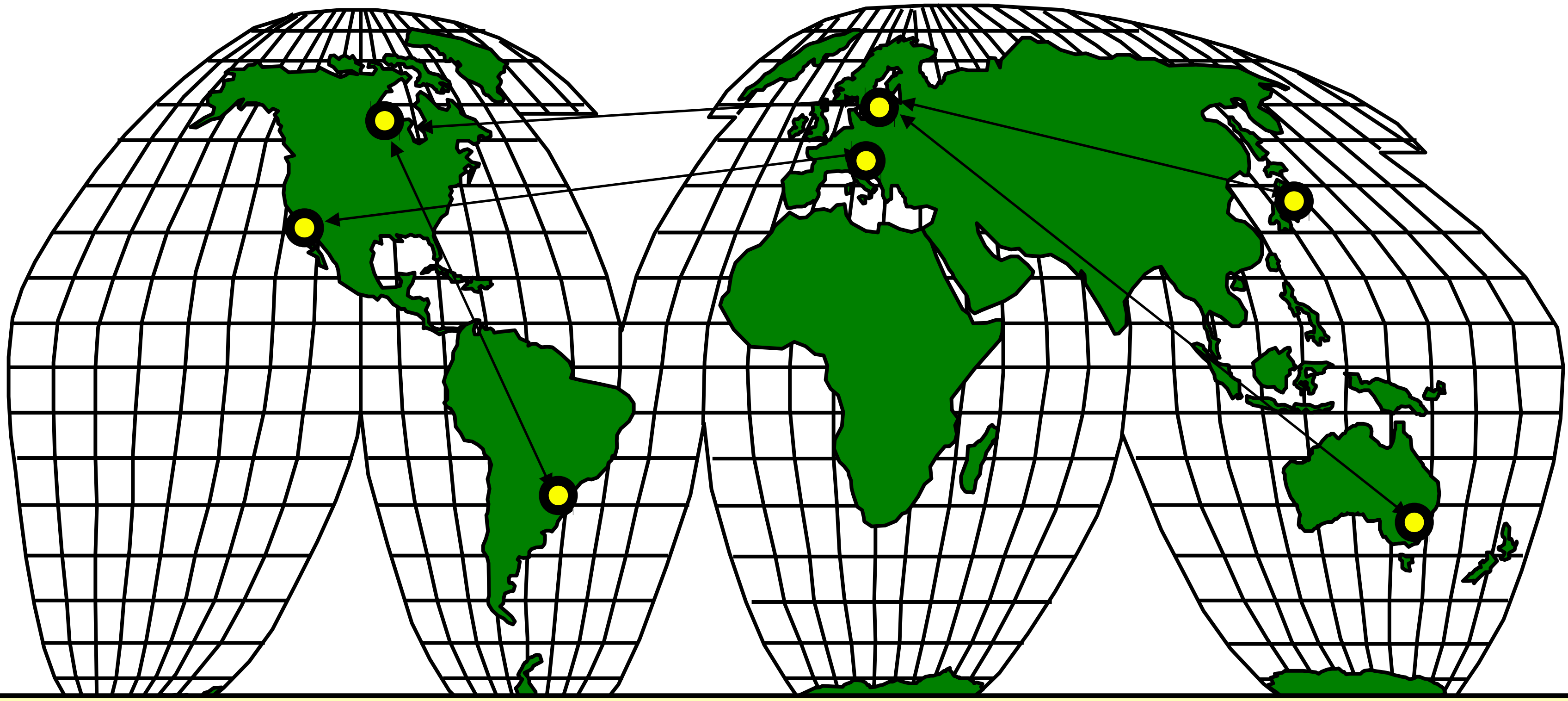
- Size and portability
  - Banks are large and unportable.
  - Storage of information can be very small and extremely portable. (So small that an entire corporations intellectual property can be stored on something the size of a postage stamp.)Ability to avoid physical contact
  - Banks: physical interaction with the bank and the loot is unavoidable or impossible to circumvent
  - Computers: require no physical contact to either gain access to, copy or remove data.
- Value of assets:
  - Bank: generally very high (or why would somebody bother to put it in a bank?)
  - Computers: Variable, from very low (useless) to very high.

Past Situation (Single Systems)



Physical security and control of access to computers

Current Situation (Int'l networks and open systems)



Authentication, message protection, authorization

Method, Opportunity and Motive

- Method: The skills knowledge and tools that enable the attack
- Opportunity: The time, access and circumstances that allow for the attack
- Motive: The reason why the perpetrator wants to commit the attack

The People Involved

Amateurs . . .
Crackers
Criminals
Regular users

Accidental access to unauthorized resources and execution of unauthorized operations (no harm to regular users)

The People Involved

Amateurs
Crackers . . .
Criminals
Regular users

Active attempts to access sensitive resources and to discover system vulnerabilities (minor inconveniences to regular users)

The People Involved

Amateurs
Crackers
Criminals . . .
Regular users

Active attempts to utilize weaknesses in protection system in order to steal or destroy resources (serious problems to regular users)

The People Involved

- Amateurs
- Crackers
- Criminals
- **Regular users . . .**

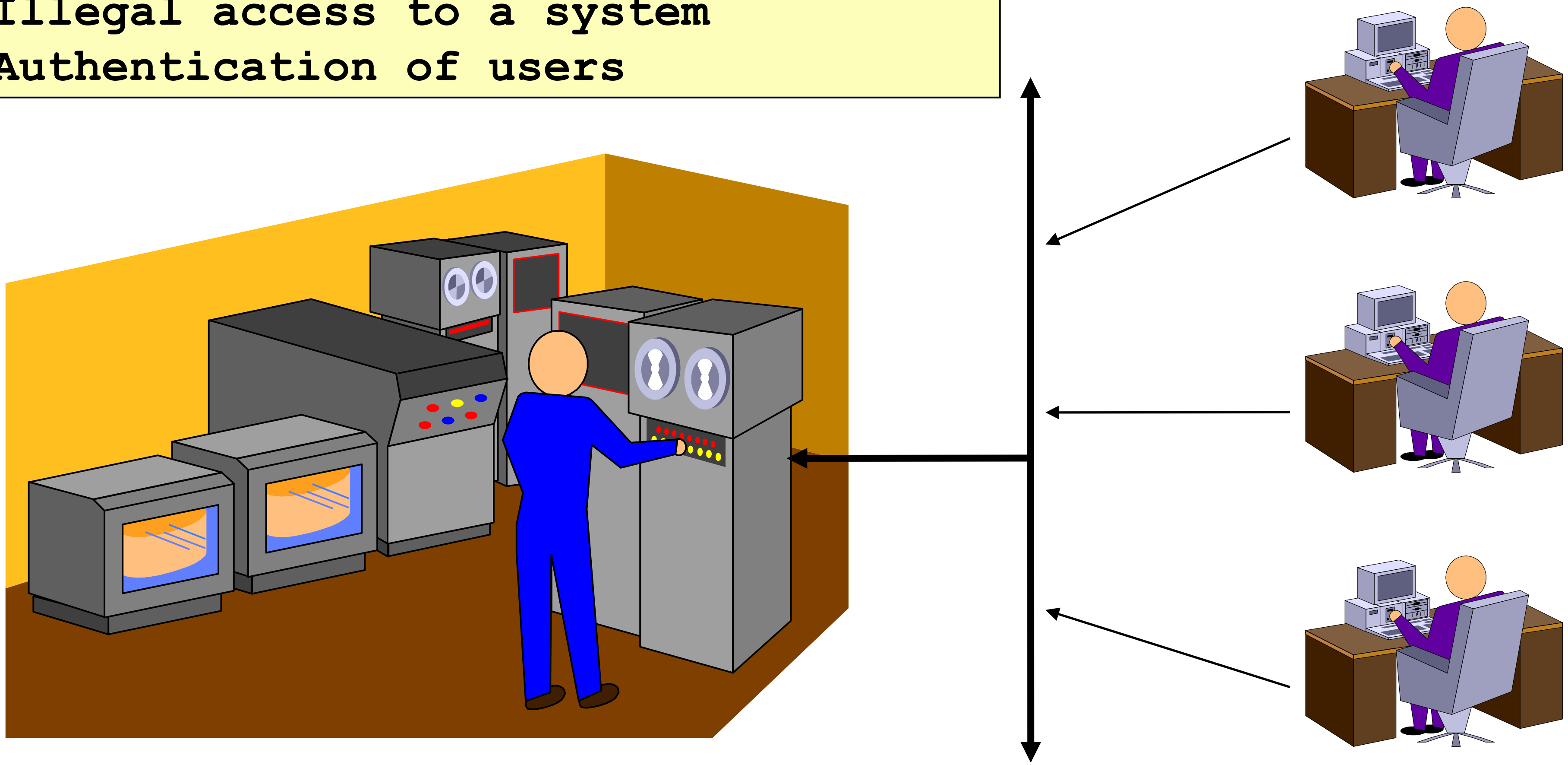
Special requirements: authentication in open networks, authorization, message integrity, non-repudiation, special transactions

Attack, Vulnerability,Control, Problems, Threats, and Risks

- Attack: A human exploitation of a vulnerability.
- Vulnerability: A weakness in the security system.
- Control: A protective measure. An action, device or measure taken that removes, reduces or neutralizes a vulnerability.
- Problems : Consequences of unintentional accidental errors
- Threat: a set of circumstances that has the potential to cause loss or harm.
- Risks : Probabilities that some threat or problem will occur due to system vulnerabilities

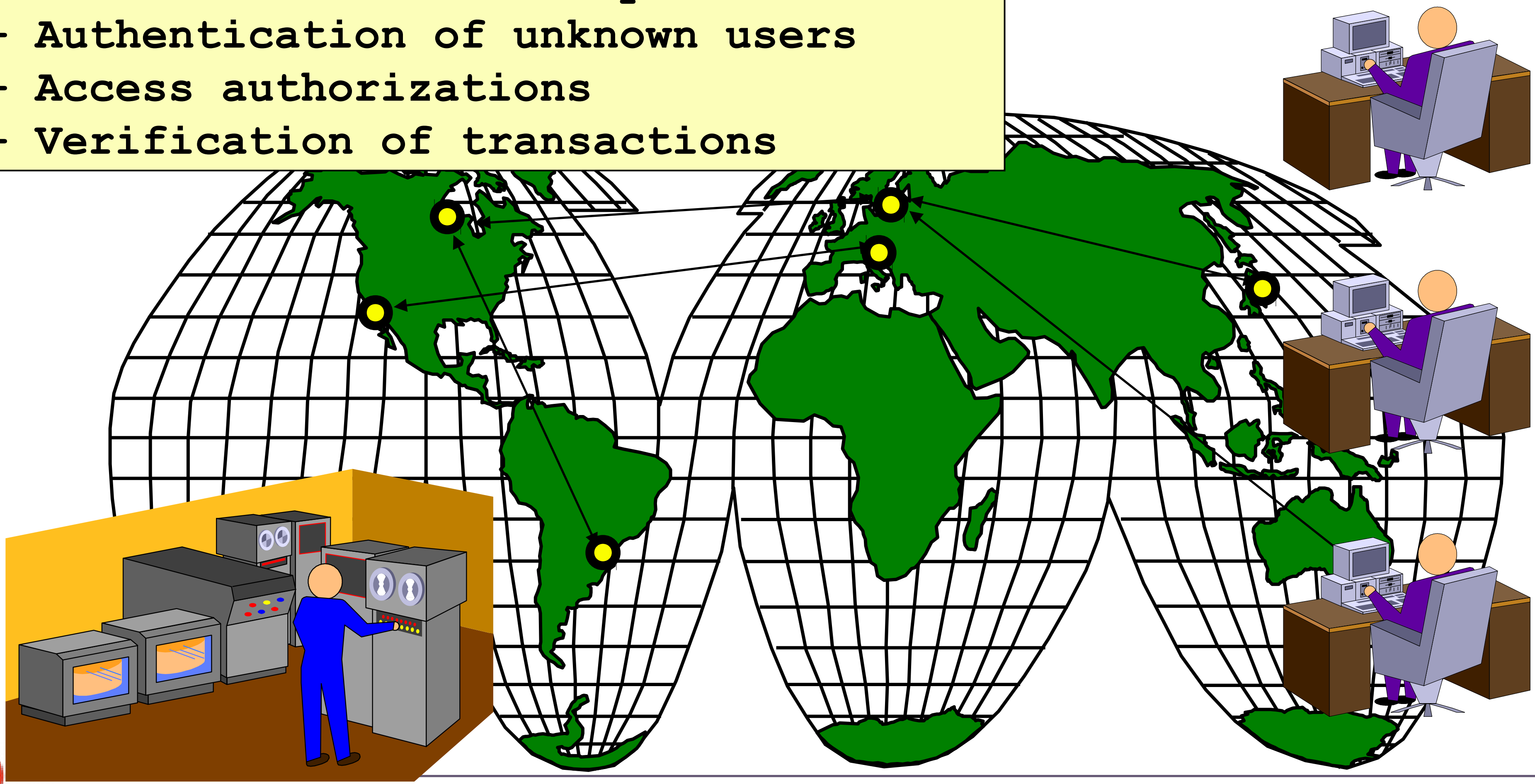
Threats with a single system

- Illegal access to a system
- Authentication of users



Threats with international networks

- Communications security
- Authentication of unknown users
- Access authorizations
- Verification of transactions



So what does computer security concern itself with?

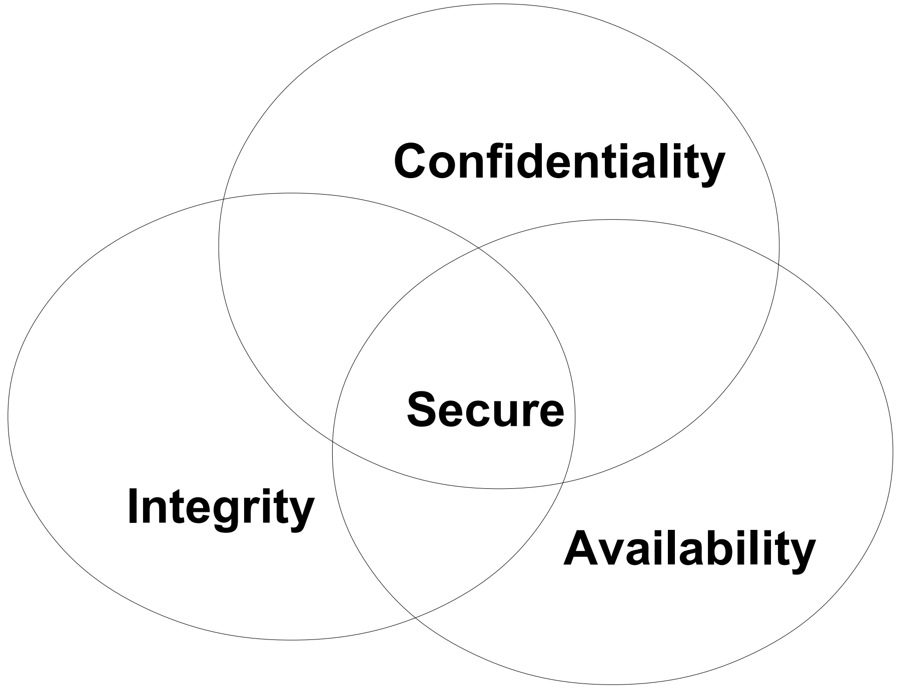
- The entire system:
  - Hardware
  - Software
  - Storage media
  - Data
  - Memory
  - People
  - Organizations
  - Communications

Security Goals (Requirements)

- What makes a "secure" system?
  - Financial "Security" requirements
  - Home "security"
  - Physical "security"
  - Information "security"
- All these concepts of security have different requirements. We are, of course, interested mostly on computer security; which requires three items:

Presence of all three

- The presence of all three things yields a secure system:



Thing one:

- Confidentiality:

  Computer related assets are only available to authorized parties. Only those that should have access to something will actually get that access.

  - "Access" isn't limited to reading. But also to viewing, printing or...
  - Simply even knowing that the particular asset exists (steganography)

  – Straight forward concept but very hard to implement.

Thing two:

- Integrity

  Can mean many things: Something has integrity if it is:

  - Precise
  - Accurate
  - Unmodified
  - Consistent
  - Meaningful and usable

Integrity

- Three important aspects towards providing computer related integrity:
  - Authorized actions
  - Seperation and protection of resources
  - Error detection and correction.
- Again, rather hard to implement; usually done so through rigorous control of who or what can have access to data and in what ways.

Thing three:

- Availability
  - There is a timely response to our requests
  - There is a fair allocation of resources (no starvation)
  - Reliability (software and hardware failures lead to graceful cessation of services and not an abrupt crash)
  - Service can be used easily and in the manner it was intended to be used.
  - Controlled concurrency, support for simultaneous access with proper deadlock and access management.

Principles of Computer Security

Confidentiality . . .

Integrity

Availability

Functionality

Threats to Data and Programs:
illegal read, illegal access, data (files) deletion, illegal users, criminal acts, sabotage, etc.

Principles of Computer Security

Confidentiality
Integrity . . .
Availability
Functionality

Threats to software and data: technical errors, software errors, processing errors, transmission correctness, etc.

Principles of Computer Security

Confidentiality
Integrity
Availability . . .
Functionality

Requirements for:
timely response, fair allocation, fault tolerance, usability, controlled concurrency

Principles of Computer Security

Confidentiality	
Integrity	
Availability	
Functionality . . .	**New functions needed for electronic data transactions: authentication, digital signature, confidentiality, and others**

“Definition” of Information Security

Information security
are methods and technologies
for protection, integrity, availability,
authenticity and extended functionality
of computer programs and data

Protection Methods

- **Encryption**
- **SW & HW Controls**
- **Policies**
- **Physical controls**

Protection Methods

Encryption . . .

SW & HW Controls

Policies

Physical controls

Effective for:
confidentiality,
users and messages
authentication, access
control

Protection Methods

Encryption

SW & HW Controls

Policies

Physical controls

Available methods: software and hardware controls (internal SW, OS controls, development controls, special HW devices)

Protection Methods

Encryption

SW & HW Controls

Policies . . .

Physical controls

Precise specifications:
special procedures,
security methods,
security parameters,
organizational issues

Protection Methods

Encryption

SW & HW Controls

Policies

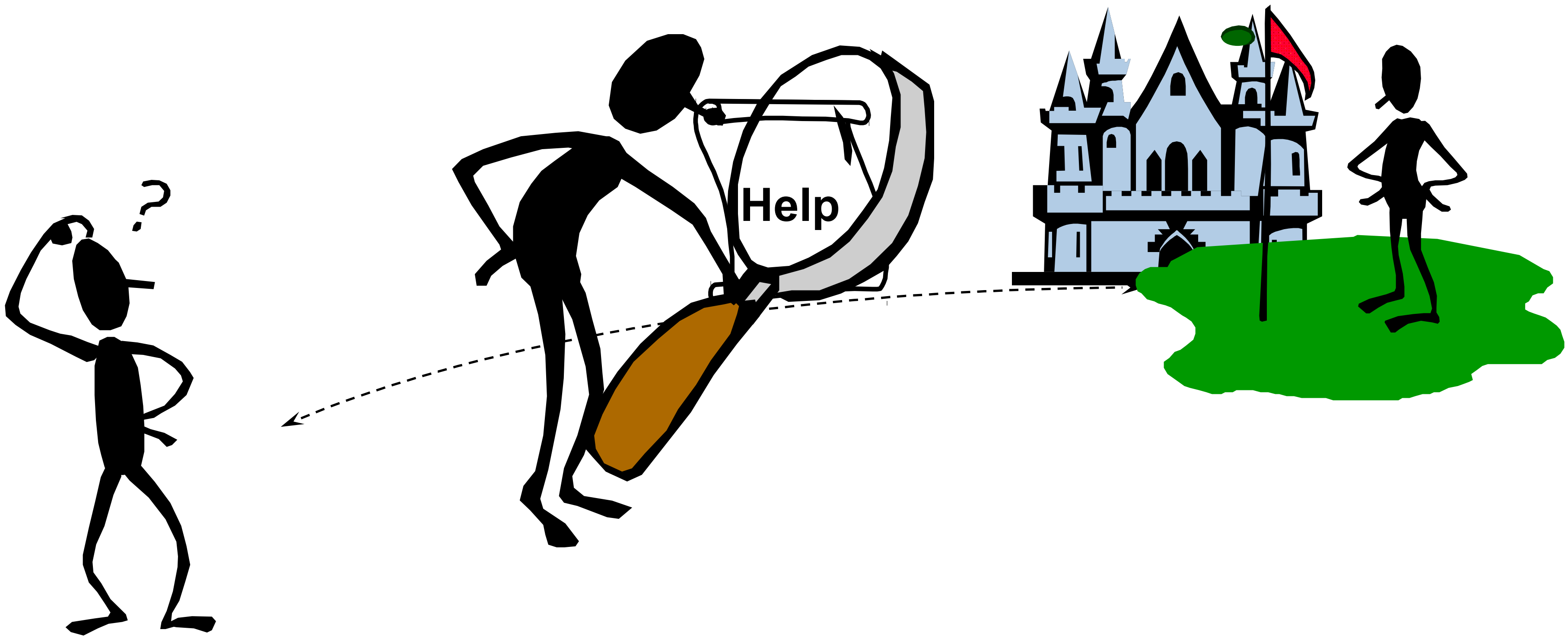
Physical controls

Measures for:
isolation of equipment,
access to equipment,
authorization for personnel,
backup and archiving

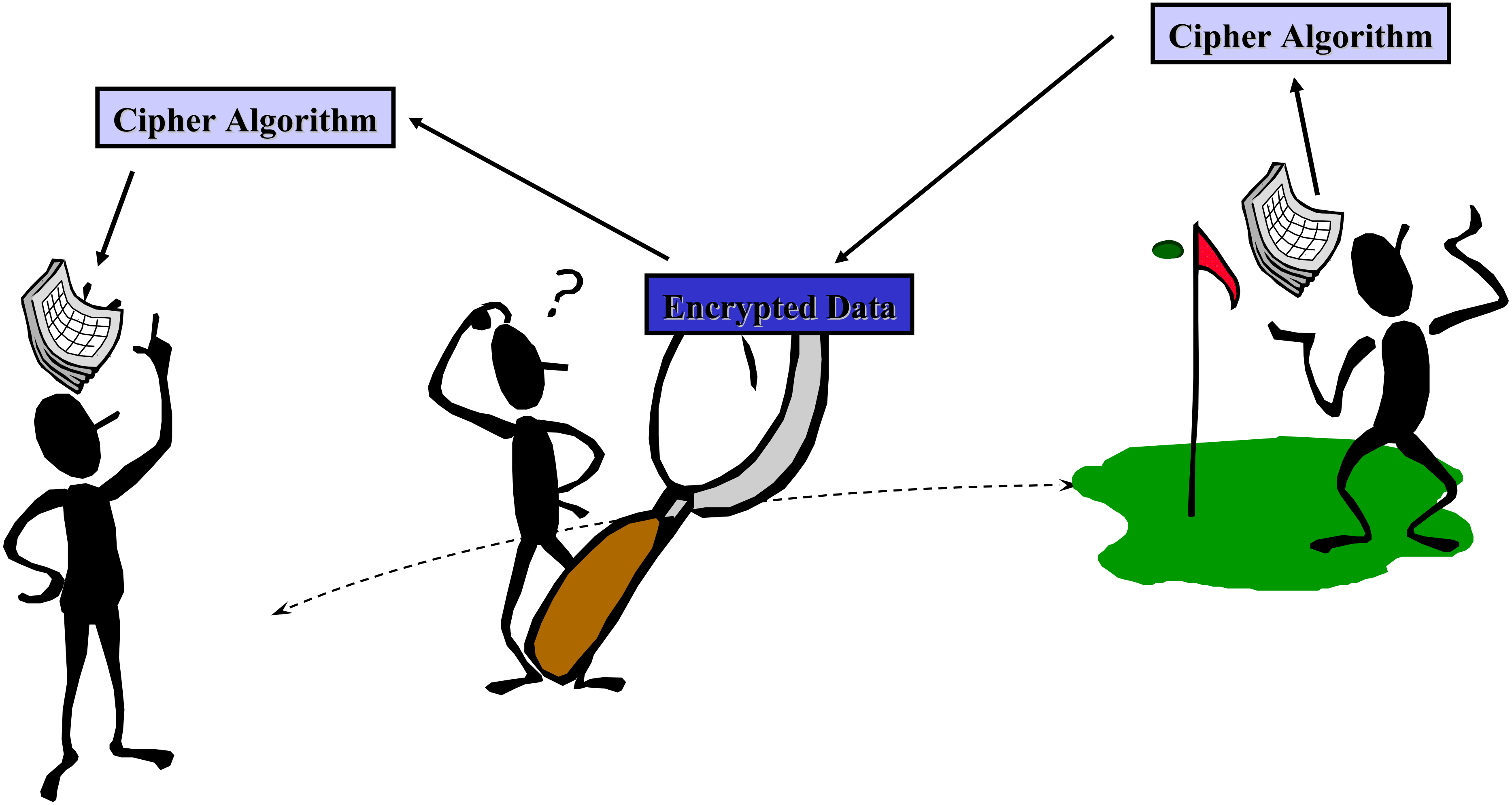
Objectives - Cryptography

The Cryptography domain addresses the <u>principles</u>, <u>means</u>, and <u>methods of disguising information</u> to ensure its integrity, confidentiality, authenticity and non-repudiation(?).

Requirement



Basic Concept



What You Should Know

- Basic concepts and terms within cryptography
  - Public and private key algorithms in terms of their applications and uses
  - Cryptography algorithm construction, key distribution, key management, and methods of attack
  - Applications, construction, and use of digital signatures
  - Principles of authenticity of electronic transactions and non-repudiation

Definitions

- **Cryptography**
  - Art or science of secret writing
  - Protects sensitive information from disclosure
  - Storing and transmitting information in a form that allows it to be revealed only to those intended
  - Cryptosystem accomplishes this
  - Identifies the corruption or unauthorized change of information
  - Designed to make compromise too expensive or too time-consuming

- **Cryptanalysis**
  - art/science relating to converting ciphertext to plaintext without the (secret) key
  - **d**escrambling without secret key ; art of breaking ciphers
  - Practice of defeating such attempts to hide info

- **Cryptology**
  - Includes both cryptography and cryptanalysis

Cryptography Basic

- **Why Encrypt?**
  - Protect stored information
  - Protect information in transmission
- Cryptography originally used for secrecy
- **Encryption** - process by which **plaintext** is converted to **ciphertext** using a **key**
- **Decryption** - process by which ciphertext is converted to plaintext (with the appropriate key)
- **plaintext** (cleartext)- intelligible data

The goal of a cryptosystem

- **The goal of a cryptosystem is to provide**
- **Confidentiality** To ensure that unauthorized parties cannot access the data, message or information
- **Authenticity** To ensure that the source / sender of the data, message or information is identifiable
- **Integrity** To ensure that the data. Message or Information was not modified during transmission
- **Nonrepudiation** To ensure that either party cannot deny sending or receiving the data, message or information

Cryptography History

- **Historic examples...**
  - Earliest cryptography: an Egyptian scribe using non-standard hieroglyphics
  - Julius Caesar ("Caesar Cipher")
    Each plaintext letter is replaced by a letter some fixed number of positions further down the alphabet (e.g. Belgica (3 positions) → ehojlfd)
  - The Kama Sutra recommends cryptography as 44th and 45th art
    (of 64) men and women should know

Cryptography History

- ENIGMA Used by the Germans in WW2 – and the subsequent
  code-breaking activities at Bletchley park
  (still a popular subject of books and movies)
- 1976: Public Key Cryptography concept
  (Whitfield Diffie & Martin Hellman)
- 1977: first (*published*) practical PKC cryptosystem invented
  (RSA - Rivest, Shamir, Adleman)
- October 2000 Rijndael is chosen as AES
  (Advanced Encryption Standard)

The Caesar Cipher

Plain Text : 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

Cipher Text : 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

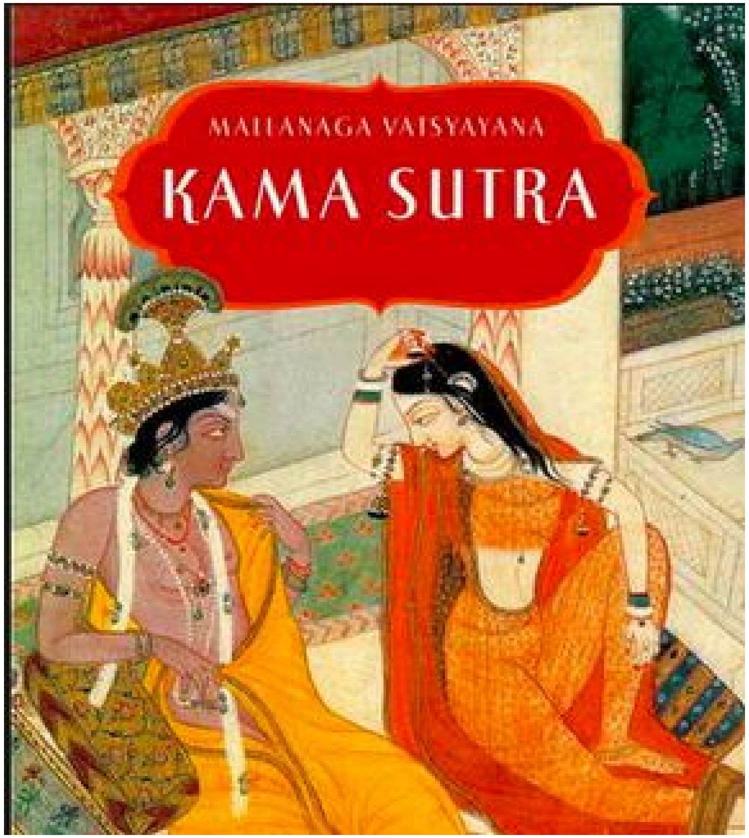
$$C_i = E(P_i) = P_i + 3$$

Kamasutra

One of the earliest descriptions of encryption by substitution appears in the Kama-sutra, a text written in the 4th century AD by the Brahmin scholar Vatsyayana, but based on manuscripts dating back to the 4th century BC.

How it work

The kamasutra generate list of 26 alphabet with no duplicate. Then divide by 2 row. Find for each letter of message text in table and choose the opposite of the letter



kamasutra

for example:

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

divide by 2 rows

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

Given String = KAMASUTRA

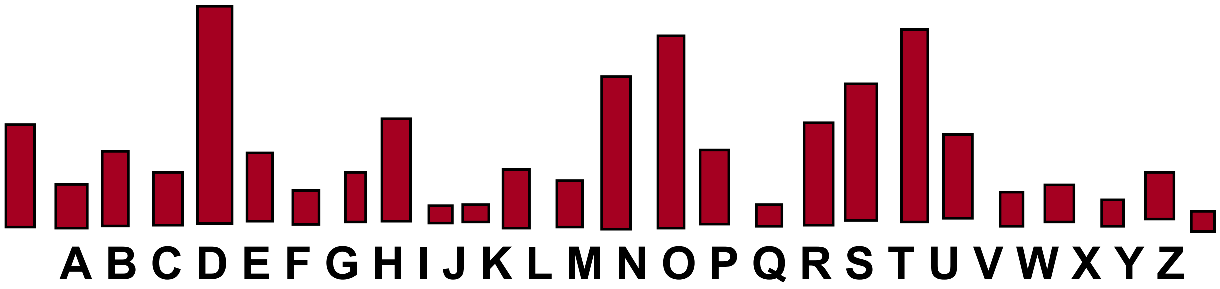
K is at 2nd row and 5th column. Get the opposite of K that is I. Do each letter until the end

Cipher : IZOZNQJYZ

Monoalphabetic Substitutions

Plain Text	**: 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**
Cipher Text	**: K E Y G H I J K L M N O P Q R S T U V W X Y Z A B C**

<u>Letter Frequency</u>



Polyalalphaberic Substitutions

Table for Odd Positions

Plain Text : 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

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

Table for Even Positions

Plain Text : 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

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

Plain Text : SSIBL

Cipher Text : czysh

Transposition (Permutation) Substitutions

<u>Columnar Transposition</u>

c1	c2	c3	c4	c5
c6	c7	c8	c9	c10
c11	c12	etc.		

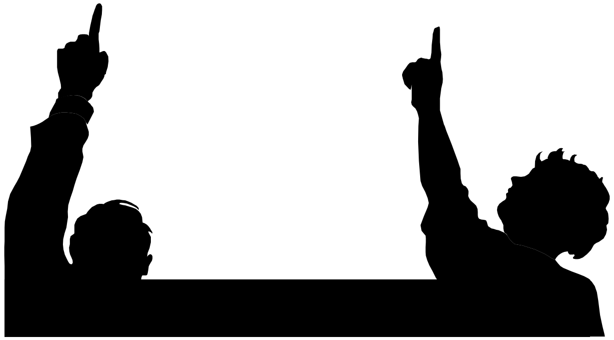
<u>Cipher text formed by</u> → **c1 c6 c11 c2 c7 c12 c3 c8 ...**

c1	c2	c3	c4	c5
c6	c7	c8	c9	c10
c11	c12	etc.		

The Perfect Substitutions Cipher

One Time Pad

- **Recipient need identical pad**
- **Pad position should be synchronized**
- **Plain text length = Key length**



The Vernam Cipher

Plain Text : 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

=Mod 26 : 19 0 7 17 18 15 8 19 23 12 0 1

Cipher text : t a h r s p l t x m a b

Binary Vernam Cipher

Plain Text : 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1

$\oplus$ Random Stream : 0 1 0 1 1 0 1 0 1 1 1 0 1 0 1

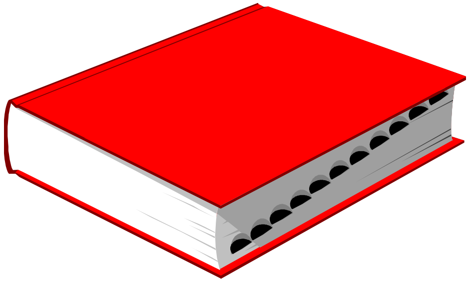
Cipher text : 1 1 1 1 1 0 0 1 0 1 1 1 0 0 0

The One-Time Pas

- If a truly random key as long as the message is used, the cipher will be secure
- Called a **One-Time pad**
- Has unconditional security:
- ciphertext bears no statistical relationship to the plaintext since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- Can only use the key **once**
- Have problem of safe distribution of key

Random Numbers

<u>1. Truly Random numbers</u>



- **Books**
- **CD**

<u>2. Pseudo Random numbers</u>

- **Linear congruential random number generation**

$$\boxed{R_{i+1} = (a * R_i + b) \bmod n}$$

Encipherment Modes

- Stream Ciphers - Message broken into characters or bits and enciphered with a “key stream”
  - key stream - should be random and generated independently of the message stream
- Block ciphers process messages in blocks, each of which is then en/decrypted

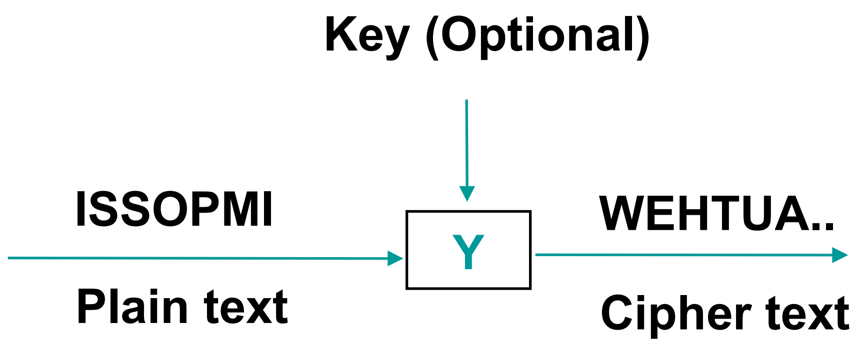
Stream Cipher

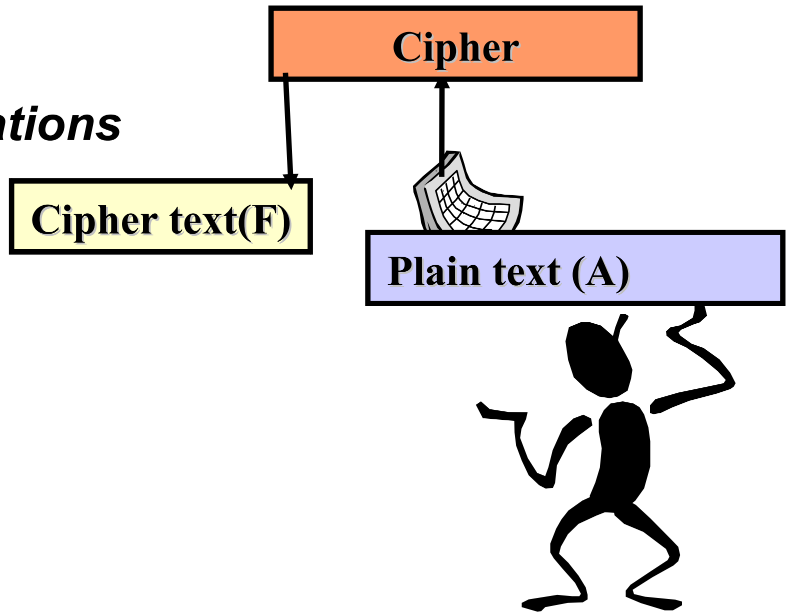
Advantage

- *Speed of transformation*
- *Low error propagation*

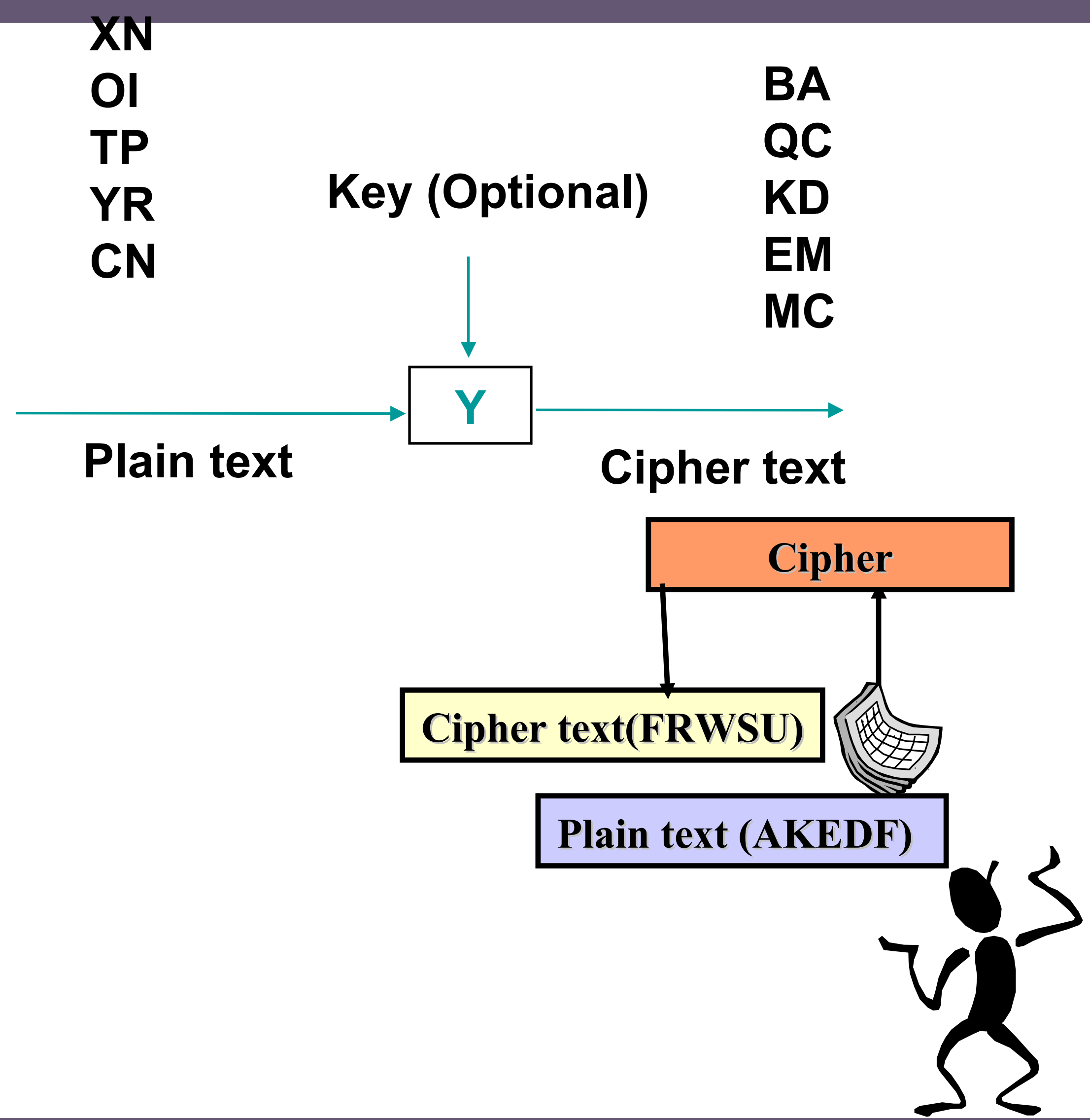
Disadvantage

- *Low diffusion*
- *Susceptibility to malicious insertion and modifications*





Block Cipher



Disadvantage

- *Slowness of encryption*
- *Error propagation*

Advantage

- *Diffusion*
- *Immunity to insertion*

Characteristic of “GOOD” Cipher

<u>Shannon Characteristics - 1949</u>

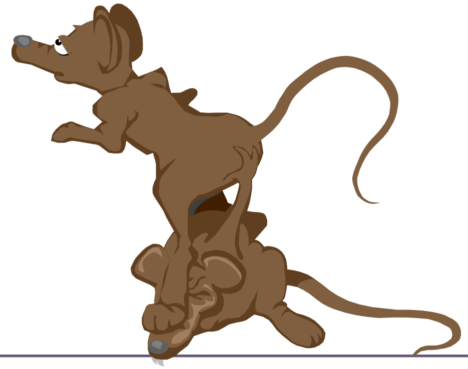
- **The amount of secrecy needed should determine the amount of labor appropriate for encryption and decryption**

- **The set of keys and the encryption algorithm should be free from complexity**

- **The implementation of the process should be as simple as possible**

- **Errors in the ciphering should not propagate and cause corruption of further information in the message**

- **The size of enciphered text should be no larger than the text of the original message**



Kerckhoff’s Principle

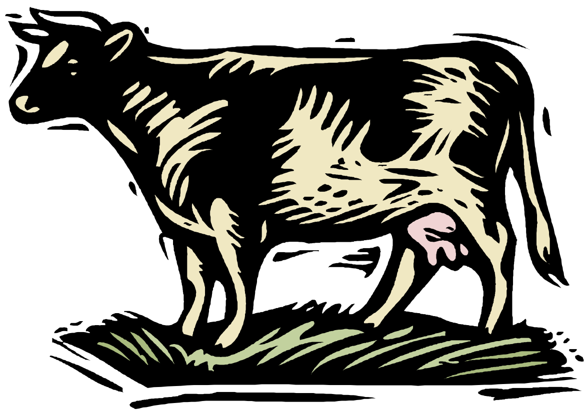
The security of the encryption scheme must depend only on *the secrecy of the key and not on the secrecy of the algorithms.*

Reasons:

- Algorithms are difficult to change
- Cannot design an algorithm for every pair of users
- Expert review
- No security through obscurity!

Confusion and Diffusion

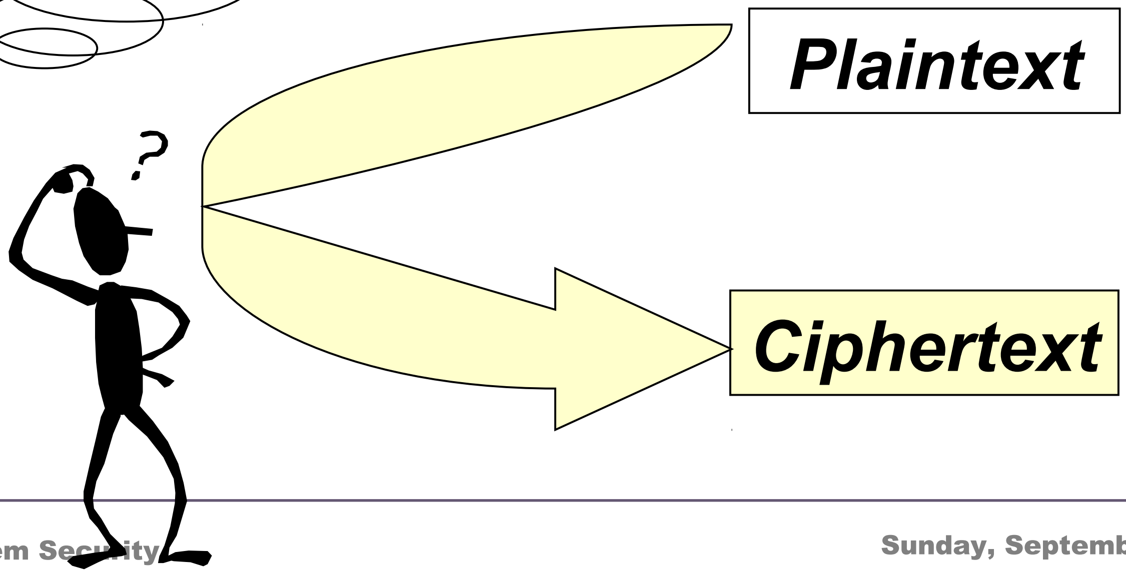
Goal: cipher needs to completely obscure statistical properties of original plaintext (like a one time pad)



Confusion

Confusion

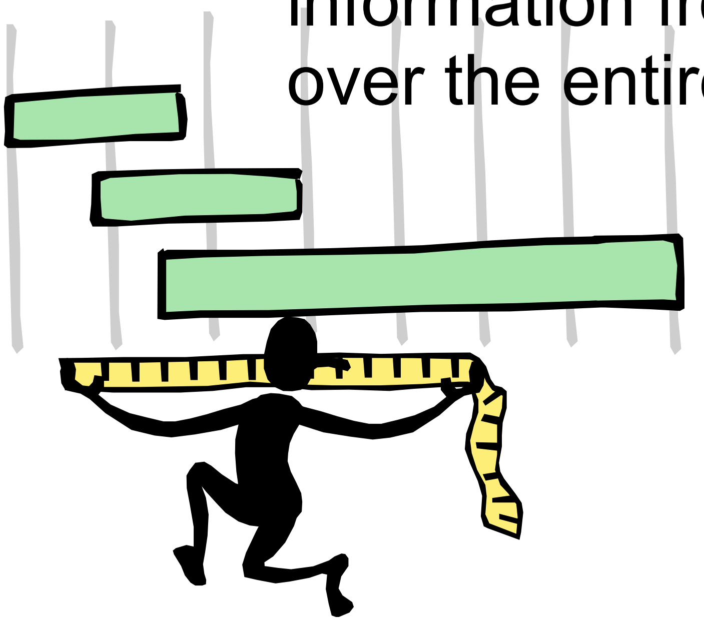
The interceptor should not be able to predict what changing one character in the plaintext will do to the ciphertext

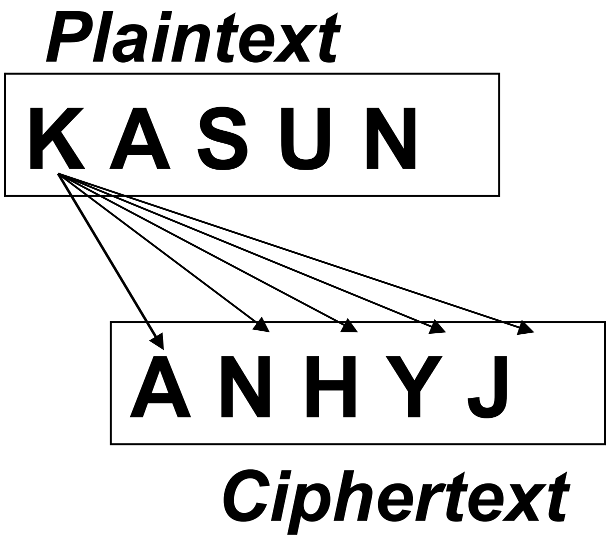


Diffusion

Diffusion

The characteristics of distributing the information from single plaintext letter over the entire ciphertext

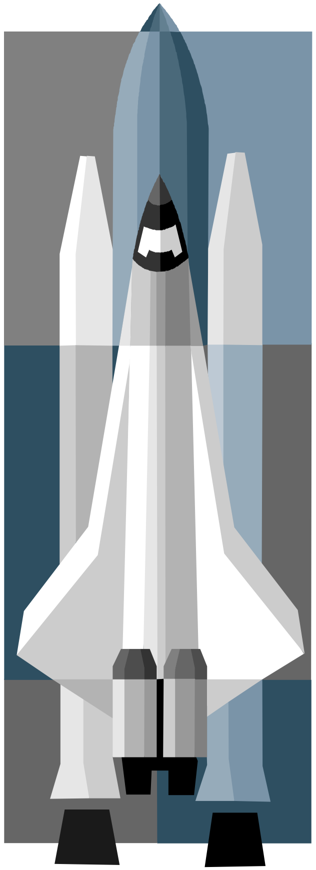




Brute Force Search

- **Always possible to simply try every key**
- **Most basic attack, proportional to key size**
- **Assume either know/recognize plaintext**

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/µs
32	$2^{32} = 4.3 \times 10^{9}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years



http://password-checker.online-domain-tools.com

password-checker.online-domain-tools.com

Inbox (219) - kasun.de.zoysa@gmail.com - Gmail | Course: SCS3106/CS3106 Information System Se... | Password Checker - E

Password: ••••••••••

Strength: 47%

Evaluation: Medium

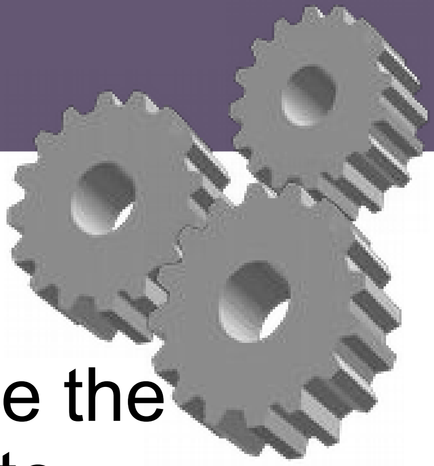
Password properties

Property	Value	Comment
Password length:	8	MEDIUM LONG
Numbers:	1	USED
Letters:	6	USED
Uppercase Letters:	1	USED
Lowercase Letters:	5	USED
Symbols	1	USED
Charset size	94	HIGH (a-z, 0-9, symbols, A-Z)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 2 years
Fast Desktop PC	About 6 months
GPU	About 2 months
Fast GPU	About 1 month
Parallel GPUs	About 4 days
Medium size botnet	About 1 minute

Unconditional/Computational Security



Unconditional security
no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

Computational security
given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

Sec_rity is not Complete without U

You, as a Computer User, have to make your contribution to computer security: **You are responsible for the security and protection** of your computers, the operating systems you run, the application you install, the software you program, the data you own - and the services and systems you manage.

Discussion