Practical Cryptography

(Introduction to Cryptography)

Kasun De Zoysa

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

Definitions

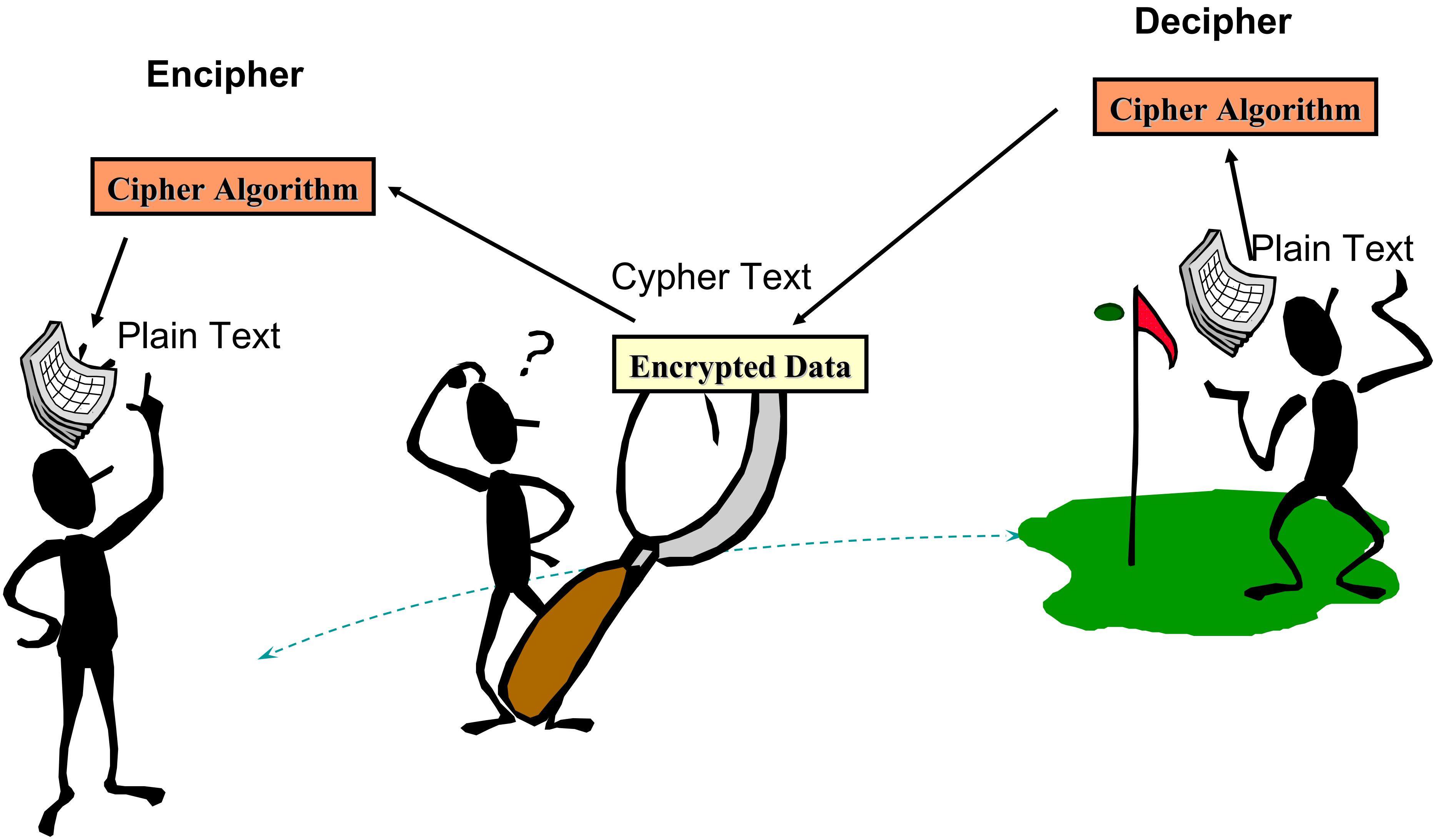
- **Cryptography**
  - Art or science of secret writing
  - Protects sensitive information from disclosure
  - Storing and transmitting information in a form that allows it to be revealed only to those intended
  - Cryptosystem accomplishes this
  - Identifies the corruption or unauthorized change of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

Objectives - Cryptography

The Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, authenticity and non-repudiation.

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



Encipher

Cipher Algorithm

Plain Text

Cypher Text

Encrypted Data

Decipher

Cipher Algorithm

Plain Text

Definitions , continued

- **Encipher**
  - act of scrambling
- **Decipher**
  - descrambling with secret key
- **Key**
  - secret sequence governing en/deciphering

- **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

Cryptography Basics

- Kerckhoffs' principle (19th century) a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
  (Opposite of “*security through obscurity*”)
- Symmetric Key Encryption Scheme
  - Each of the parties involved has to know the secret key
- Public Key Cryptography (Asymmetric)
  - Each of the parties own two keys, a private key and a public key
  - The private key must be kept secret
  - The public key can be freely distributed

Cryptography Business Use

:

- Prevent unauthorized disclosure of information
- Prevent unauthorized access to information, computers, web sites, applications,etc.
- Detect tampering
- Detect injection of false data
- Detect deletion of data
- Prevent repudiation

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

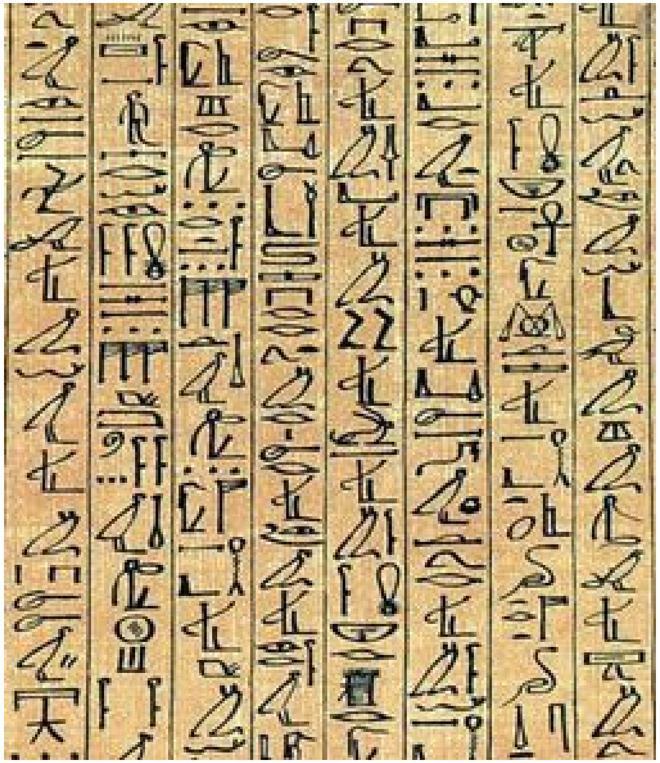
- **Historic examples...**
  - Earliest cryptography: an Egyptian scribe using non-standard hieroglyphics
  - Julius Caesar ("Caesar Cipher") Each plaintext letter is replaced by a letter some fixed number of positions further down the alphabet
  - The Kama Sutra recommends cryptography as 44th and 45th art (of 64) men and women should know
  - One-Time Pad (OTP) first described by Frank Miller in 1882 and Gilbert Vernam for the XOR operation in 1917.

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)

Hieroglyphs

The earliest known use of cryptography is found in non-standard hieroglyphs carved into the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC.



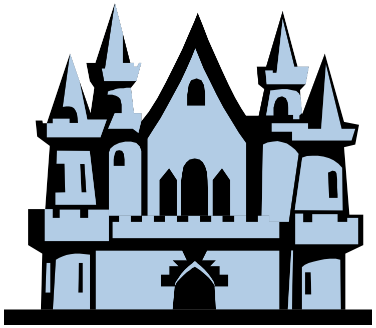
These are not thought to be serious attempts at secret communications, however, but rather to have been attempts at mystery, intrigue, or even amusement for literate onlookers [Wikipedia].

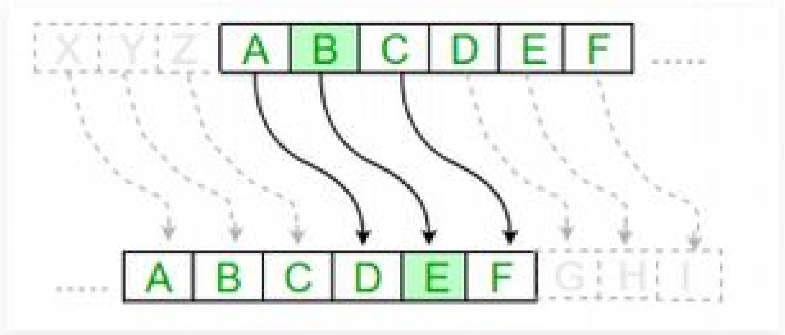
The Caesar Cipher

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

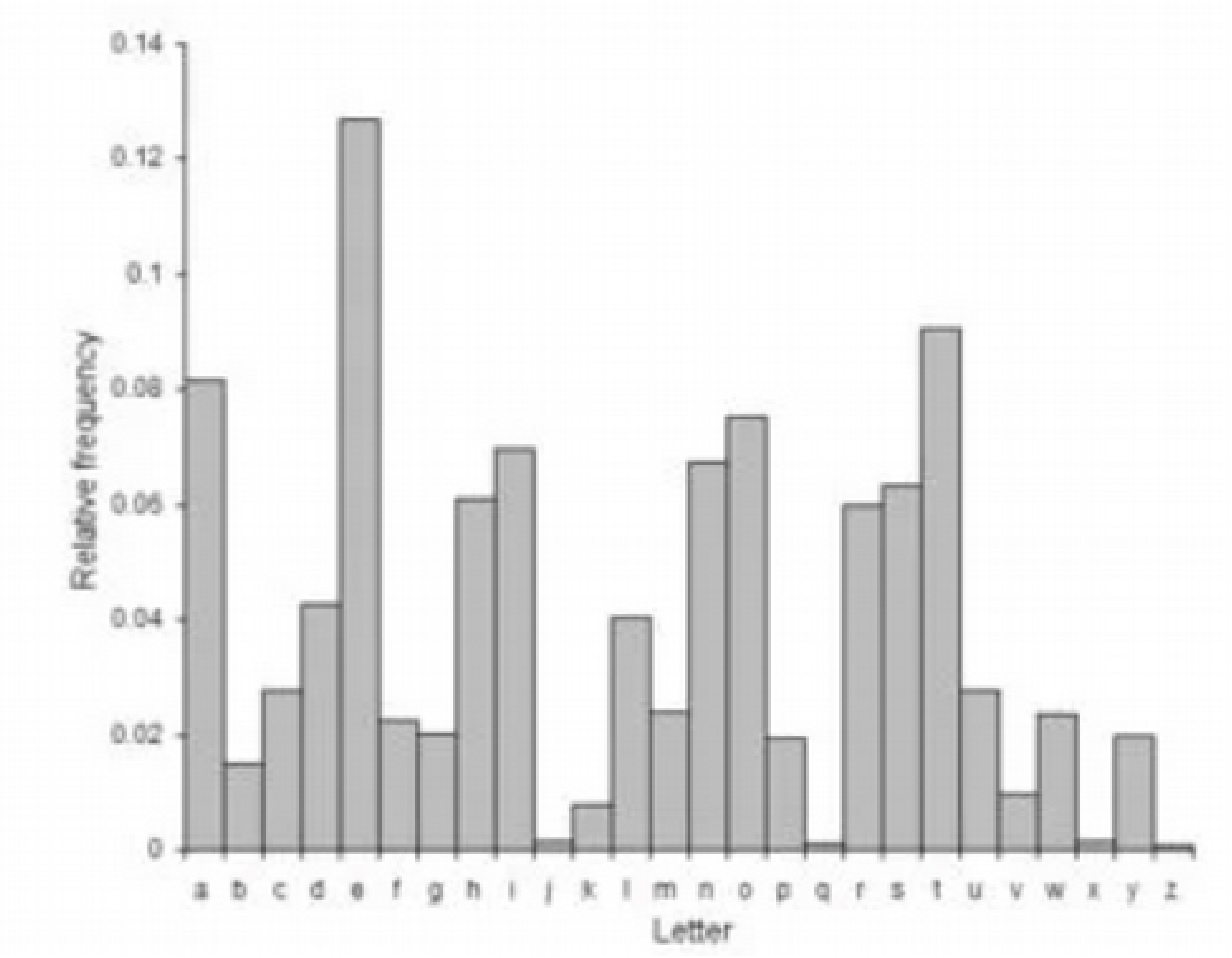
Cipher : IZOZNQJYZ

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

Letter Frequency



Polyalalphabetic 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

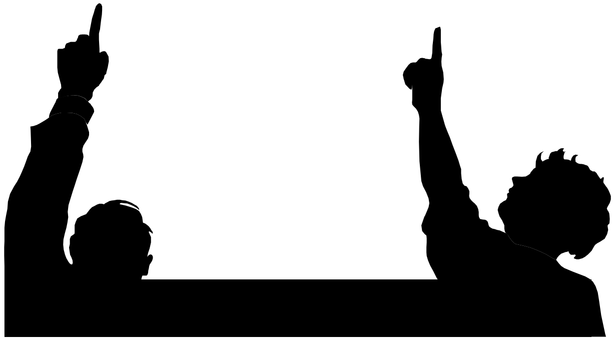
One Time Pad / Vernam Cipher

- Invented in 1917 by Gilbert Vernam and Joseph Mauborgne.
- Usually implemented as a stream cipher using the XOR function.
- Key is used once and discarded by both sender and receiver.
- Length of the Key character stream is equal to the message length.
- Not practical for large amounts of data (MB / GB).
- Pad is theoretically unbreakable by exhaustive brute force.
- Implementation uses a Key that consists of a set of random
- non-repeating characters.
- Each Key letter and Plaintext are added modulo 26 to each other and then converted back into a letter.

One - Time Pad

- Two identical pads (keys), one with sender, one with recipient
- The random pads (keys) are the same length as the message
- Unbreakable by exhaustive search
- Relies on physical security of the pads
- Pads can only be used once

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



One Time Pad / 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

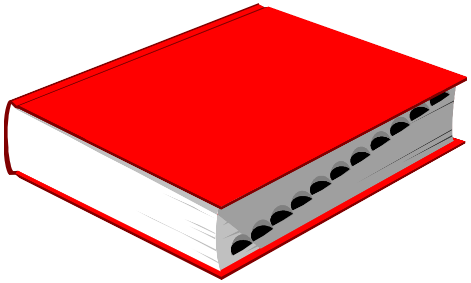
Plain Text : 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1

⊕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

Random Numbers

1. Truly Random numbers



- Books
- CD

2. Pseudo Random numbers

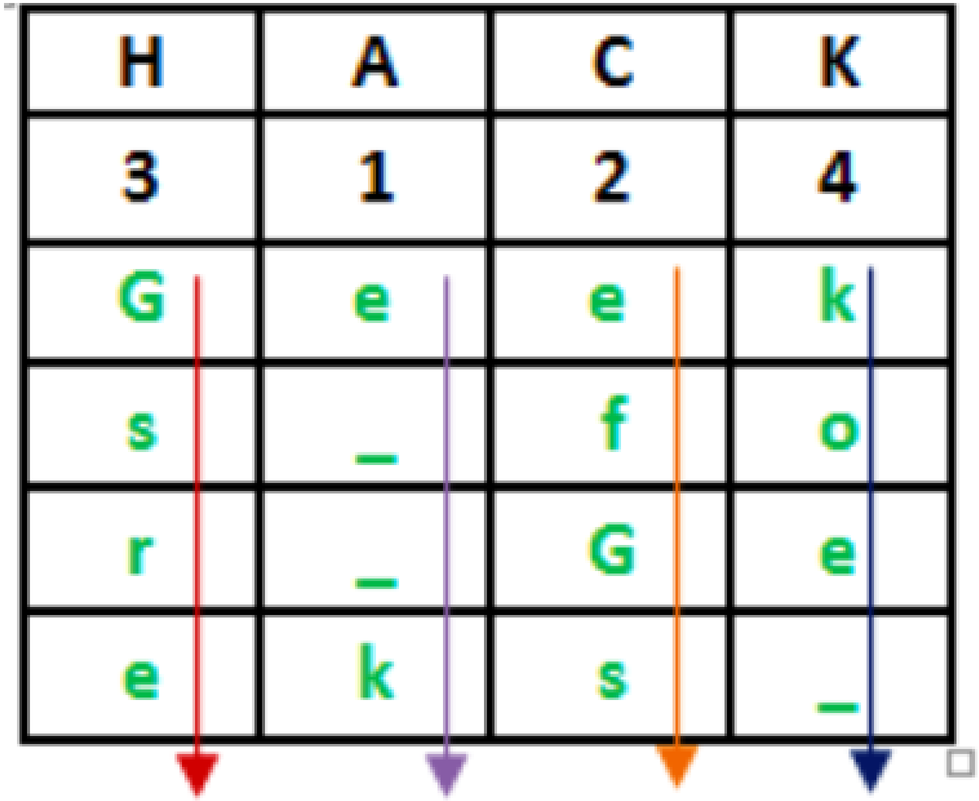
- Linear congruential random number generation

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

Columnar Transposition Cipher

Plain tex = Geeks for Geeks
Key = HACK

Length of Key = 4 (no of rows)
Order of Alphabets in HACK = 3124



H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

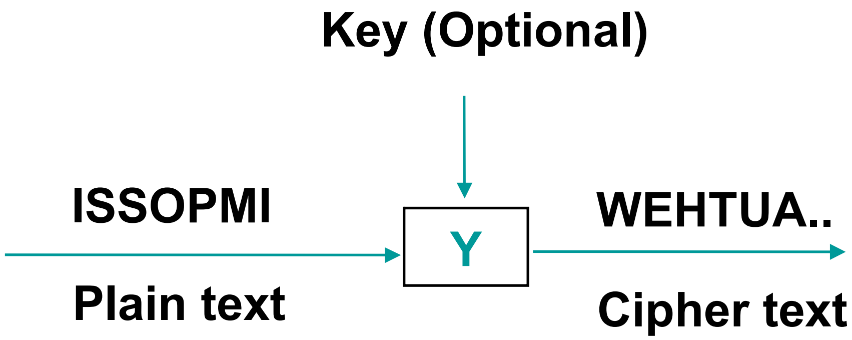
Cypher text = e__kefGsGsrekoe_

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



Key (Optional)

ISSOPMI

Y

WEHTUA..

Plain text

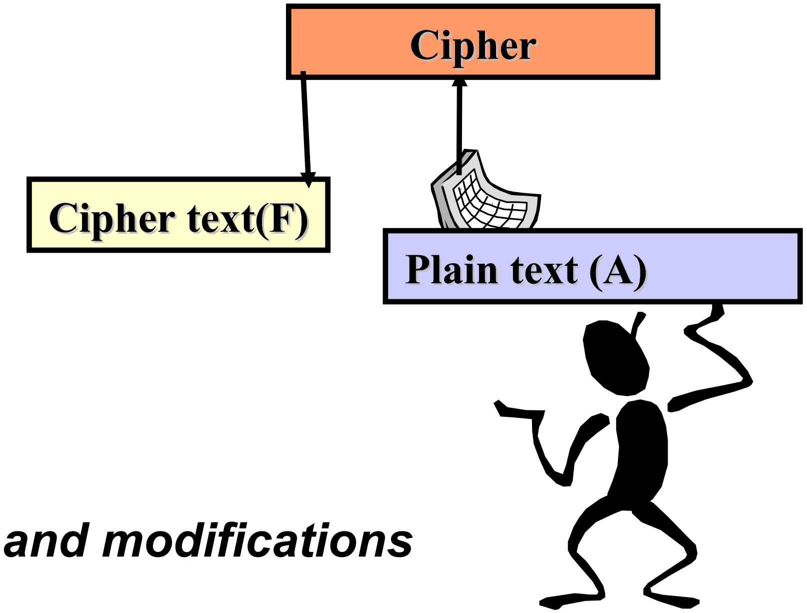
Cipher text

Advantage

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

Disadvantage

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

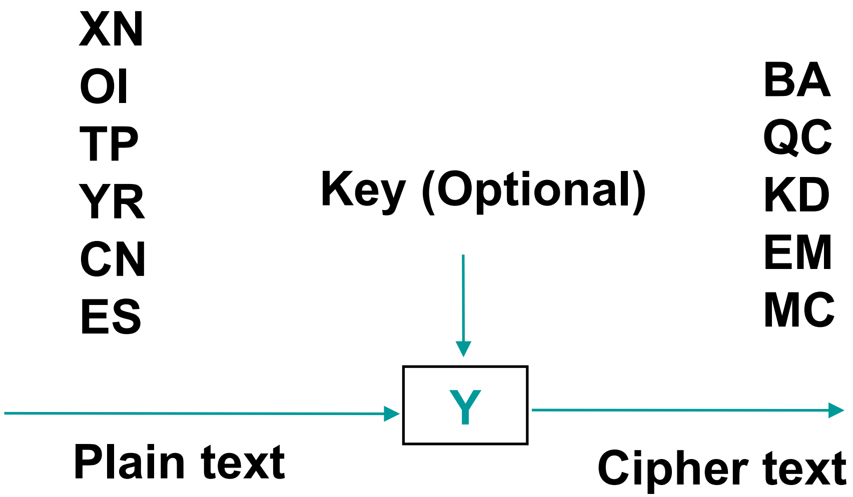


Cipher

Cipher text(F)

Plain text (A)

Block Cipher



XN
OI
TP
YR
CN
ES

Key (Optional)

BA
QC
KD
EM
MC

Y

Plain text

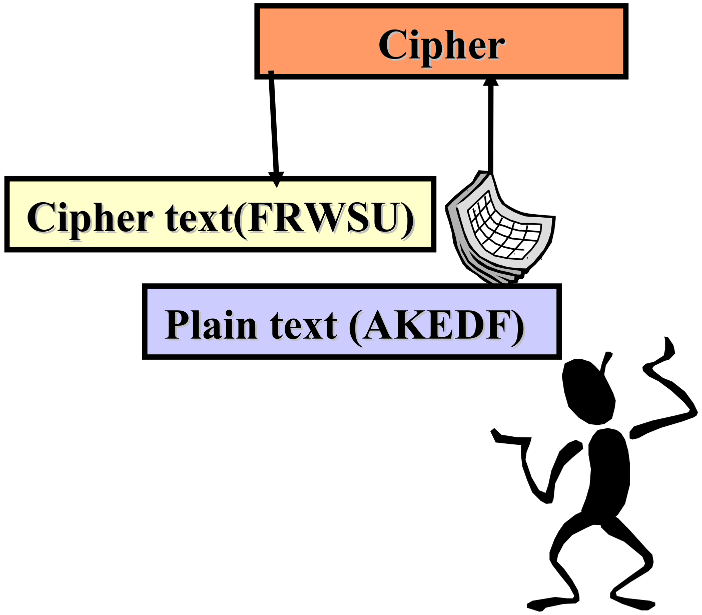
Cipher text

Disadvantage

- *Slowness of encryption*
- *Error propagation*

Advantage

- *Diffusion*
- *Immunity to insertion*



Cipher

Cipher text(FRWSU)

Plain text (AKEDF)

Block vs Stream Ciphers

- Block ciphers process messages in blocks, each of which is then en/decrypted
- Like a substitution on blocks of characters
  - 64-bits or more

- Stream ciphers process messages a bit or byte at a time when en/decrypting
- E.g. Vernam cipher, one time pad

- Many current ciphers are block ciphers

Secrecy Requirements

- If ciphertext and plaintext are known, it should be computationally infeasible to determine the deciphering algorithm
- It should be computationally infeasible to systematically determine plaintext from intercepted ciphertext (Even if you decrypt ciphertext once, it should require the same amount of work to do it again.)
- Note: **“systematically”** allows for a lucky guess
- Note: “**Computationally infeasible”** means great effort, doesn’t account for advances in computing, mathematics

Characteristic of “Good” Cipher - Shannon Characteristics - 1949

1. The amount of secrecy needed should determine the amount of labor appropriate for encryption and decryption
2. The set of keys and the encryption algorithm should be free from complexity
3. The implementation of the process should be as simple as possible
4. Errors in the ciphering should not propagate and cause corruption of further information in the message
5. The size of enciphered text should be no larger than the text of the original message

Kerckhoff's Principle

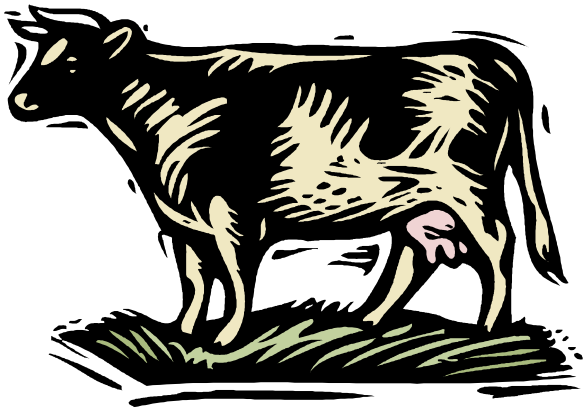
The security of the encryption scheme must depend only on *the secrecy of the key and not on the secrecy of the algorithms.*

Reasons:

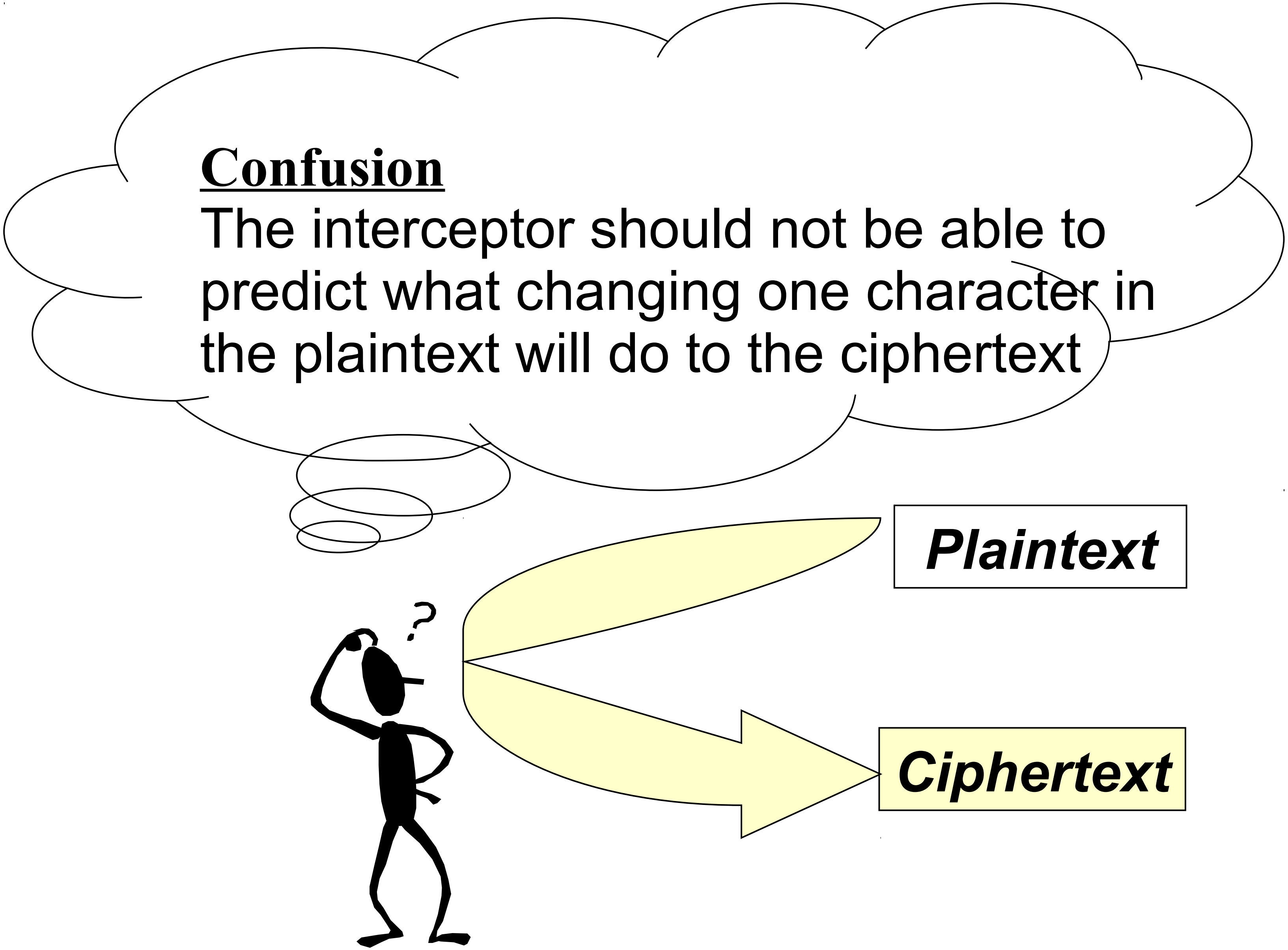
- Algorithms are difficult to change
- Cannot design an algorithm for every pair of users
- Expert review
- No security through obscurity!

Confusion and Diffusion

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



Confusion



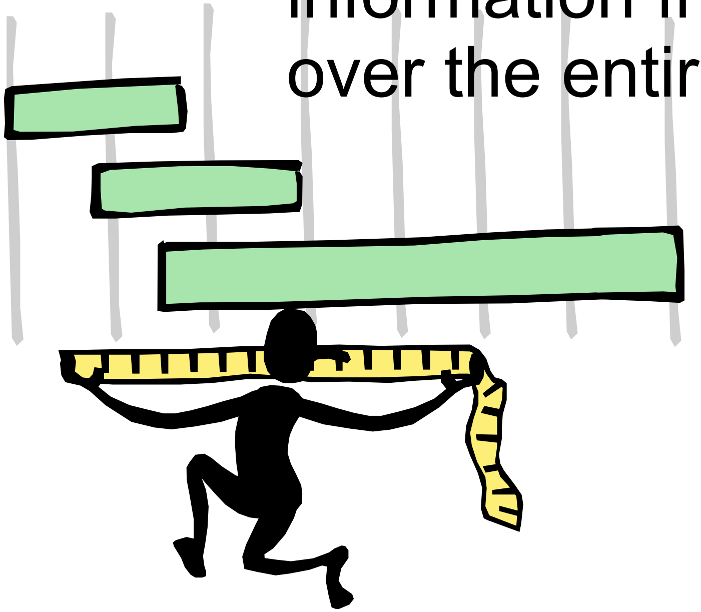
Confusion

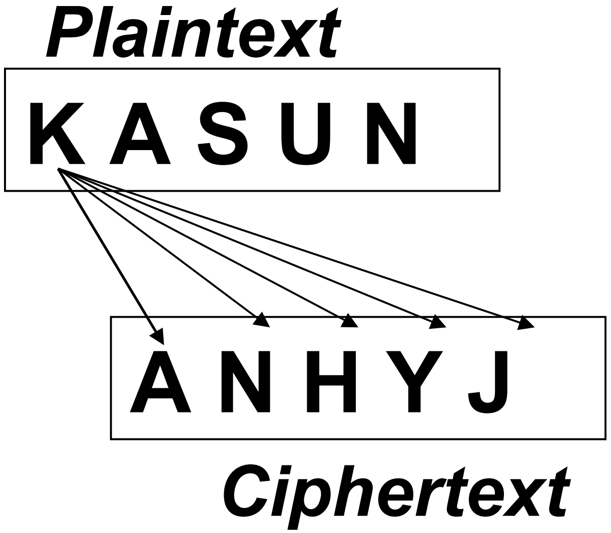
The interceptor should not be able to predict what changing one character in the plaintext will do to the ciphertext

Diffusion

Diffusion

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





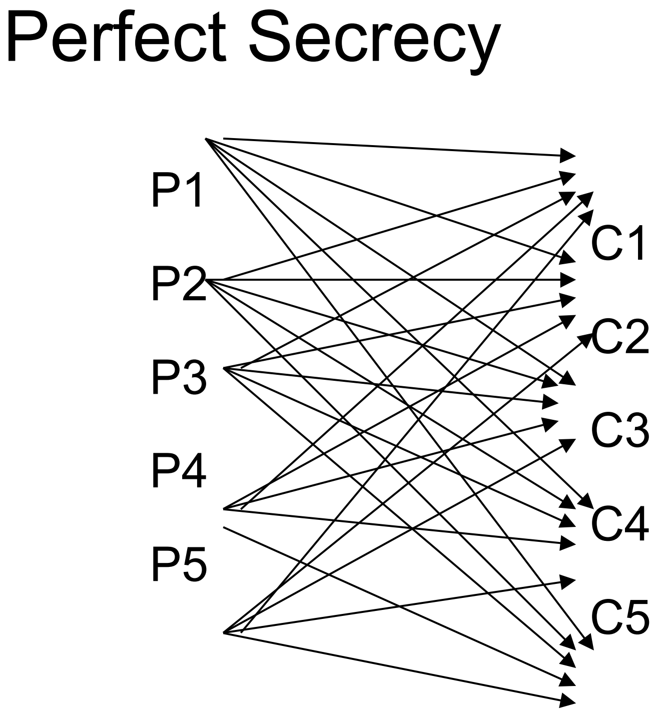
Plaintext

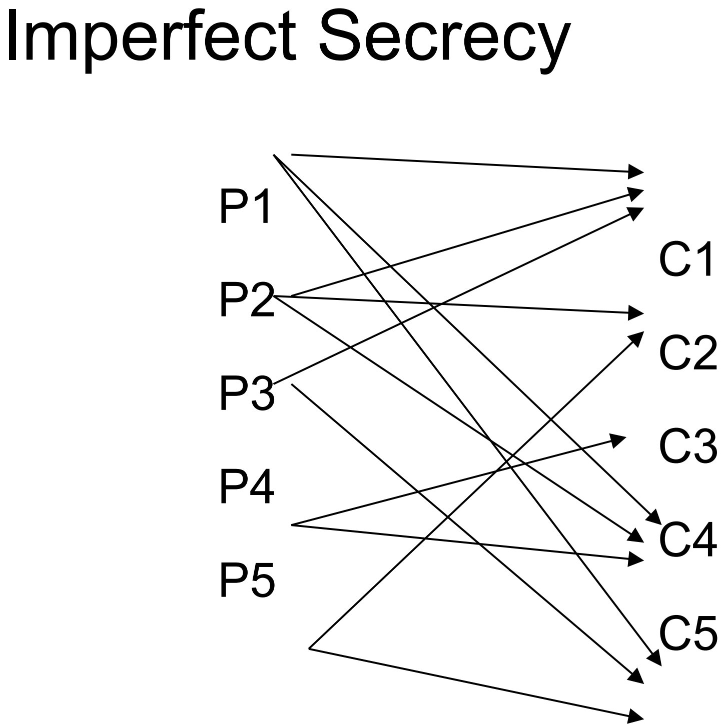
K A S U N

A N H Y J

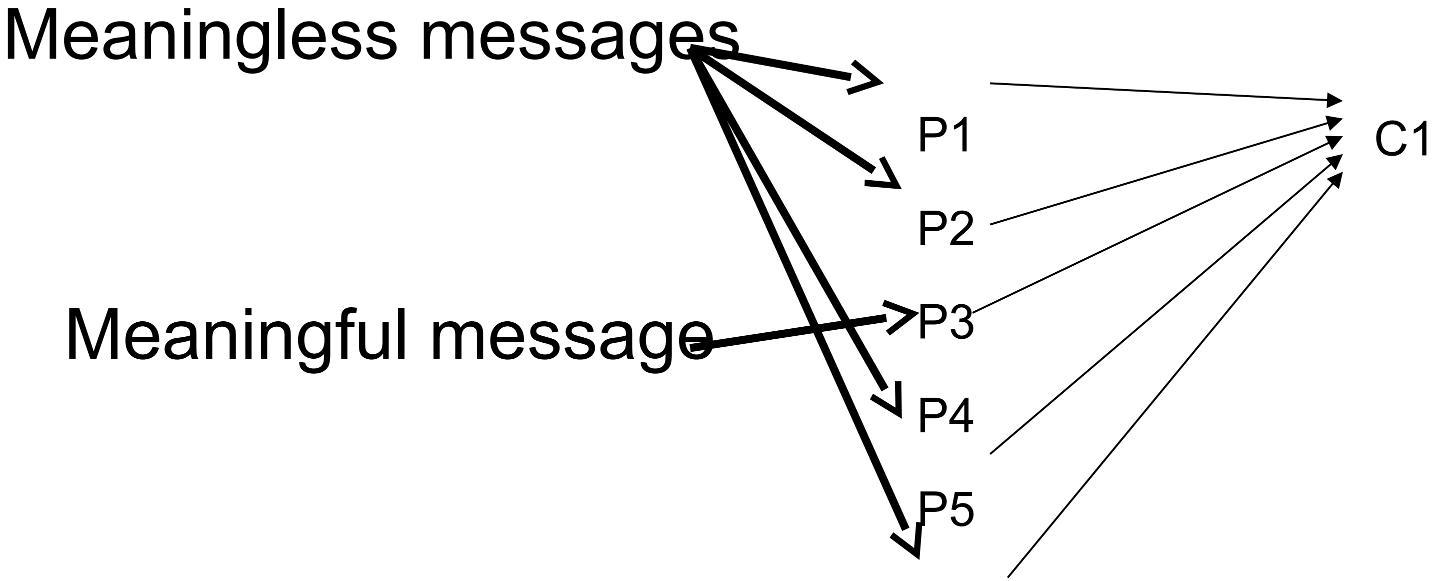
Ciphertext

Information Theoretic Tests





Redundancy



Meaningless messages

Meaningful message

P1

P2

P3

P4

P5

C1

What the Cryptanalyst Has to Work With

- Ciphertext only
- Full or partial plaintext
- Ciphertext of any plain text
- Algorithm of ciphertext

Types of Cryptanalytic Attacks

Ciphertext only
only knows encryption algorithm and ciphertext, goal is to identify plaintext

Known plaintext
know encryption algorithm and one or more plaintext & ciphertext pairs formed with the secret key

Types of Cryptanalytic Attacks

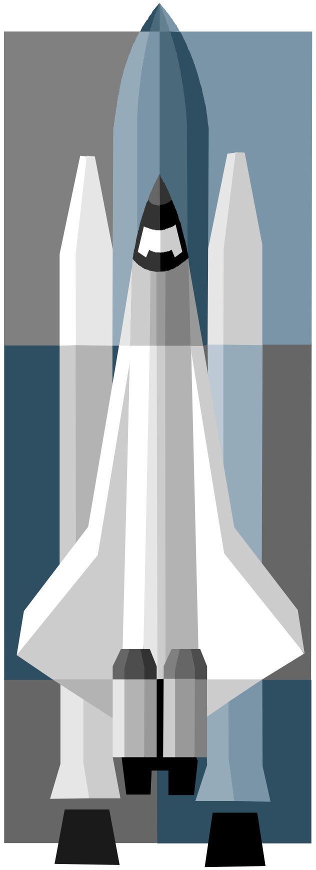
Chosen ciphertext
know encryption algorithm and can select ciphertext and obtain
plaintext to attack cipher

Chosen text
know encryption algorithm and can select either plaintext or ciphertext to en/decrypt to attack cipher

Brute Force Search

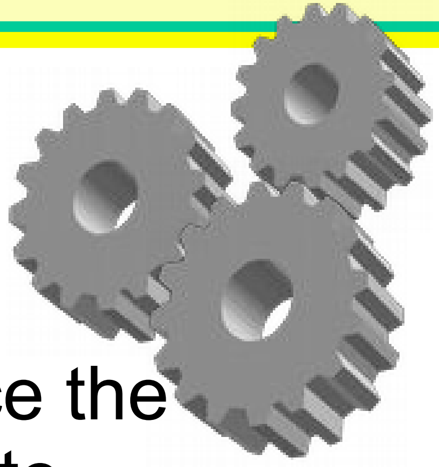
- Always possible to simply try every key
- Most basic attack, proportional to key size
- Assume either know/recognize plaintext

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/

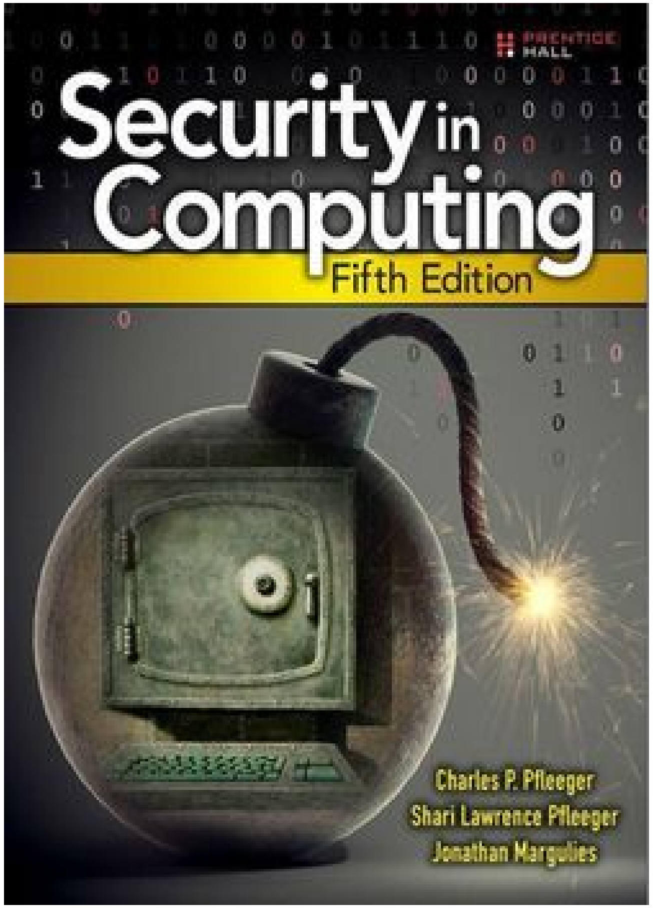
Unconditional/Computational Security

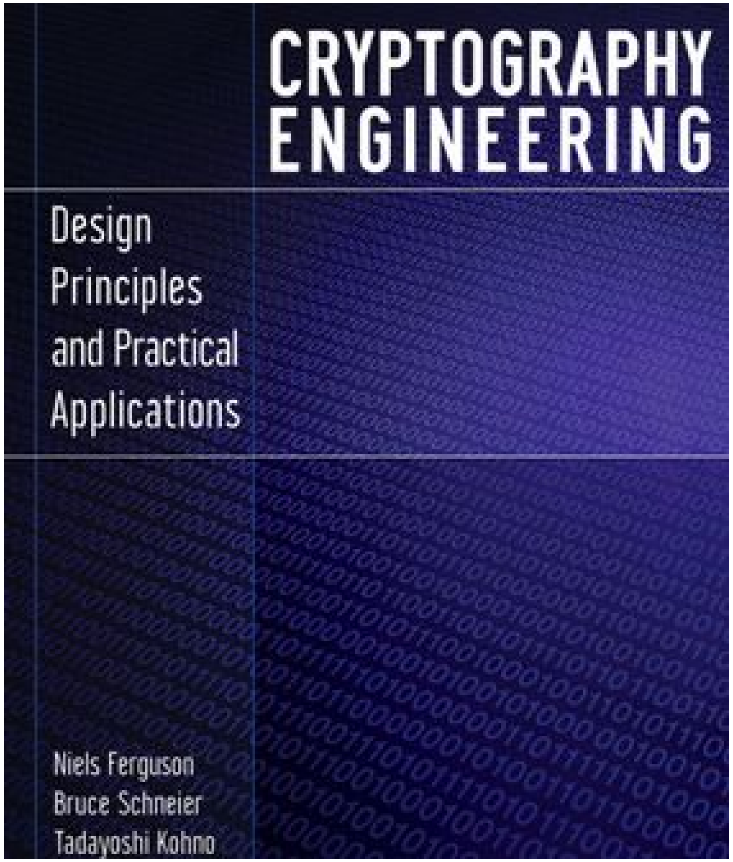


Unconditional security
no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

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

Books





Slides and Java Source Codes are available at:
`https://github.com/BDREN/PracticalCrypto.git`

e-mail: kasun@ucsc.cmb.ac.lk