Security of Information System

Basic Encryption and Decryption

Dr. Kasun De Zoysa

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

kasun@ucsc.cmb.ac.lk

Objectives:

Basic Encryption and Decryption

- Understand the concept of encryption/decryption
- Describe the different types of ciphers
- Identify the characteristics of good cipher

kasun@ucsc.cmb.ac.lk

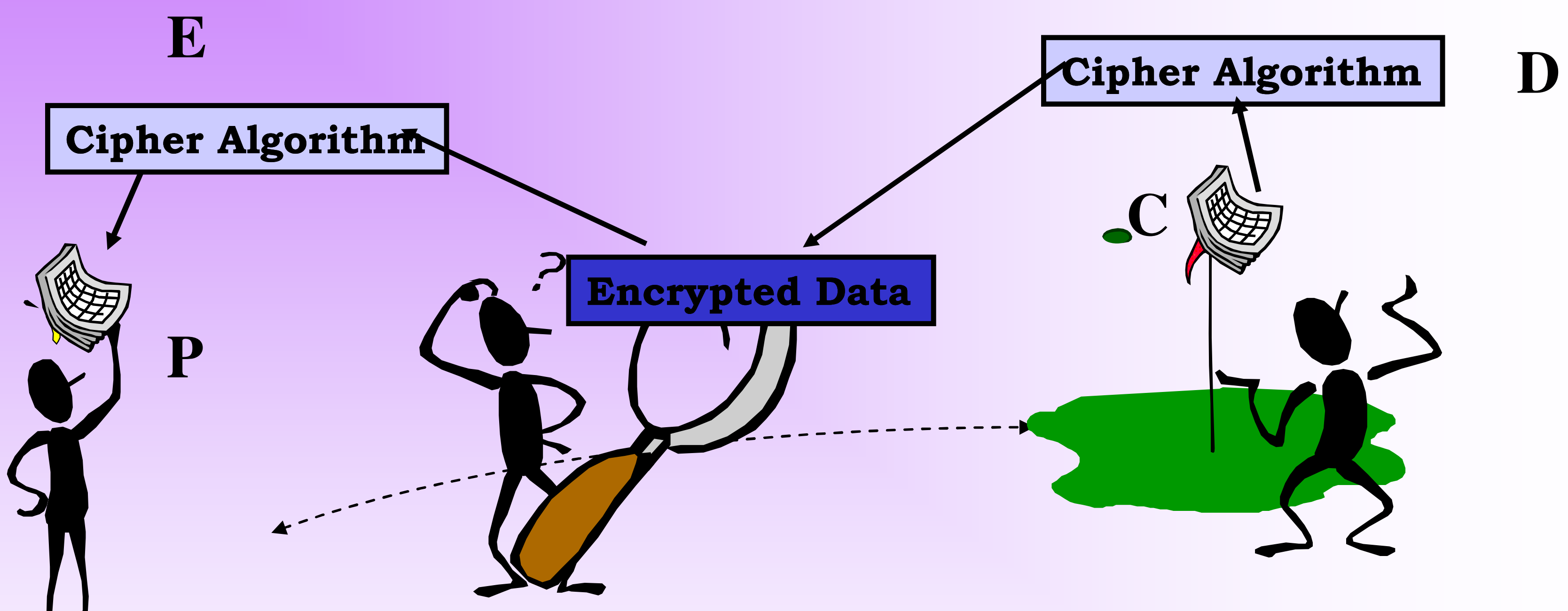
Basic Encryption and Decryption

1.1 Terminology and Background

- Encryption, Decryption and Cryptosystems
- Plain Text and Cipher Text
- Encryption Algorithms
- Cryptanalysis

UCSC
kasun@ucsc.cmb.ac.lk

Basic Concept



P clear (plain) text, message-readable (intelligible) information

C ciphertext-encrypted information

E encryption (enciphering)-transforming clear text into ciphertext

D decryption (deciphering)-transforming ciphertext back into plaintext

kasun@ucsc.cmb.ac.lk

Cipher Algorithm

Encrypting algorithm: a mathematical function having the following form:

C = E (P, Ke) where Ke encryption key

Decryption algorithm: a mathematical function having the following form:

P = D (C, Kd) where Kd encryption key

kasun@ucsc.cmb.ac.lk

Cryptanalysis

Attacker (cryptanalysis, intruder) - person that tries to discover C (compromise the encryption algorithm)

kasun@ucsc.cmb.ac.lk

What the Cryptanalyst Has to Work With

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

UCSC
kasun@ucsc.cmb.ac.lk

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

Chosen plaintext

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

kasun@ucsc.cmb.ac.lk

Types of Cryptanalytic Attacks

Chosen ciphertext

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

Chosen text

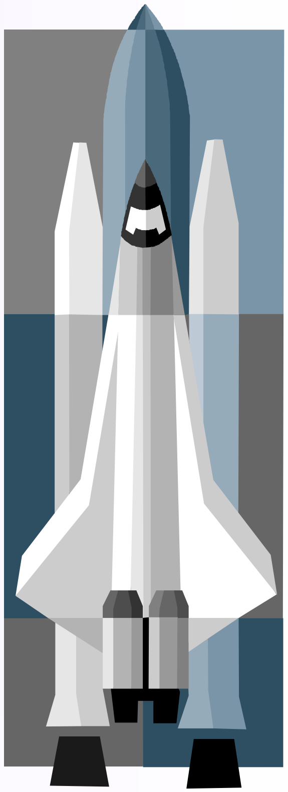
know encryption algorithm and can select either plaintext or ciphertext to en/decrypt to attack cipher

kasun@ucsc.cmb.ac.lk

Brute Force Search

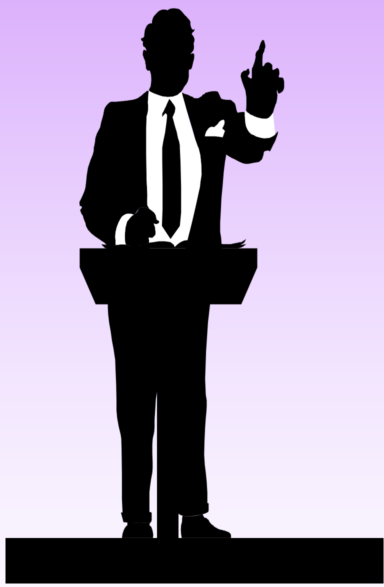
- **Always possible to simply try every key**
- **Most basic attack, proportional to key size**
- **Assume either know/recognize plaintext**

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



UCSC
kasun@ucsc.cmb.ac.lk

Basic Encryption and Decryption



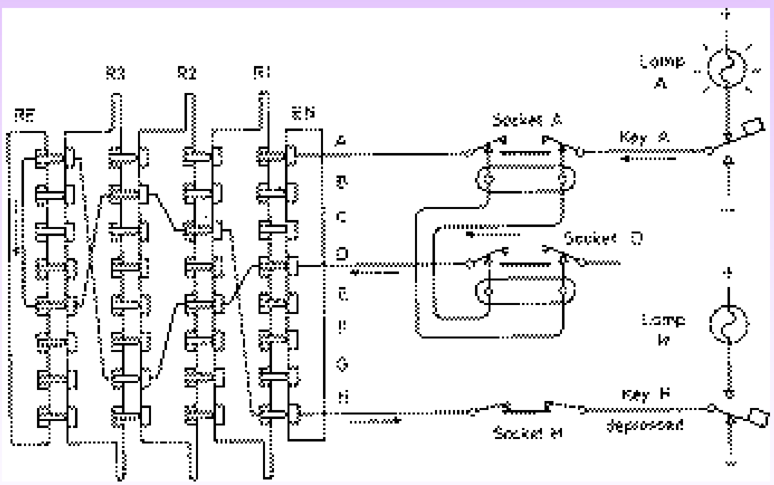
1.2 Introduction to Ciphers

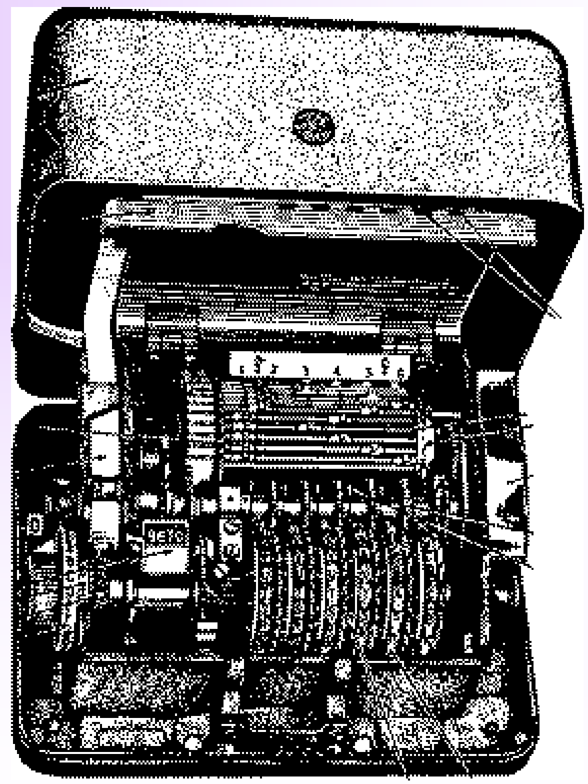
- Monoalphabetic Substitutions such as the Caesar Cipher
- Cryptanalysis of Monoalphabetic Ciphers
- Polyalphabetic Ciphers such as Vigenere Tableaux
- Cryptanalysis of Polyalphabetic Ciphers
- Perfect Substitution Cipher such as the Vernam Cipher
- Stream and Block Ciphers

UCSC
kasun@ucsc.cmb.ac.lk

Machine ciphers

- The Enigma Rotor Machine (WW2)





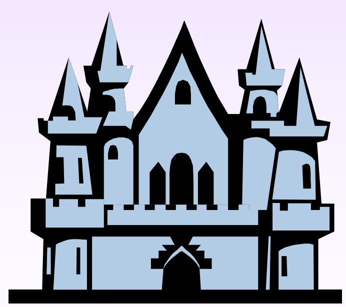
UCSC
kasun@ucsc.cmb.ac.lk

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

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



UCSC

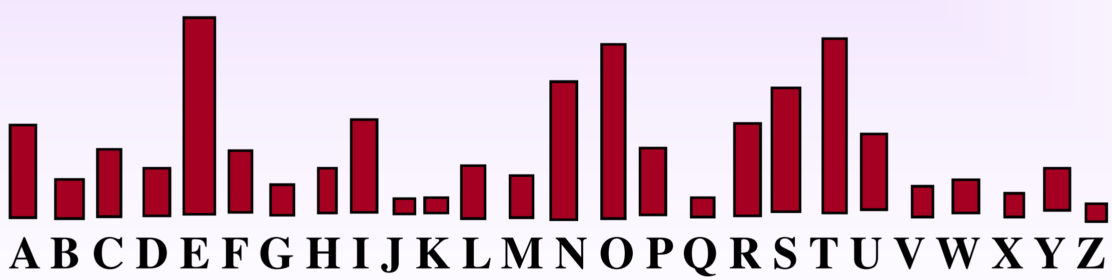
kasun@ucsc.cmb.ac.lk

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>



kasun@ucsc.cmb.ac.lk

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

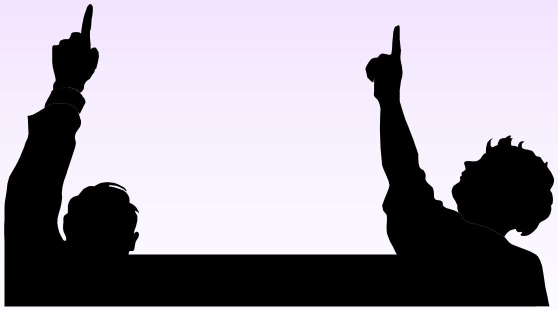
Cipher Text : czysh

kasun@ucsc.cmb.ac.lk

The Perfect Substitution Cipher

One Time Pad

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



kasun@ucsc.cmb.ac.lk

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	I	t	x	m	a	b	

<u>Binary Vernam Cipher</u>

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

UCSC

kasun@ucsc.cmb.ac.lk

The One-Time Pad

- 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

kasun@ucsc.cmb.ac.lk

Transpositions (Permutation)

Columnar Transposition

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

Cipher text formed by → **c1 c6 c11 c2 c7 c12 c3 c8 ...**

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

UCSC
kasun@ucsc.cmb.ac.lk

Block vs Stream Ciphers

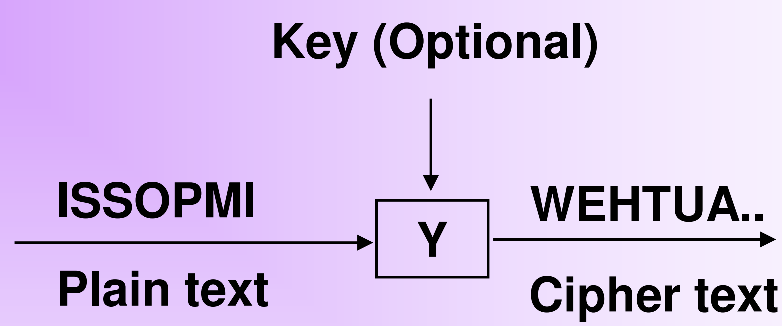
- Block ciphers process messages in blocks, each of which is then en/decrypted
- Like a substitution on blocks of characters
    - 64-bits or more

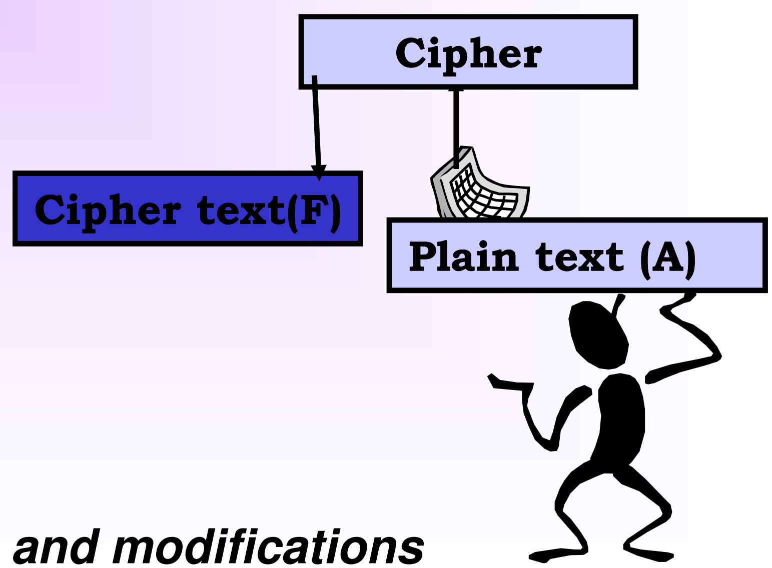
- Stream ciphers process messages a bit or byte at a time when en/decrypting
- E.g. Vernam cipher, one time pad

- Many current ciphers are block ciphers

kasun@ucsc.cmb.ac.lk

Stream Cipher





Advantage

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

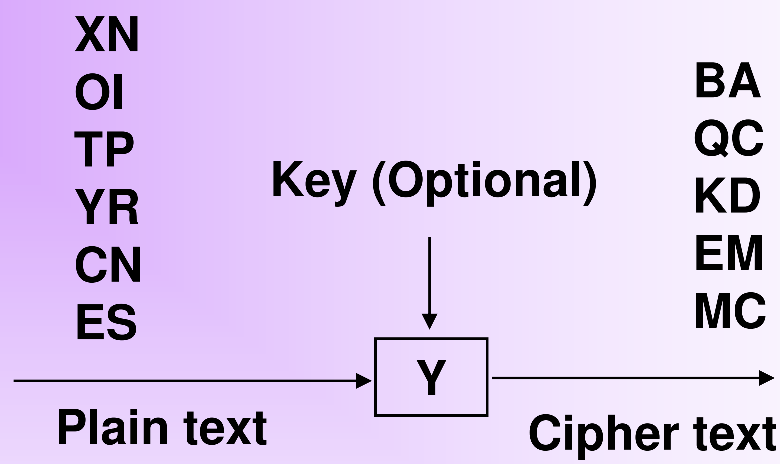
Disadvantage

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

UCSC

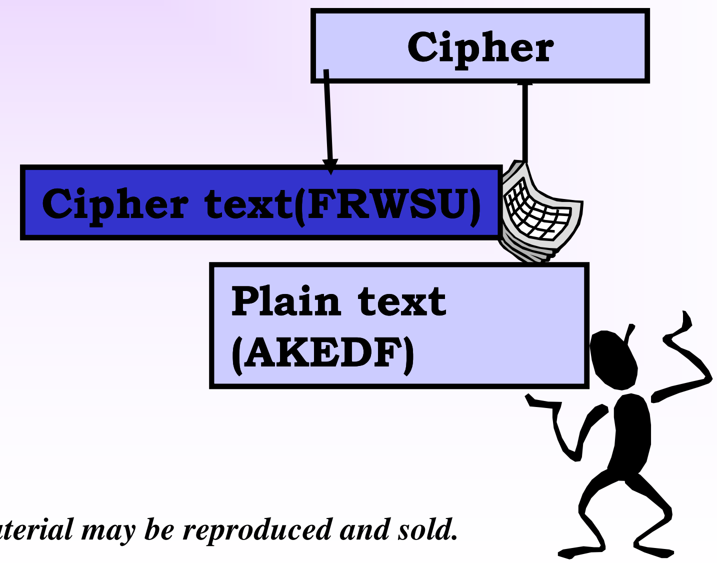
kasun@ucsc.cmb.ac.lk

Block Cipher



Disadvantage

- *Slowness of encryption*
- *Error propagation*



Advantage

- *Diffusion*
- *Immunity to insertion*

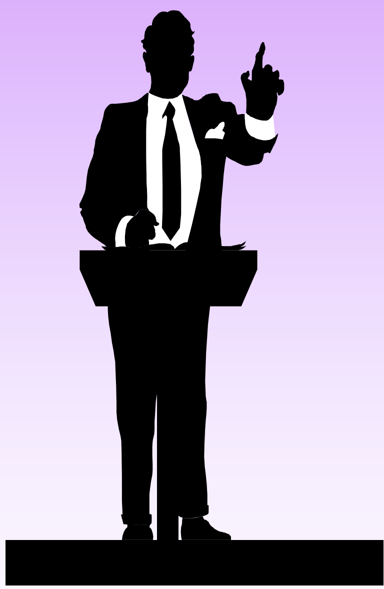
UCSC
kasun@ucsc.cmb.ac.lk

Block Ciphers

- Substitution-Permutation Ciphers
  - Product cipher
  - S-P networks is the basis of modern symmetric cryptography
- Substitution box (S-Box)
  - We have an input as a n bits word
  - The output will be a n bit word that the input has been substituted for.

kasun@ucsc.cmb.ac.lk

Basic Encryption and Decryption



1.3 Characteristics of ‘Good’ Ciphers

- Shannon Characteristics
- Confusion and Diffusion
- Information Theoretic Tests
- Unicity Distance

UCSC
kasun@ucsc.cmb.ac.lk

Characteristic of "Good" Cipher

Shannon Characteristics - 1949

- **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**

UCSC
kasun@ucsc.cmb.ac.lk

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.*

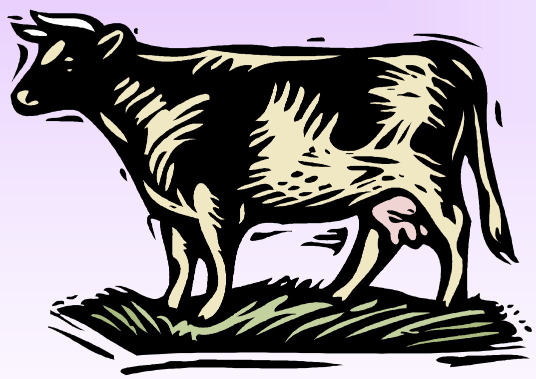
Reasons:

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

kasun@ucsc.cmb.ac.lk

Confusion and Diffusion

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

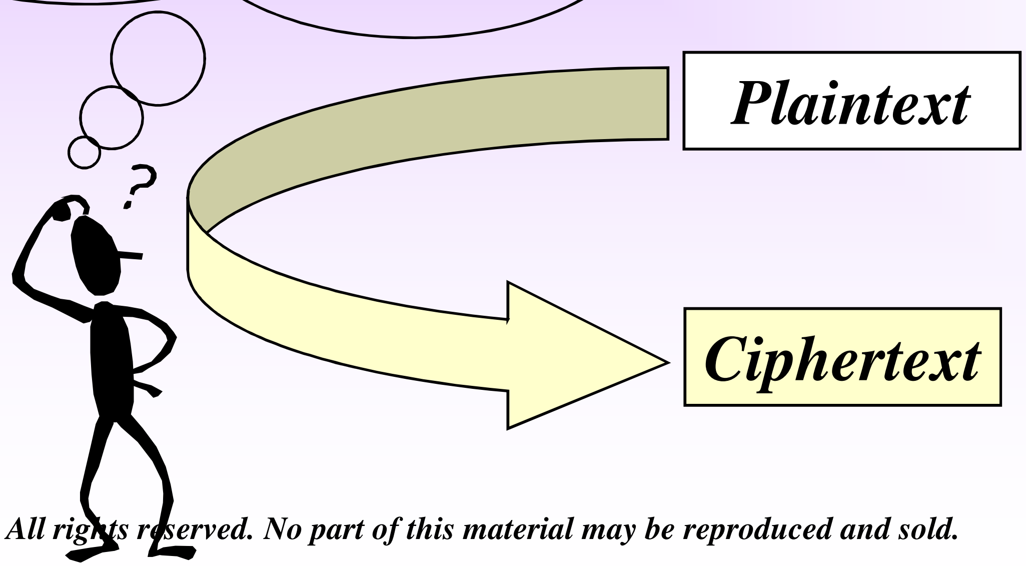


UCSC
kasun@ucsc.cmb.ac.lk

Confusion

Confusion

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

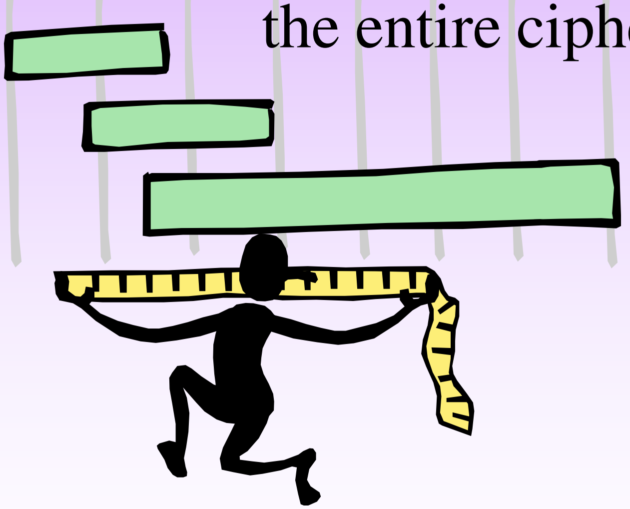


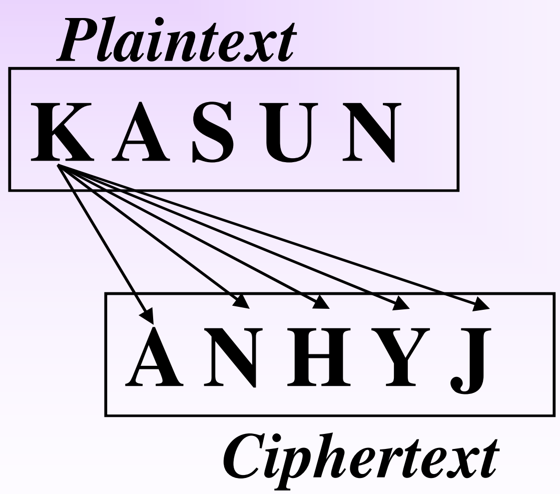
UCSC
kasun@ucsc.cmb.ac.lk

Diffusion

<u>Diffusion</u>

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





UCSC
kasun@ucsc.cmb.ac.lk