

# Encryption Overview and Encryption Techniques

# A quick Quiz

- What are the **three major security goals**?
- What goal are we going to refer to today?

# Lecture Outline

- **Encryption Basics**
- Simple Encryption –Caesar and VigenereCiphers
- Computers and Encryption
- Encryption Techniques
- Crypto-analytic Attacks

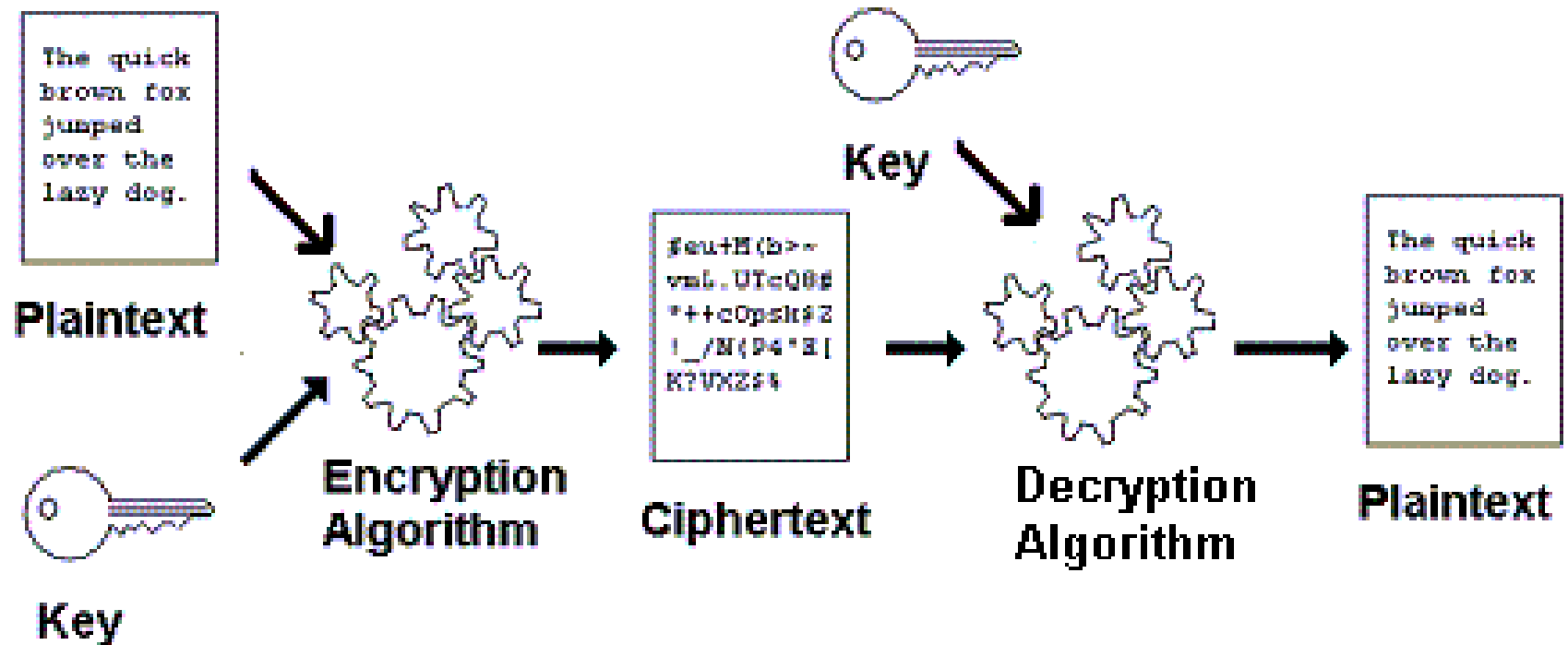
# Encryption and Security Goals

- Encryption is used to provide confidentiality.

# Definitions

- Encryption: a process of transforming data using an algorithm so that data is no longer recognisable, and at the same time, recoverable.
- 3 Important inputs:
  - **Plaintext**: message to be encrypted, or call it clear text.
  - **Encryption Key**: Another **input** to the Encryption algorithm that determines the output of the algorithm for a specific plaintext.
  - **Encryption Algorithm**: The set of procedures with *plaintext* and encryption *key* as **inputs** and the encrypted plaintext (ciphertext) as **output**.

# Encryption and Decryption



# Terms

- **Ciphertext**: Encrypted data –output of encryption algorithm and input of decryption algorithm.
- **Symmetric Encryption**: An encryption method where encryption key and the decryption key are the same.
- **Asymmetric Encryption**: An encryption method where the encryption key and decryption key are different also known as **Public Key Encryption**.

# Cryptology

## Cryptology :

The study of secure communications. A very old science (dating from at least the time of the Romans). It consists of two sections - Cryptanalysis and Cryptography.

## Cryptanalysis :

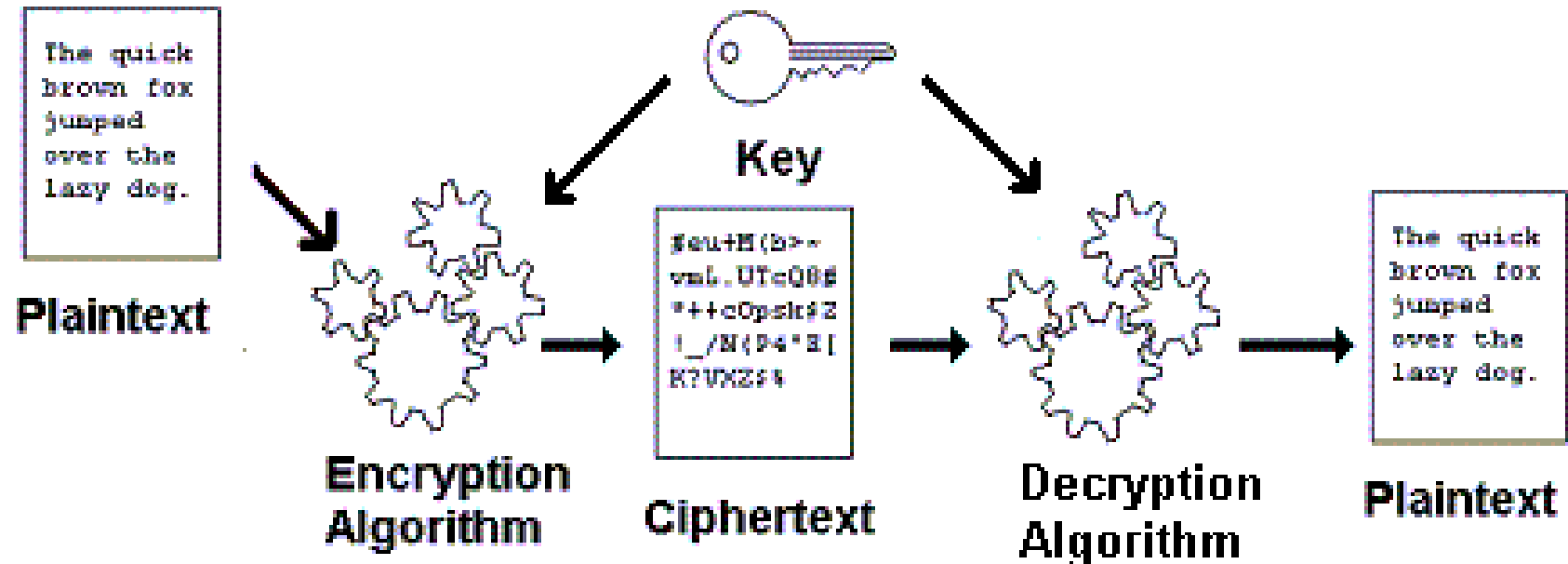
This is the branch of cryptology concerned with the breaking of encoded messages.

## Cryptography:

This is the branch of Cryptology concerned with the creation, development, application and testing of encoding methods.

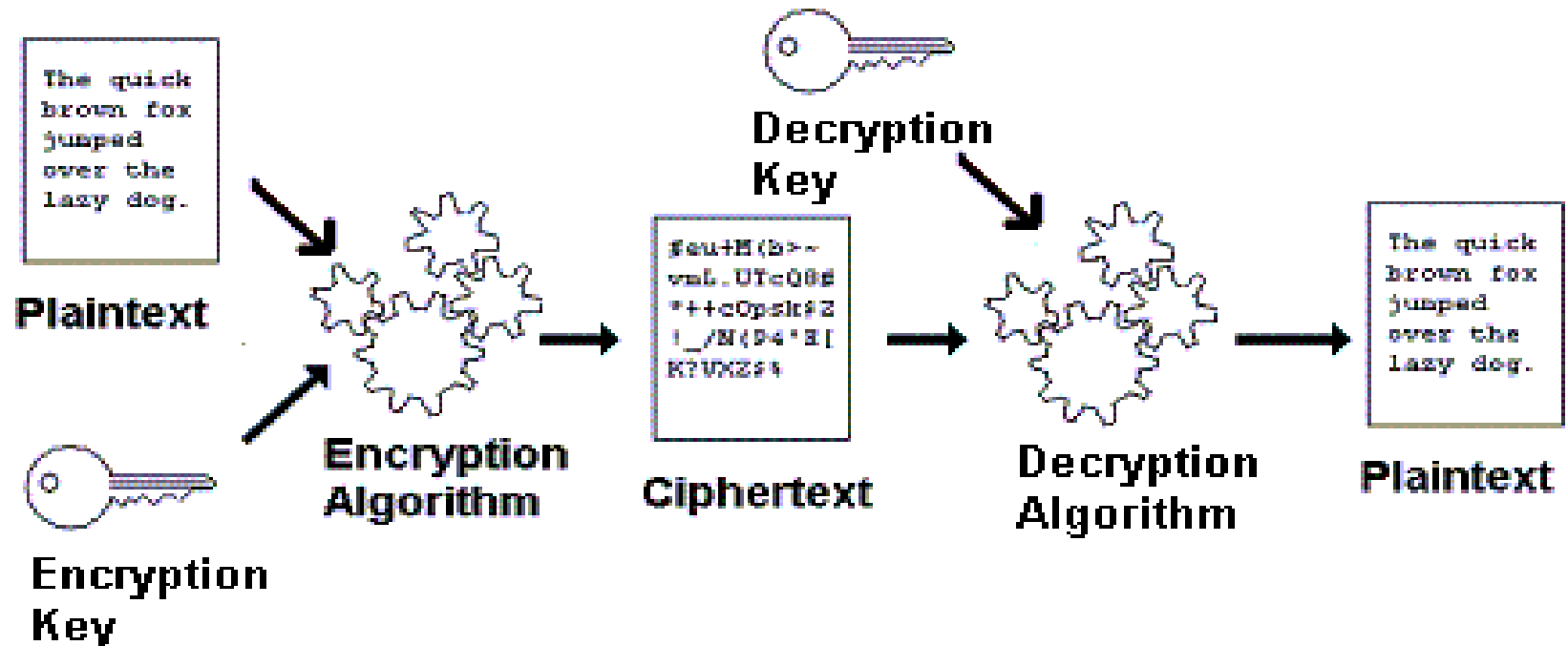


# Symmetric Encryption



In Symmetric Encryption the same key is used in the encryption and decryption algorithms. Also, the encryption and decryption algorithms are often closely related. Provided the shared key remains a secret communication through symmetric encryption is secure.

# Asymmetric Encryption



In Asymmetric Encryption different keys are used for encryption and decryption. Asymmetric Encryption is also known as Public Key Encryption. The decryption algorithm is often the reverse or complement of the encryption algorithm.

# Historical Context of encryption

- Encryption has been used for hundreds of years.
- A very simple (and easily breakable) method of encryption is the Caesar Cipher.
- A slightly more secure method of encryption is the VigenereCipher.

# Caesar Cipher

The plaintext:

Punctually at six o'clock, the sun set, with a last yellow flash behind the Blue Mountains.

(Opening lines of the novel Dr. NO by Ian Fleming)

Step 1 : - remove punctuation and make entirely lower case

punctually at six oclock the sun set with a last yellow flash  
behind the blue mountains.

Step 2 : - decide on key - a number between 0 and 25 - we choose a key of 6. Then draw up a table showing how each letter is changed.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |

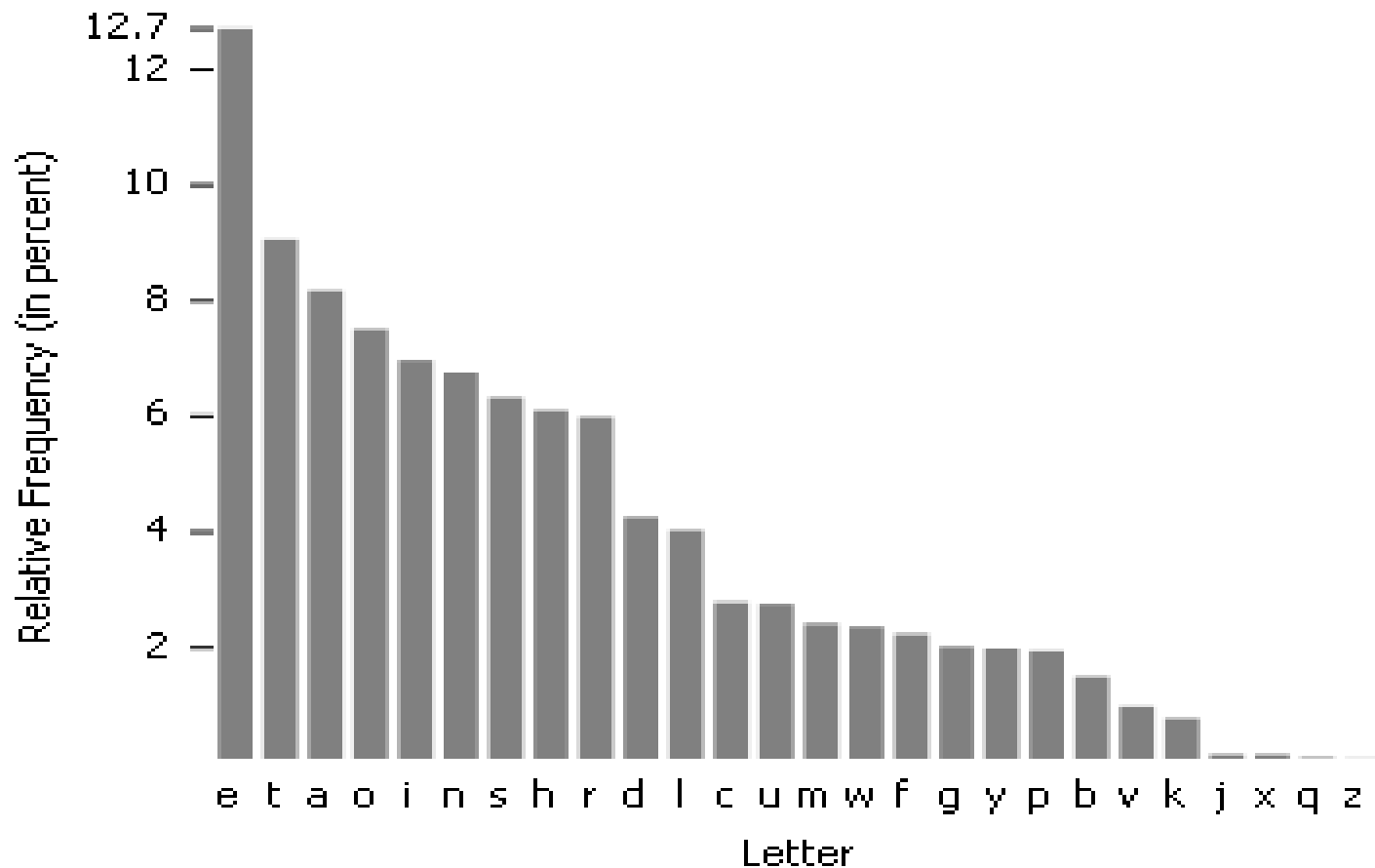
Step 3: - transform the plaintext into the ciphertext

vatizagre g z yod uiruiq znk yat ykz cozn g cgyz ekrruc lrgyn  
hknotj znk hrak suatzgoty

# An obvious way to crack it?

- It vulnerable to a Brute Force attack. There are only 25 possibilities. It does not take long to run through all these to see which one generates sensible plaintext.

# Give you a hint: English letter frequencies



Source : Wikipedia article “letter frequency”

# Caesar Cipher weaknesses

Vulnerable to Frequency Analysis attack.

- Each letter is always transformed to same character.
- Frequency of each letter in English is known.
- Hence it is possible to match the most frequent letters in English with the most frequent letters in the ciphertext.

# Vignere Cipher

- Vignere Cipher is essentially a repeated Caesar Cipher.
- The Vignere Cipher requires a key. The key is a word such as “university”. This translates to successive Caesar Cipher shifts of 20,13,8,21,4,17,18,8,19,24 as the letters “u”, “n”, “i”, “v”, “e”, “r”, “s”, “i”, “t” and “y” are the 20th, 13th, 8th... etc. letters of the alphabet.
- A Vignere Square (shown on the next slide) helps in the encryption and decryption process.



# Vigenere Square and Demonstration

| Plain | 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 |
|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1     | 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 |
| 2     | 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 |
| 3     | 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 |
| 4     | 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 |
| 5     | 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 |
| 6     | 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 |
| 7     | 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 |
| 8     | 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 |
| 9     | 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 |
| 10    | 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 |
| 11    | 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 |
| 12    | 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 |
| 13    | 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 |
| 14    | 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 |
| 15    | 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 |
| 16    | 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 |
| 17    | 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 |
| 18    | 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 |
| 19    | 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 |
| 20    | 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 |
| 21    | 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 |
| 22    | 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 |
| 23    | 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 |
| 24    | 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 |
| 25    | 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 |
| 26    | 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 |

```

key      u n i v e r s i t y u n i v e r s i
shifts   20 13 8 21 4 17 18 8 19 24 20 13 8 21 4 17 18 8
plaintext s e n d r e i n f o r c e m e n t s
ciphertext m r v y v v a v y m l r k h i e l a
  
```

# Vignere Cipher Security

- More secure than Caesar Cipher.
- If the key is a meaningful word or phrase, then the strength is diminished as the key is easier to guess.
- Techniques exist to estimate the length of the key (Kasiski Examination)
- If the key is made the same length as the message itself, then the system becomes a one time pad –i.e. a key that is random, as long as the plaintext, is used only once and is known only to the sender and receiver.

# Lecture Outline

- Encryption Basics
- Simple Encryption – Caesar and VigenereCiphers
- **Computers and Encryption**
- Encryption Techniques
- Cryptoanalytic Attacks

# Computers and Encryption

- The availability of computers and internet has changed encryption and encoding number of ways.:
- Encryption and decryption by computers is much faster. Encryption schemes need much more robust.
- Traditional encryption methods (Caesar and Vigenere) work at the level of characters. Computer encryption works at the bit level.
- Many of the applications used on the internet such as e-commerce and VPNs require robust, open and secure encryption.

# What makes an effective Encryption?

- Encryption transforms the plaintext into ciphertext.
- It should be **very, very, very** hard (if not impossible) to ascertain the plaintext from the ciphertext, even when the encryption method is known, but the key is not.
- For modern computer based encryption the encryption algorithm is known by all – it is the key or keys which are kept secret.

# Substitution and Transposition Ciphers

- Caesar and Vigenere Ciphers are examples of **Substitution Ciphers**—one character in the plaintext is replaced by another character in the ciphertext.
- **Transposition Cipher**—another simple cipher in which the plaintext is re-arranged (positions transposed).
- Ciphers which only perform substitution or only perform transposition are inherently weak.
- A cipher which performs more than one operation on the plaintext will tend to be stronger. This type of cipher is a **Product Cipher**.

# Modern Digital Ciphers

- Modern Digital Ciphers can operate on one character at a time or on blocks of characters.
- Ciphers operating on one character at a time are **Stream Ciphers**. Ciphers operating on blocks of characters **are Block Ciphers**.
- Modern Block Ciphers are all Product Ciphers

# Product Ciphers

- Operations which may be performed by product ciphers operating on bits rather than characters include:
  - Substitution
  - Transposition
  - Swap
  - Bit Inversion
  - Circular Shift
  - XOR operation



# S-Box

- Stands for “Substitution Box”.
- Used in many symmetric encryption algorithms.
- S-Box is specified as an  $m \times n$  table.
- Involves substituting blocks of  $m$  bits with blocks of  $n$  bits (note  $n$  is often  $< m$ )
- An S-Box where the  $m=n$  (i.e. the number of input bits is the same as the number of output bits) is reversible.

# 3 x 3 S-Box Example

|              | Right 2 Bits → | 00  | 01  | 10  | 11  |
|--------------|----------------|-----|-----|-----|-----|
| Left 1 Bit ↓ |                |     |     |     |     |
| 0            |                | 011 | 101 | 111 | 100 |
| 1            |                | 000 | 010 | 001 | 110 |

- This is a very simple example of an S-Box. Real S-Boxes are larger. An  $n \times n$  S-Box is invertible (i.e. knowing the outputs, you can deduce the inputs)
- This example takes 3 input bits and outputs 3 different bits

## 3 x 3 S-Box Example (2)

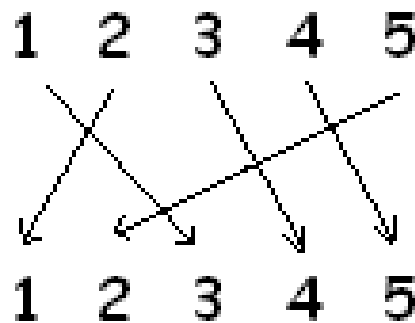
|              | Right 2 Bits → | 00  | 01  | 10  | 11  |
|--------------|----------------|-----|-----|-----|-----|
| Left 1 Bit ↓ |                |     |     |     |     |
| 0            |                | 100 | 110 | 101 | 000 |
| 1            |                | 011 | 001 | 111 | 010 |

- The S-Box above decrypts the output of the S-Box on the previous page.

# P-Boxes

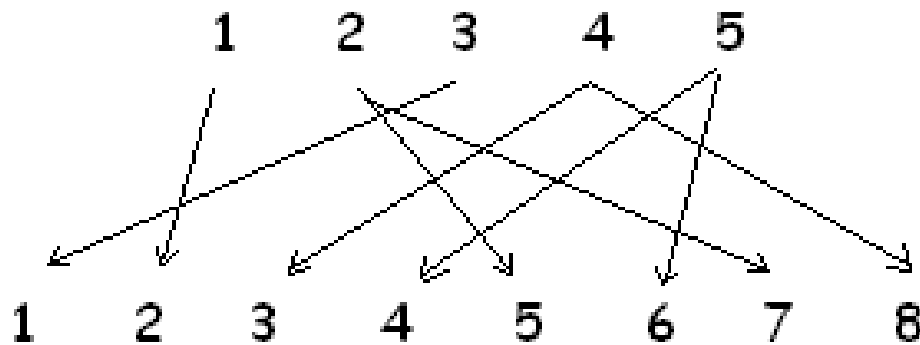
- This is a Permutation Box
- Involves the transposition of binary digits within blocks.
- May also involve expansion or compression of the input bits.
- Used to bring about **diffusion**.

# Example P-Box



In this simple P-Box 5 bits are permuted. The input abcde would become beacd. In practice, bits at particular positions rather than letters are permuted.

# Expansion P-Box

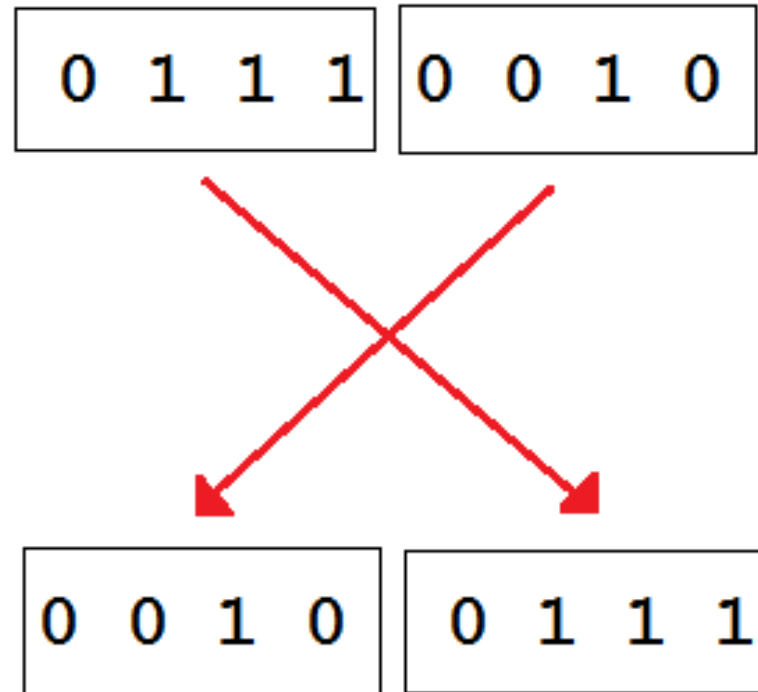


In this P-Box with expansion the bits at the 2nd, 4th and 5th positions are expanded to the 5th and 7th, 3rd and 8th and 4th and 6th positions respectively. The other bit positions are only moved to one other position.

The input "abcde" becomes permuted and expanded to "cadebebd".

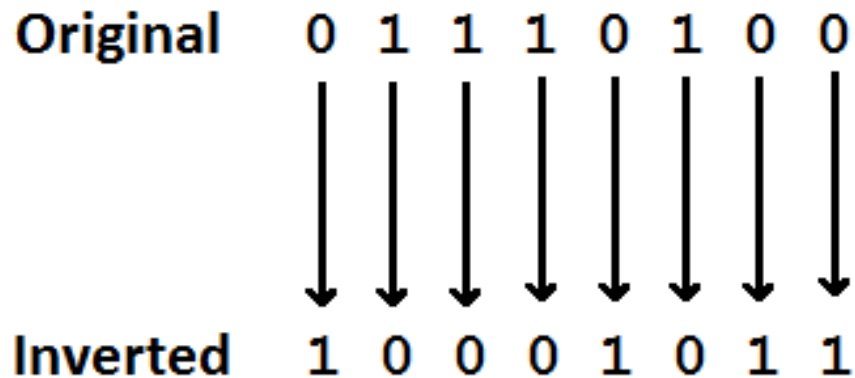
# Swap

In the swap operation, an even numbered set of bits  $> 0$  is split into left and a right halves and the two halves are swapped.



# Bit Inversion (aka complement)

- In bit inversion every 0 is changed to a 1 and every 1 is changed to a 0.





# Circular Shift

- In a shift operation, bits are rotated either to the left or right. No bits are lost, but their position is changed.

Original Number   0   1   1   0   0   1   0   1

Shift 1 left   1   1   0   0   1   0   1   0

Shift 2 left   1   0   0   1   0   1   0   1

Shift 3 left   0   0   1   0   1   0   1   1

Shift 4 left   0   1   0   1   0   1   1   0

Shift 5 left   1   0   1   0   1   1   0   0

Shift 6 left   0   1   0   1   1   0   0   1

Shift 7 left   1   0   1   1   0   0   1   0

Shift 8 left   (Original Number)   0   1   1   0   0   1   0   1

# XOR Operation

- Boolean function that works on binary values i.e. 1 and 0
- Stands for Exclusive OR
- Extensively used in cryptographic algorithms.
- XOR encipherment does not give any real security but is useful when combined with other operations.

# XOR Truth Table

| Input 1 | Input 2 | Output |
|---------|---------|--------|
| 0       | 0       | 0      |
| 1       | 0       | 1      |
| 0       | 1       | 1      |
| 1       | 1       | 0      |

- Produces an output of 1 when one, and only one of the inputs is 1 –hence the name “exclusive or”

# Example XOR

## Encipherment/Decipherment

**XOR Encrytion of plaintext "demo" with  
the key "show"**

**"demo" is acsii 100,101,109,111**

**"show" is ascii 115,104,111,119**

Translating both of these to strings to 8 bit binary  
per character we get

```
demo = 01100100 01100101 01101101 01101111
⊕ show = 01110011 01101000 01101111 01110111
-----
Output = 00010111 00001101 00000010 00011000
```

If we then carry out another XOR operation with the  
output and the key we get our original plaintext back

```
Output = 00010111 00001101 00000010 00011000
⊕ show = 01110011 01101000 01101111 01110111
-----
demo = 01100100 01100101 01101101 01101111
```

# Confusion and Diffusion

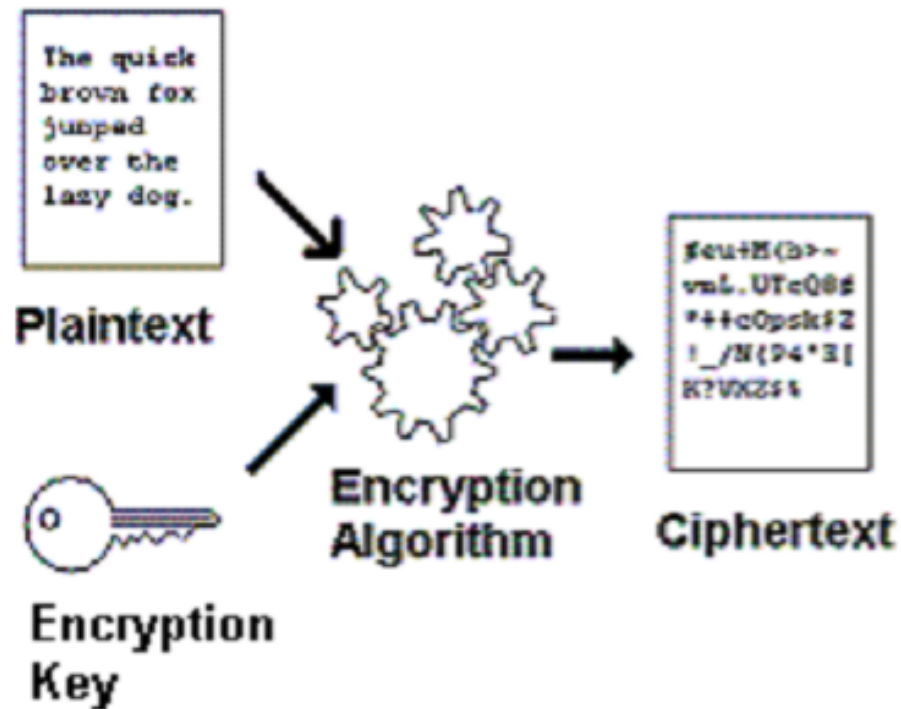
- Confusion and Diffusion are desirable features of encryption algorithms because they make cryptanalysis difficult. That is, they make it more difficult to break encrypted code.
- All modern encryption algorithms produce confusion and diffusion.

# Confusion and Diffusion

**Confusion and Diffusion** 2 desirable features of all encryption ciphers.

Change the message just a little and the ciphertext changes completely. This is **Diffusion**.

Change the encryption key just a little and the ciphertext changes completely. This is **Confusion**.



# Confusion and Diffusion - simple explanations

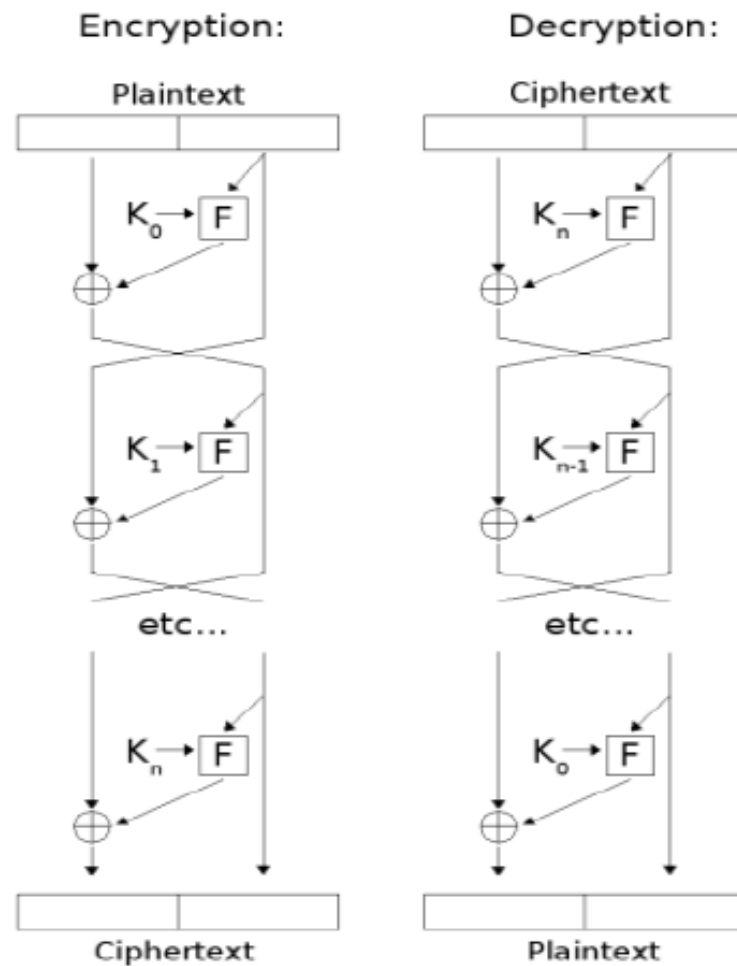
- Confusion looks at the relationship between the key and the ciphertext. Change the key even slightly and the encrypted message (the ciphertext) changes completely. This frustrates attempts to find the key using different samples of ciphertext.
- Diffusion looks at the relationship between message (the plaintext) and the encrypted message (the ciphertext). Change the original message even slightly and the encrypted message changes a lot. This frustrates attempts to find the plaintext using statistics drawn from the ciphertext.

# Types of Product Ciphers

- Feistel Product Ciphers: Both invertible and non-invertible operations are performed on the plaintext. – one example is the DES encryption standard.
- Non-Feistel Product Cipher : only invertible operations are performed on the plaintext. One example of this is the AES encryption standard.



# Feistel



Feistel Cipher

# Cryptoanalytic Attacks

- Classified along 2 dimensions:
  - Resources possessed by attacker
  - Method of attack adopted

# Resources possessed by the attacker

We always assume the attacker knows what encryption algorithm has been used but does not know the key. He/she has a ciphertext that they wish to decode. Possible other resources available to the attacker :


One or more samples of plaintext and the corresponding ciphertext. Neither the plaintext or ciphertext was chosen by the attacker.

A plaintext chosen by the attacker and its corresponding ciphertext.

A plaintext and corresponding ciphertext where the attacker fabricated the ciphertext and recovered the corresponding plaintext.

# Attack Types

- **Ciphertext only** : attacker only has ciphertext.
- **Plaintext** : Attacker has one or more samples of plaintext and corresponding ciphertext.
- **Chosen plaintext** : Attacker has one or more samples of plaintext and ciphertext where they chose the plaintext.
- **Chosen Ciphertext** : Attacker has fabricated ciphertext and has corresponding plaintext.
- **Chosen text** : Attacker has resources from chosen plaintext and chosen ciphertext and their corresponding ciphertext and plaintext.



Fewer  
Resources  
therefore  
harder

More  
resources  
therefore  
easier

# Attack Types

- Encryption scheme vulnerable to either ciphertext only or plaintext only attack is extremely weak.
- Caesar and Vigenere Ciphers are both vulnerable to ciphertext only and plaintext attacks.
- Chosen plaintext attack can be difficult to resist as a knowledgeable cryptanalyst can choose a plaintext that will reveal the key.
- Chosen ciphertext and text attacks are less common.

# Attack Methods

- Brute Force: This method goes through all the available keys, testing each one until the correct key is found.
- Exploit a weakness in the encryption algorithm.

# Brute Force Attack

- Brute Force attack will always find the key eventually.
- Main defence is to make the number of possible keys a large number –at least  $2^{128}$ . This makes the search for the key time-prohibitive.
- The effectiveness of brute force attacks can be enhanced by adding more hardware. Purpose designed hardware can be even more effective.

# Attacks based on a weakness

- All of the commonly used protocols have been extensively analysed.
- Encryption standards with known weaknesses are dropped fairly quickly.
- Networking protocols that exchange encrypted data allow attackers to collect encrypted data and from there possibly mount an attack.



# Lecture Summary

- Encryption Basics
  - Terms
  - Cryptology, Cryptanalysis, Cryptography
- Simple Encryption –Caesar and Vigenere Ciphers
  - Caesar Cipher –how it works
  - Vigenere Cipher –how it works

# Lecture Summary

- Computers and Encryption
  - Effects of Computers on encryption
  - Encryption and Security Goals
- Encryption Techniques
  - Substitution, Transposition and Product Ciphers
  - Encryption processes -substitution, transposition, swap, invert, circular shift, XOR
  - Unary/binary, reversible/non-reversible operations
  - Confusion and Diffusion

# Lecture Summary

- Cryptoanalytic Attacks
  - Attack Resources –plaintext, chosen plaintext, chosen ciphertext, text.
  - Attack Types –Brute Force, exploit weakness