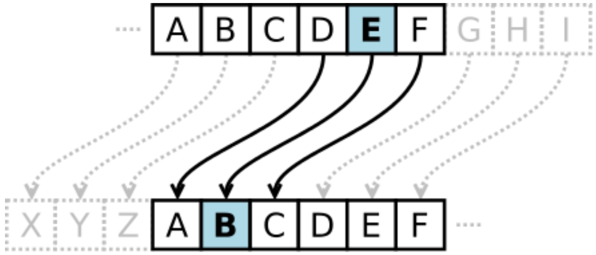
# Symmetric Cryptography

# Substitution Cipher

**Substitution ciphers: swap one letter to another one.**

- Simple substitution cipher
  - Simplest one is Caesar Cipher
  - Easy to break
- Monoalphabetic cipher
- Polyalphabetic cipher
- Code book cipher



(https://en.wikipedia.org/wiki/Caesar_cipher)

# Simple Substitution

**Writing out the alphabet in some order to represent the substitution**

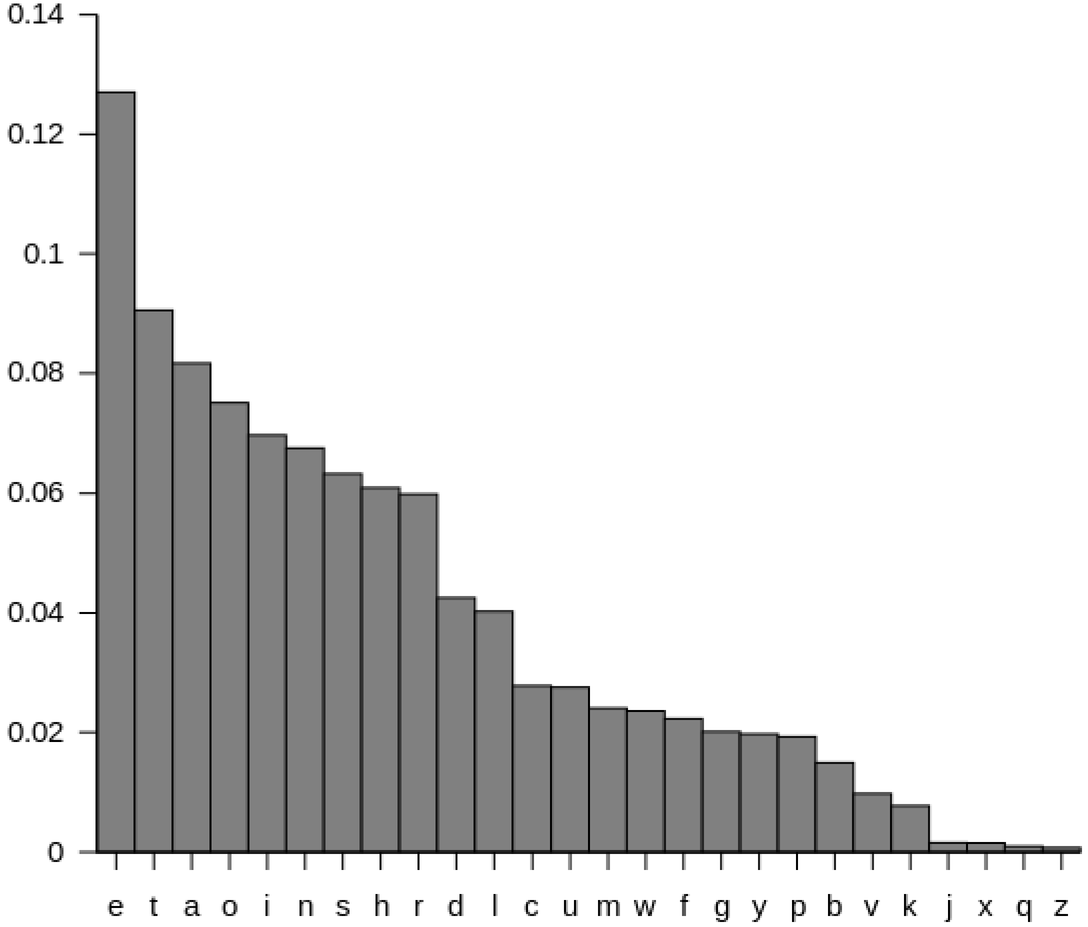
- **Write out a keyword**
- **Remove repeated letters**
- **Write all remaining letters alphabetically**
- **a.k.a monoalphabetic**

Keyword: **zebras**
Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

Message: **welcome to it security**
Encrypted: **VAIBLJA QL PABTOFQX**
FIVE LETTER: **VAIBL JAQLP ABTOF QXXXX**

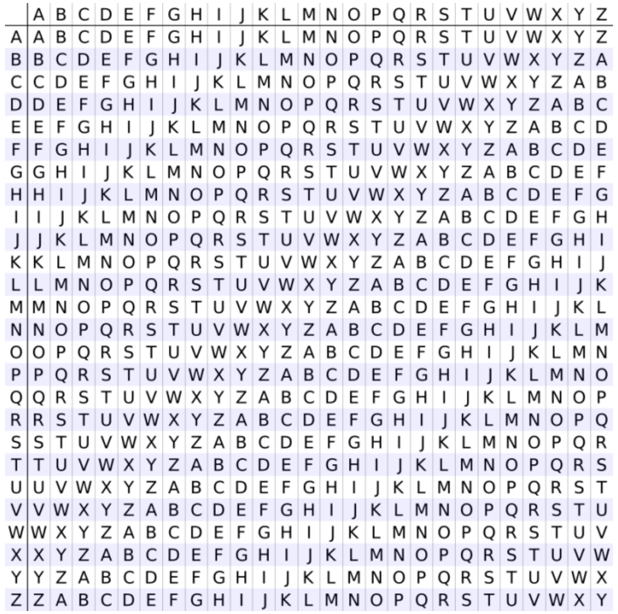
# Polyalphabetic

- Each character "rotated" by a different amount (1-25). The key is a look-up table (shared).
- mapping of each crypto-letter to plain-letter is repeated.
- Easy to crack using statistical methods (no shuffling) and knowledge of commonly used words.



# Codebook cipher

- Each character "rotated" by a different amount (1-25). The key different for every instance of a letter. **Constantly-changing**
- mapping of each cipher-letter to plain-letter is rarely repeated.
- Very hard to crack if word groupings are preserved.
- Impossible to crack if punctuation removed, key totally random, no repetition.



| | 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 |

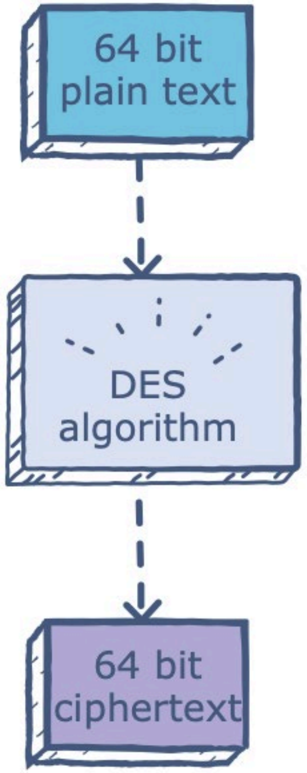
# Data Encryption Standard (DES)

### Definition

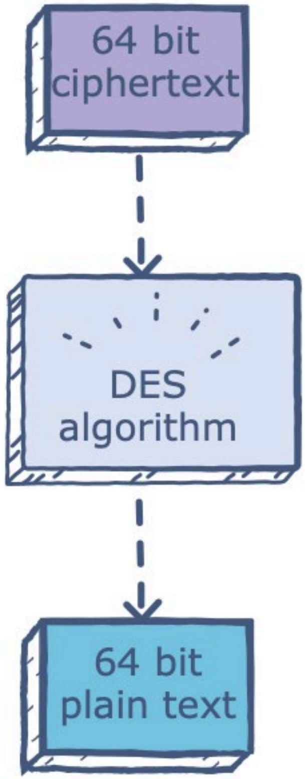
- Block Cipher
- symmetric key
- Out-dated now

### History

- 1972: National Bureau of Standards begins search
- 1975: DES: Lucifer by IBM, modified by NSA Approved by NBS ‘76, ANSI ‘81
- renewed every 5 years by NIST
- now considered obsolete



**Encryption**

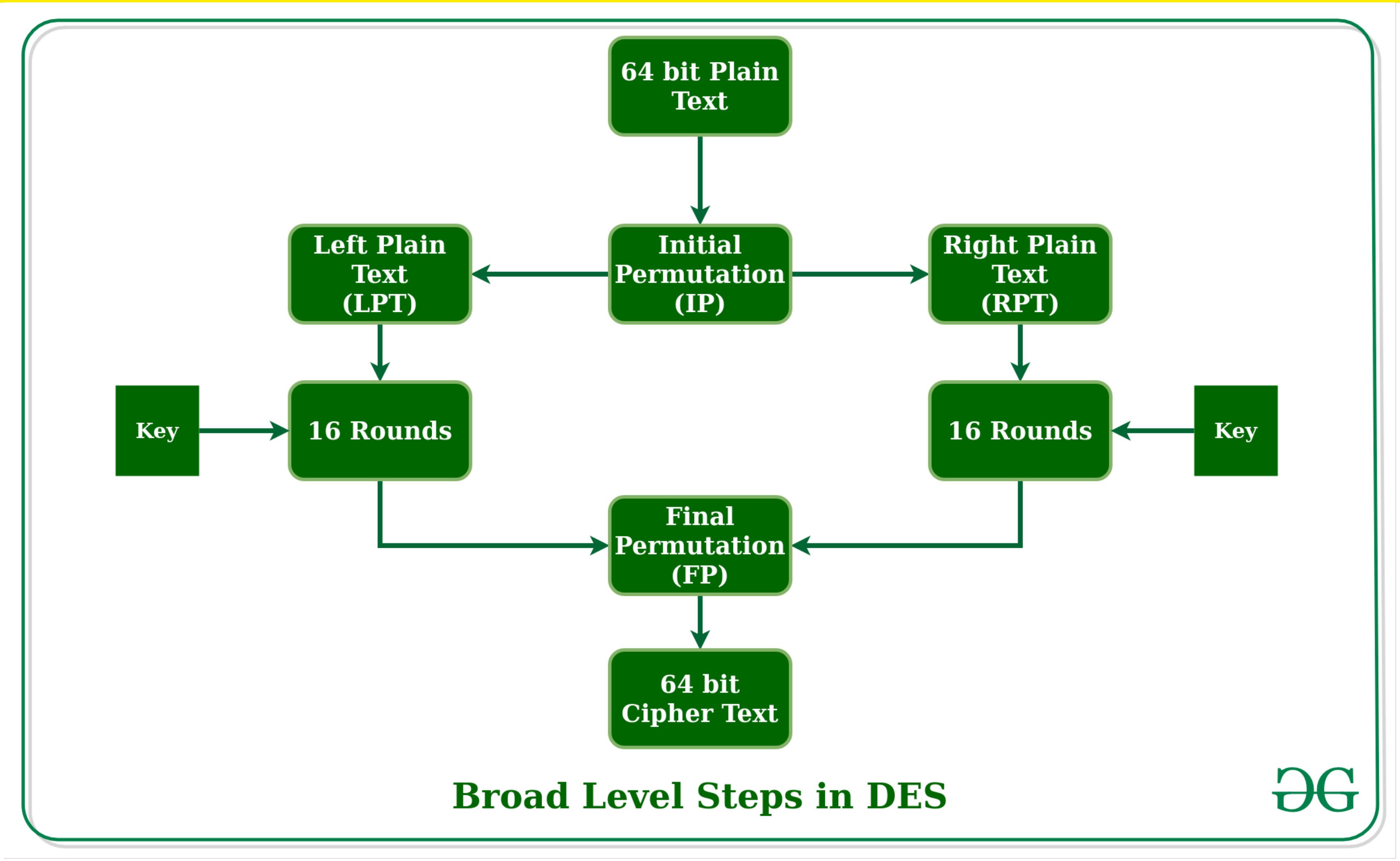


**Decryption**

# DES

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64 bit plaintext input
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase  (“Strong cryptography makes the world a safer place”) decrypted (brute force) in 4 months
  - no known “backdoor” decryption approach
- making DES more secure
  - use three keys sequentially (3-DES) on each datum (triple DES)
  - use cipher-block chaining

# How does DES work



Broad Level Steps in DES

https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

# Advantages

1. DES has been around a long time (since 1977), even now no real weaknesses have been found: the most efficient attack is still brute force.
2. DES is an official United States Government standard; the Government is required to re-certify, DES every five years and ask it be replaced if necessary.
3. DES is also an ANSI and ISO standard - anybody can learn the details and implement it.
4. Since DES was designed to run on 1977 hardware, it is fast in hardware and ***relatively*** fast in software.

# Disadvantages

1. The 56-bit key size is the biggest defect of DES.
2. DES was not designed for software and hence runs relatively slowly.
3. As the technology is improving lot more day by day so there is a possibility to break the encrypted code, so AES is preferred than DES.
4. Only one private key is used for encryption as well as for decryption.