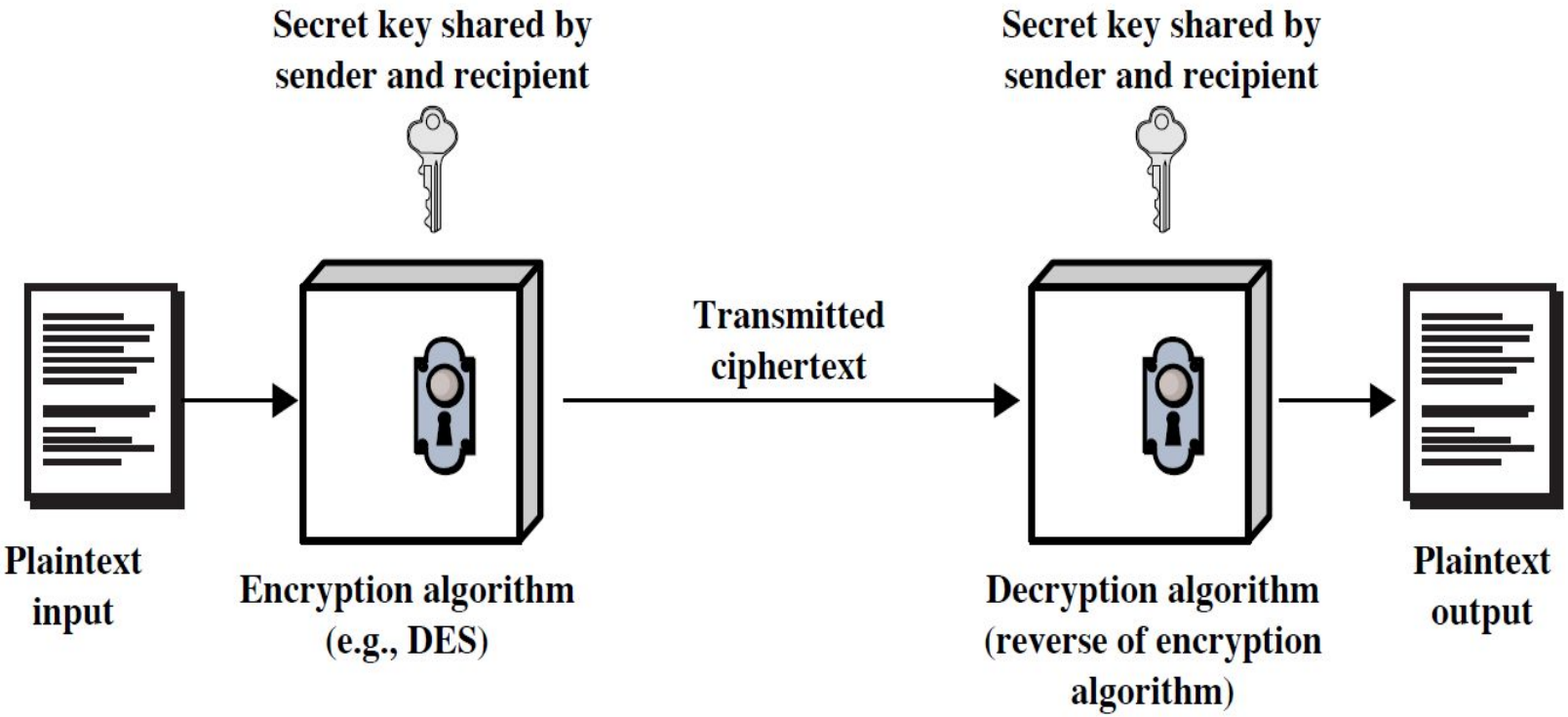
# Classical Encryption Techniques

# Goal

To introduce basic concepts & terminology of encryption

# Symmetric Cipher Model



# Caesar Cipher

- Earliest known substitution cipher
- Invented by Julius Caesar
- Each letter is replaced by the letter **three positions** further down the alphabet.
- 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
  Cipher: 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
- Example: ohio state □ RKLR VWDWH

# Caesar Cipher

- Mathematically, map letters to numbers:

  `a, b, c, ..., x,  y,  z`

  `0, 1, 2, ..., 23, 24, 25`

- Then the general Caesar cipher is:

  $c = E_K(p) = (p + k) \bmod 26$

  $p = D_K(c) = (c - k) \bmod 26$

- Can be generalized with any alphabet.

# Cryptanalysis of Caesar Cipher

- Key space:  {0, 1, ..., 25}
- Vulnerable to brute-force attacks.

# Monoalphabetic Substitution Cipher

- Shuffle the letters and map each plaintext letter to a different random ciphertext letter:

  Plain letters: abcdefghijklmnopqrstuvwxyz

  Cipher letters: DKVQFIBJWPESCXHTMYAUOLRGZN

  Plaintext: ifwewishtoreplaceletters

  Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

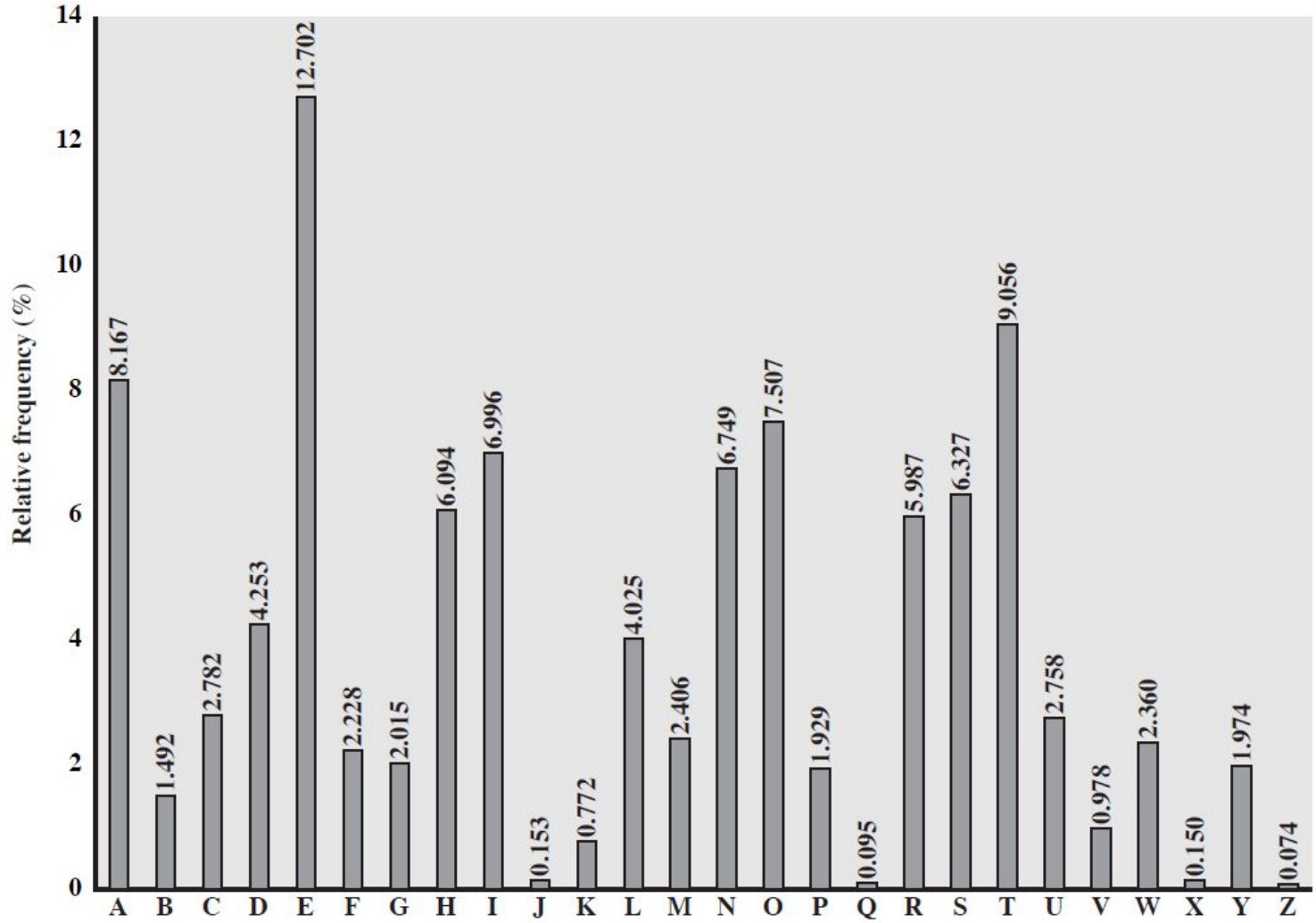
# Monoalphabetic Cipher Security

- Now we have a total of 26! = 4 x $10^{26}$ keys.
- With so many keys, it is secure against brute-force attacks.
- But not secure against some cryptanalytic attacks.
- Problem is language characteristics.

# Language Statistics and Cryptanalysis

- Human languages are not random.
- Letters are not equally frequently used.
- In English, E is by far the most common letter, followed by T, R, N, I, O, A, S.
- Other letters like Z, J, K, Q, X are fairly rare.

# English Letter Frequencies



# Use in Cryptanalysis

- Key concept: monoalphabetic substitution does not change relative letter frequencies

- To attack, we
  - calculate letter frequencies for ciphertext
  - compare this distribution against the known one

# Polyalphabetic Ciphers

- **Polyalphabetic substitution ciphers**
- Improve security using multiple cipher alphabets
- Make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- Use a key to select which alphabet is used for each letter of the message

# Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security.
- One approach to improving security is to encrypt multiple letters at a time.
- The **Playfair Cipher** is the best known such cipher.
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

# Playfair Key Matrix

- Use a 5 x 5 matrix.
- Fill in letters of the key (w/o duplicates).
- Fill the rest of matrix with other letters.
- E.g., key = MONARCHY.

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

# Encrypting and Decrypting

Plaintext is encrypted two letters at a time.

1. If a pair is a repeated letter, insert filler like 'X’.
2. If both letters fall in the same row, replace each with the letter to its right (circularly).
3. If both letters fall in the same column, replace each with the the letter below it (circularly).
4. Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.

# Security of Playfair Cipher

- A brute force attack on a Playfair  cipher is very difficult. The size of the key domain is 25! (factorial 25).
- Security is much improved over the simple monoalphabetic cipher.
- Was widely used for many decades
  - eg. by US & British military