Lecture 4 Symmetric Encryption (Part 2)

# Monoalphabetic Substitution Cipher

A monoalphabetic substitution cipher is a simple form of substitution cipher in cryptography where each letter of the plaintext is replaced by a corresponding letter from a fixed substitution alphabet. In other words, it involves substituting one letter in the plaintext with a different letter in the ciphertext. This substitution is done consistently throughout the entire message.

In a monoalphabetic cipher, each letter in the plaintext alphabet is mapped to a unique letter in the ciphertext alphabet. For example, if the letter "A" in the plaintext is always replaced with the letter "D" in the ciphertext, every occurrence of "A" in the message will be substituted with "D". This substitution pattern remains the same for all occurrences of each letter.

Monoalphabetic ciphers are relatively easy to understand and implement, but they are also highly vulnerable to frequency analysis attacks. This is because the same letter in the plaintext will always be replaced with the same letter in the ciphertext, allowing an attacker to analyze the frequency of letters in the ciphertext and make educated guesses about their corresponding letters in the plaintext.

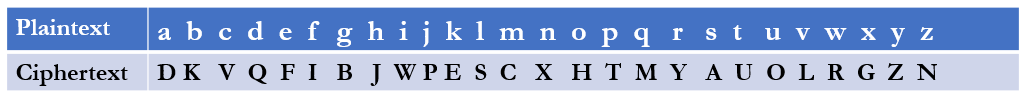
Examples: Caesar Cipher, Atbash Cipher, Simple Substitution Cipher, Keyword Cipher, Pigpen Cipher.

## Simple Substitution Cipher

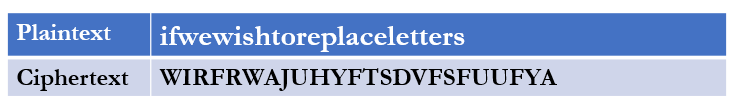
A Simple Substitution Cipher is a type of monoalphabetic cipher where each letter in the plaintext is replaced by a different letter in the ciphertext. The substitution is determined by using a fixed and consistent mapping between the letters of the plaintext alphabet and the corresponding letters of the ciphertext alphabet.

To create a Simple Substitution Cipher, a substitution key or alphabet is chosen. This substitution key is a random permutation of the letters in the alphabet. Each letter in the plaintext is then replaced with its corresponding letter from the substitution key.

For example, let's say the substitution key is as follows:



Using this substitution key, the following would be a plaintext to ciphertext mapping:



It's important to note that Simple Substitution Ciphers are vulnerable to frequency analysis attacks. Since each letter in the plaintext is always replaced by the same letter in the ciphertext, an attacker can analyze the frequency of letters in the ciphertext and make educated guesses about their corresponding letters in the plaintext.

### Security of Simple Substitution Cipher

Simple Substitution Cipher has a total of 26! keys. With so many keys, one can think Simple Substitution Ciphers are secure, but it is a wrong assumption. Simple Substitution Ciphers are vulnerable to frequency analysis attacks.

# Frequency Analysis

Frequency analysis is a technique used in cryptanalysis, which is the study of breaking codes and ciphers. It involves analyzing the frequency distribution of letters, symbols, or other linguistic units in a given piece of encrypted text (ciphertext) in order to gain insights about the underlying plaintext. Frequency analysis attacks are particularly effective against simple substitution ciphers, where each letter in the plaintext is replaced by a corresponding letter in the ciphertext according to a fixed rule.

The basic idea behind frequency analysis is that in any language, certain letters or symbols appear more frequently than others. By observing the frequency of letters in the ciphertext and comparing it to the expected frequency distribution of letters in the target language, the attacker can deduce the substitution rules and ultimately decrypt the message.

For example, in English, the letter "E" is the most commonly used letter, followed by "T," "A," and so on (Figure 1). By examining the frequency of letters or symbols in the ciphertext, an attacker can make educated guesses about the substitution pattern used in the encryption.

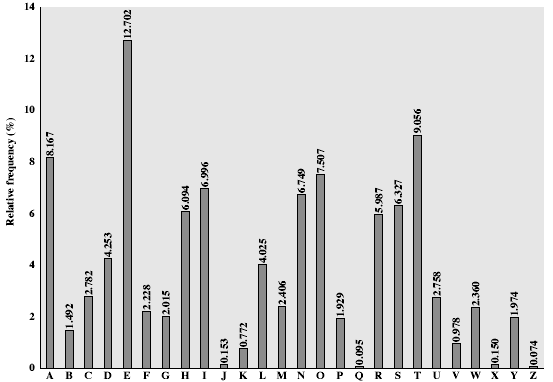
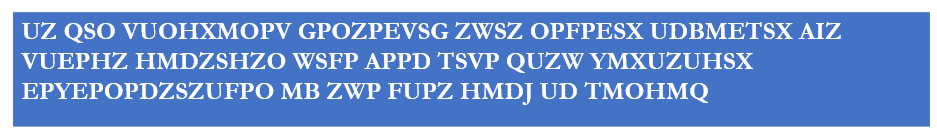


Figure : English Letter Frequencies

The key concept is that monoalphabetic substitution ciphers do not change relative letter frequencies. Discovered and studied extensive by Arab Muslim polymath Al-Kindi in 9th century. By examining the frequency of letters or symbols in the ciphertext, an attacker can make educated guesses about the substitution pattern used in the encryption.

**Example Cryptanalysis**

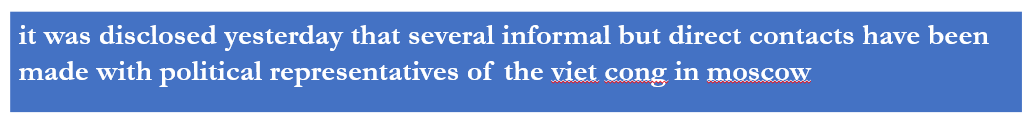
Ciphertext:



Steps:

* Count relative letter frequencies (see text)
* Assume ‘P’ and ‘Z’ are ‘e’ and ‘t’
* Guess ‘ZW’ is ‘th’ and hence ‘ZWP’ is ‘the’
* Proceed a trial-and-error to finally get the plaintext:

Finally get the following plaintext:



## Counter Measures

To counter frequency analysis attacks, more complex encryption techniques such as polyalphabetic ciphers, transposition ciphers, or modern cryptographic algorithms like AES or RSA are used. These methods make it much more difficult to discern patterns in the ciphertext and prevent attackers from exploiting the frequency distribution of letters.

# Polyalphabetic Substitution Cipher

Polyalphabetic substitution cipher is a cryptographic technique that involves the use of multiple substitution alphabets. Unlike a monoalphabetic substitution ciphers where each letter is replaced by a fixed corresponding letter, in a polyalphabetic substitution cipher, the substitution rules vary based on the position of the letter within the plaintext. This approach makes frequency analysis (cryptanalysis) harder with more alphabets to guess.

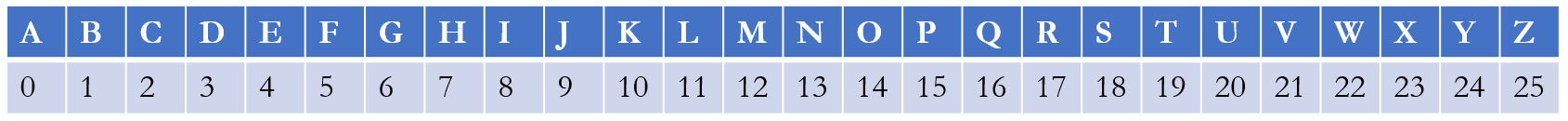
Examples: Vigenère Cipher, Beaufort Cipher, Autokey Cipher, Playfair Cipher, and Hill Cipher.

## Vigenère Cipher

The most well-known example of a polyalphabetic cipher is the Vigenère cipher. This cipher uses a keyword to determine the shifting of letters in multiple Caesar ciphers. The keyword is repeated to match the length of the plaintext, and each letter of the keyword determines the shift value for the corresponding letter of the plaintext.

Example 1:

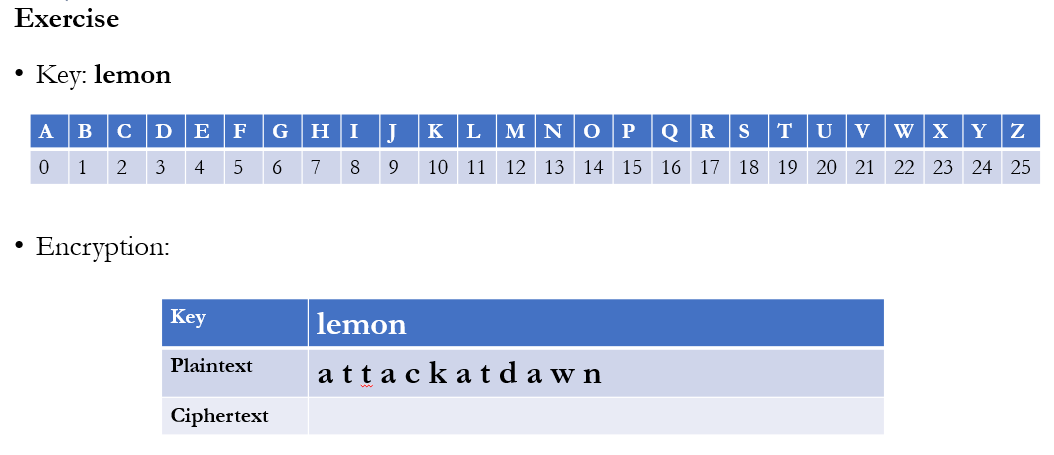
Key: ***deceptive***



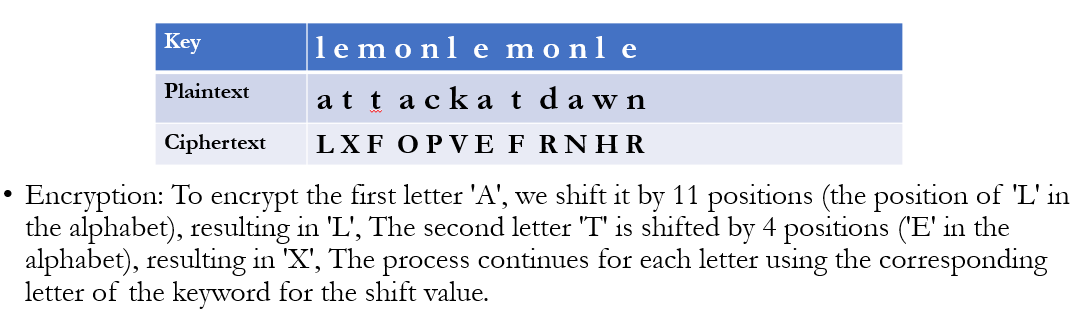
To encrypt the plaintext using the Vigenère cipher with the keyword “deceptive”, repeat the keyword to match the length of the plaintext.

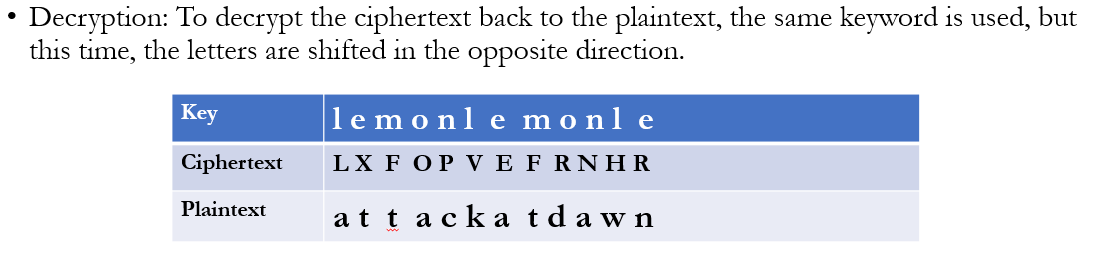


To encrypt the first letter 'w’, shift it by 3 positions (the position of ‘d’ in the alphabet), resulting in ‘Z’. The second letter ‘e’ is shifted by 4 positions (‘e’ in the alphabet), resulting in ‘I’. The process continues for each letter using the corresponding letter of the keyword for the shift value.



Solution:





# Transposition Cipher

Transposition ciphers are a type of cryptographic technique that involves rearranging the order of letters or characters in a message without altering the actual letters themselves. Instead of substituting letters as in substitution ciphers, transposition ciphers focus on manipulating the positions or order of the letters.

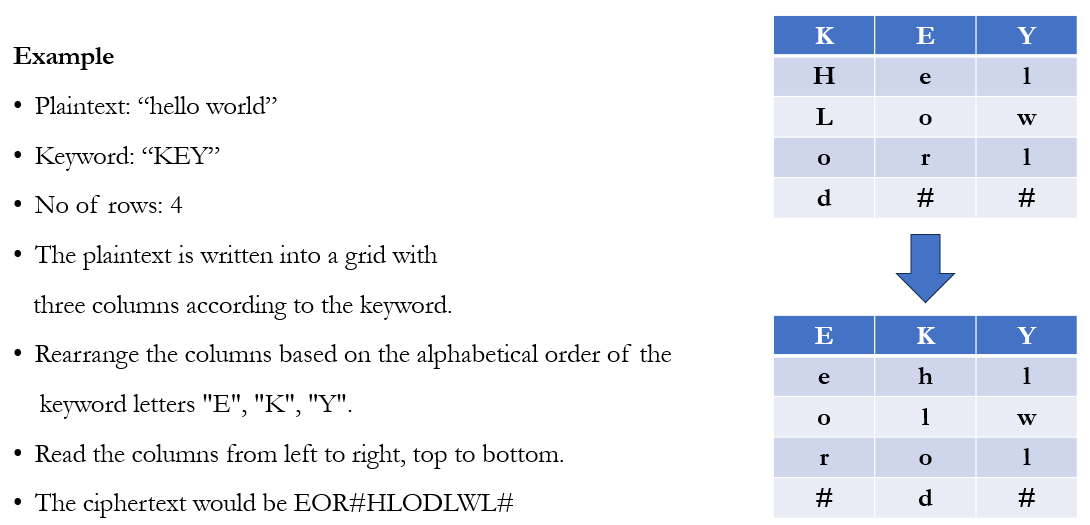
There are various methods for implementing transposition ciphers, but the underlying principle remains the same: the original letters remain unchanged, but their arrangement is altered according to a specific rule or pattern.

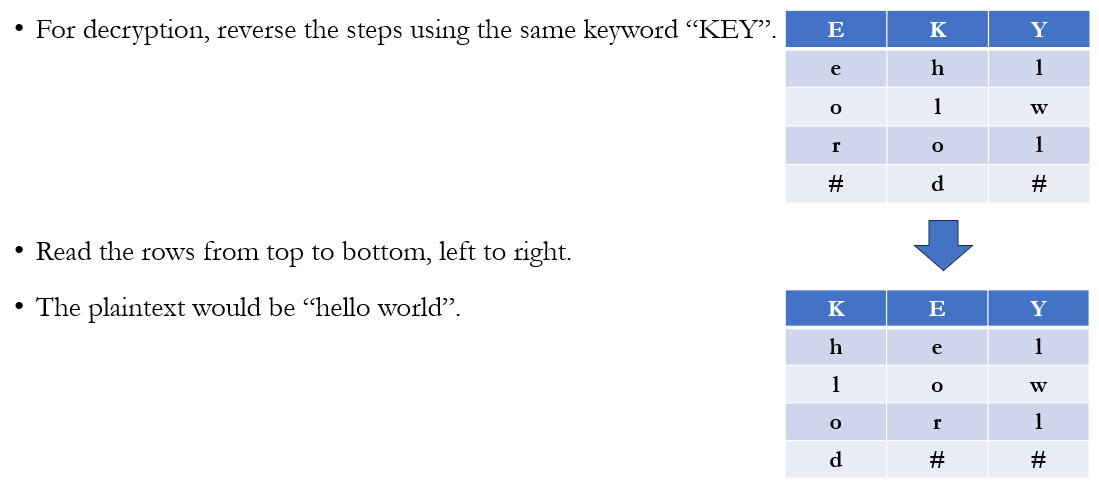
Transposition ciphers can operate on individual letters, groups of letters, or even blocks of characters. The rearrangement of the text can occur horizontally (row-wise) or vertically (column-wise). The resulting ciphertext maintains the same characters as the plaintext but alters their arrangement, making it difficult for an unauthorized recipient to read the original message.

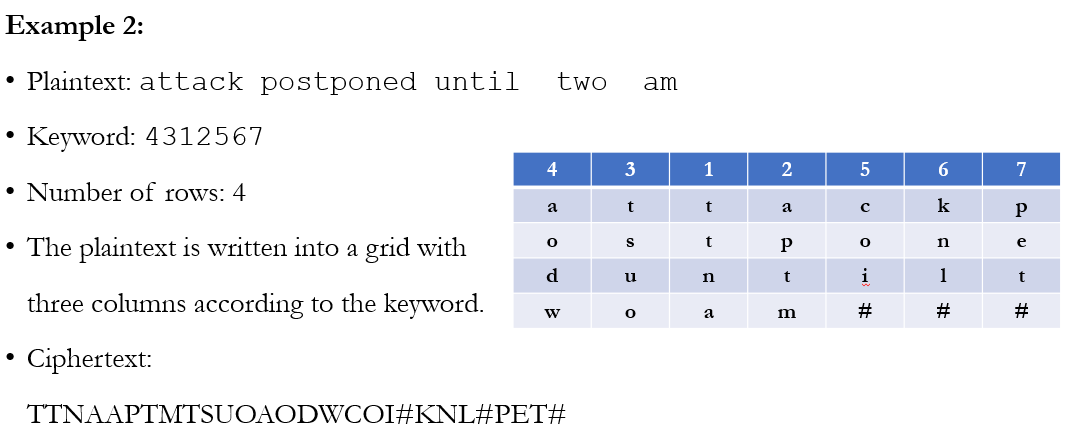
A few common types of transposition ciphers are Columnar Transposition Cipher, Rail Fence Cipher, Route Cipher, and Scytale Cipher.

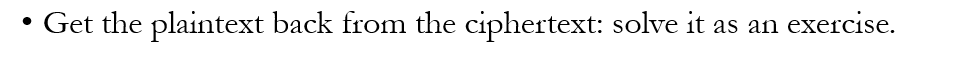
## Columnar Transposition Cipher

This type of cipher rearranges the characters of a plaintext message by writing it out in a grid of a fixed number of columns and then reading the ciphertext off column by column. The key determines the order in which the columns are read. This cipher preserves the original letters but changes their order, making the message difficult to decipher without knowledge of the column arrangement.









# Reference

[1] Book: Cryptography and Network Security, 7th Edition. Chapter 3, Sections 3.1, 3.2, and 3.3.