

CVS8301:Cryptography

Theory and Applications -

Lecture 2

Habeebah Adamu Kakudi (Mrs) PhD

2025-08-24

Table of contents

| | |
|---|----------|
| 1 Lecture Notes: Classical Cryptographic Algorithms | 5 |
| 1.1 Introduction to Classical Cryptography | 5 |
| 1.2 Key Concepts and Terminology | 5 |
| 1.3 Caesar Cipher: A Classical Substitution Technique | 6 |
| 1.3.1 Overview | 6 |
| 1.3.2 Mathematical Formulation | 6 |
| 1.3.3 Example | 7 |
| 1.3.4 Cryptanalytic Evaluation | 7 |
| 1.3.4.1 Strengths | 7 |
| 1.3.4.2 Weaknesses | 8 |
| 1.3.5 Historical and Educational Relevance | 8 |

| | | |
|--------|---|----|
| 1.4 | Excercise | 8 |
| 1.5 | Vigenère Cipher: A Polyalphabetic Substitution System | 8 |
| 1.5.1 | Historical Context | 8 |
| 1.6 | Cipher Description | 9 |
| 1.6.1 | Mathematical Formulation | 9 |
| 1.7 | Worked Example | 10 |
| 1.8 | Diagram (Mermaid) | 11 |
| 1.9 | Cryptanalytic Evaluation | 11 |
| 1.9.1 | Strengths | 11 |
| 1.9.2 | Weaknesses | 11 |
| 1.10 | Applications and Legacy | 12 |
| 1.10.1 | Educational Use | 12 |
| 1.10.2 | Cultural Reference | 12 |
| 1.11 | Summary | 12 |
| 1.12 | Excercise | 13 |

| | | |
|----------|---|-----------|
| 2 | Substitution vs. Transposition in Classical Cryptography | 13 |
| 2.1 | Conceptual Distinction | 13 |
| 2.2 | Historical Context | 14 |
| 2.2.1 | Substitution | 14 |
| 2.2.2 | Transposition | 14 |
| 2.3 | Substitution Ciphers | 14 |
| 2.3.1 | Mechanism | 14 |
| 2.3.2 | Mathematical Model | 15 |
| 2.3.3 | Example | 15 |
| 2.3.4 | Cryptanalytic Insight | 15 |
| 2.4 | Transposition Ciphers | 16 |
| 2.4.1 | Mechanism | 16 |
| 2.4.2 | Mathematical Model | 16 |
| 2.4.3 | Example | 16 |

| | | |
|--------|---|----|
| 2.4.4 | Cryptanalytic Insight | 17 |
| 2.5 | Comparative Analysis | 17 |
| 2.6 | Applications in Modern Cryptography | 17 |
| 2.6.1 | Substitution | 17 |
| 2.6.2 | Transposition | 18 |
| 2.7 | Case Study: Hybrid Classical Cipher | 18 |
| 2.7.1 | Scenario | 18 |
| 2.7.2 | Excercise | 18 |
| 2.7.3 | Result | 18 |
| 2.8 | Summary | 19 |
| 2.9 | Frequency Analysis in Classical Cryptanalysis | 19 |
| 2.9.1 | Conceptual Foundation | 19 |
| 2.9.2 | Historical Significance | 19 |
| 2.10 | Methodology | 20 |
| 2.10.1 | Step-by-Step Procedure: | 20 |
| 2.10.2 | Example Frequency Table (English): | 20 |
| 2.11 | Applied Activity: Caesar Cipher Analysis | 21 |
| 2.11.1 | Ciphertext: | 21 |
| 2.11.2 | Observed Frequencies: | 21 |
| 2.11.3 | Hypothesis: | 21 |
| 2.11.4 | Decryption Attempt (Shift = 3): | 21 |
| 2.11.5 | Result: | 23 |
| 2.12 | Cryptanalytic Insights | 23 |
| 2.12.1 | Strengths: | 23 |
| 2.12.2 | Limitations: | 23 |
| 2.13 | Advanced Techniques | 24 |
| 2.13.1 | Modern Relevance | 24 |
| 2.14 | Activities | 24 |
| 2.14.1 | Manual Encryption/Decryption | 24 |
| 2.14.2 | Decoding Challenge | 25 |

| | |
|---|----|
| 2.15 Exercises | 25 |
| 2.15.1 Group Discussion Prompts | 25 |
| 2.15.2 Cipher Challenge Worksheet | 25 |
| 2.15.3 Group Discussion | 25 |

1 Lecture Notes: Classical Cryptographic Algorithms

1.1 Introduction to Classical Cryptography

Classical cryptography refers to the early methods of securing communication before the advent of digital computers. These techniques laid the foundation for modern cryptographic systems and are still studied today for their simplicity, educational value, and historical significance.

1.2 Key Concepts and Terminology

| Term | Definition |
|--------------------|---|
| Cipher | An algorithm for transforming plaintext into ciphertext |
| Substitution | Replacing each element of plaintext with another symbol |
| Transposition | Rearranging the order of plaintext characters without changing them |
| Frequency Analysis | A cryptanalytic technique that studies the frequency of letters or groups |

1.3 Caesar Cipher: A Classical Substitution Technique

1.3.1 Overview

The Caesar cipher is one of the earliest known and simplest forms of encryption, classified as a **monoalphabetic substitution cipher**. It operates by shifting each letter of the plaintext by a fixed number of positions down the alphabet. This transformation is consistent across the entire message, making it deterministic and easily reversible with knowledge of the shift value.

Historically attributed to **Julius Caesar**, who reportedly used it to protect military communications, the cipher exemplifies the foundational principles of substitution-based cryptography.

1.3.2 Mathematical Formulation

Let each letter be represented by an integer value from 0 to 25 (A = 0, B = 1, ..., Z = 25). The encryption function is defined as:

$$E_k(x) = (x + k) \mod 26$$

Where:

- x is the plaintext letter's numeric value
- k is the fixed shift (key)
- $E_k(x)$ is the resulting ciphertext letter

Decryption is performed using:

$$D_k(y) = (y - k) \mod 26$$

1.3.3 Example

Given a shift value $k = 3$:

- **Plaintext:** HELLO
- **Numeric Mapping:** H(7), E(4), L(11), L(11), O(14)
- **Ciphertext:** KHOOR → K(10), H(7), O(14), O(14), R(17)



1.3.4 Cryptanalytic Evaluation

1.3.4.1 Strengths

- **Simplicity:** Easy to implement manually or programmatically.
- **Pedagogical Value:** Ideal for introducing core cryptographic concepts.

1.3.4.2 Weaknesses

- **Limited Keyspace:** Only 25 non-trivial shifts, making brute-force attacks trivial.
- **Frequency Preservation:** Letter frequencies remain unchanged, enabling effective frequency analysis.
- **Lack of Key Confidentiality:** Once the shift is known, all messages encrypted with that key are compromised.

1.3.5 Historical and Educational Relevance

Despite its vulnerabilities, the Caesar cipher remains a cornerstone in cryptographic education. It illustrates the importance of key secrecy, the limitations of deterministic substitution, and the evolution toward more secure systems like polyalphabetic ciphers and modern block ciphers.

1.4 Excercise

1. Simulate the Ceaser cipher in Python

1.5 Vigenère Cipher: A Polyalphabetic Substitution System

1.5.1 Historical Context

The **Vigenère Cipher**, often misattributed to Blaise de Vigenère, was first described by Giovan Battista Bellaso in 1553. Vigenère later

published a stronger autokey variant in 1586, but the cipher bearing his name became widely known as a **polyalphabetic substitution cipher**—a significant advancement over the monoalphabetic Caesar cipher.

For centuries, the Vigenère cipher was considered unbreakable and earned the nickname *le chiffre indéchiffrable* (“the indecipherable cipher”) until Charles Babbage and Friedrich Kasiski independently developed methods to break it in the 19th century.

1.6 Cipher Description

The Vigenère cipher encrypts alphabetic text by applying a series of Caesar shifts based on the letters of a **repeating keyword**. Each letter in the plaintext is shifted by an amount determined by the corresponding letter in the keyword.

1.6.1 Mathematical Formulation

Let:

- P_i be the i^{th} letter of the plaintext (as an integer from 0 to 25)
- K_i be the i^{th} letter of the keyword (repeated as needed)
- C_i be the resulting ciphertext letter

Then:

$$C_i = (P_i + K_i) \mod 26$$

Decryption is performed using:

$$P_i = (C_i - K_i + 26) \mod 26$$

1.7 Worked Example

- **Plaintext:** HELLO
 - H(7), E(4), L(11), L(11), O(14)
 - K(10), E(4), Y(24), K(10), E(4)
- **Keyword:** KEY
 - H + K = 7 + 10 = 17 → R
 - E + E = 4 + 4 = 8 → I
 - L + Y = 11 + 24 = 35 → 9 → J
 - L + K = 11 + 10 = 21 → V
 - O + E = 14 + 4 = 18 → S
- **Ciphertext:** RIJVS

1.8 Diagram (Mermaid)



1.9 Cryptanalytic Evaluation

1.9.1 Strengths

- **Polyalphabetic Nature:** Each letter is encrypted differently, reducing frequency signature.
- **Keyword Flexibility:** Longer keywords increase resistance to brute-force and statistical attacks.
- **Historical Importance:** Introduced the concept of key-dependent encryption cycles.

1.9.2 Weaknesses

- **Repetition Vulnerability:** If the keyword is short or reused, patterns emerge.
- **Kasiski Examination:** Detects repeated sequences in ciphertext to infer keyword length.
- **Frequency Analysis:** Once keyword length is known, ciphertext can be split and analyzed as Caesar ciphers.

1.10 Applications and Legacy

While obsolete for modern security, the Vigenère cipher remains a pedagogical tool in cryptography education. It introduces key concepts such as:

- Key-dependent encryption
- Modular arithmetic
- Statistical cryptanalysis

1.10.1 Educational Use

Used in introductory cryptography courses to demonstrate the evolution from monoalphabetic to polyalphabetic systems.

1.10.2 Cultural Reference

Featured in puzzles, escape rooms, and historical fiction involving secret codes.

1.11 Summary

The Vigenère cipher represents a pivotal moment in cryptographic history—where the limitations of simple substitution were overcome by introducing key-dependent variability. Though vulnerable to modern cryptanalysis, its conceptual elegance and historical significance make it a cornerstone of classical cipher studies.

1.12 Excercise

1. Simulate the Vigenère cipher in Python

2 Substitution vs. Transposition in Classical Cryptography

Cryptographic systems are broadly categorized by the transformation techniques they employ. Two foundational methods—**substitution** and **transposition**—have shaped the evolution of encryption from ancient ciphers to modern algorithms. Understanding their mechanics, strengths, and vulnerabilities is essential for analyzing both historical and contemporary cryptographic schemes.

2.1 Conceptual Distinction

| Technique | Description | Transformation Type |
|----------------------|--|-------------------------------|
| Substitution | Replaces each symbol in the plaintext with another symbol according to a defined rule or key | Symbol-level transformation |
| Transposition | Rearranges the symbols of the plaintext without altering their identity | Position-level transformation |

2.2 Historical Context

2.2.1 Substitution

- **Earliest Use:** Attributed to Julius Caesar (~1st century BCE) with the Caesar cipher.
- **Evolution:** Grew into polyalphabetic systems like the Vigenère cipher.
- **Legacy:** Formed the basis for modern block cipher substitution layers (e.g., AES S-boxes).

2.2.2 Transposition

- **Ancient Use:** Spartan scytale (~5th century BCE) used physical rearrangement.
- **Modernization:** Columnar transposition and rail fence ciphers became popular in military communications.
- **Legacy:** Inspired permutation operations in modern cryptographic primitives.

2.3 Substitution Ciphers

2.3.1 Mechanism

Each character in the plaintext is replaced with a corresponding character from a substitution alphabet or rule.

2.3.2 Mathematical Model

Let P be the plaintext character and K be the substitution key. The ciphertext C is:

$$C = S_K(P)$$

Where S_K is the substitution function defined by the key.

2.3.3 Example

- Plaintext: **ATTACK**
- Substitution Rule: A → D, T → W, C → F, K → N
- Ciphertext: **DWWDFN**

2.3.4 Cryptanalytic Insight

- **Monoalphabetic substitution** preserves frequency distribution, making it vulnerable to frequency analysis.
- **Polyalphabetic substitution** (e.g., Vigenère) mitigates this but is still susceptible to statistical attacks if the key is short or reused.

2.4 Transposition Ciphers

2.4.1 Mechanism

Characters are rearranged according to a fixed permutation pattern or key, without altering the actual symbols.

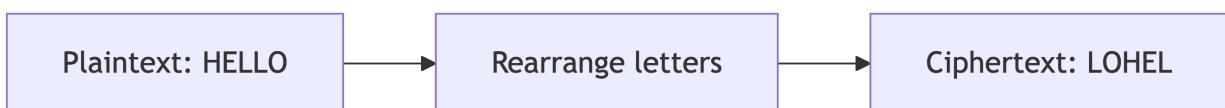
2.4.2 Mathematical Model

Let $P = p_1, p_2, \dots, p_n$ be the plaintext and π be a permutation of indices. The ciphertext C is:

$$C = p_{\pi(1)}, p_{\pi(2)}, \dots, p_{\pi(n)}$$

2.4.3 Example

- Plaintext: **HELLO**
- Transposition Rule: Swap positions 1 4, 2 5
- Ciphertext: **LOHEL**



2.4.4 Cryptanalytic Insight

- Frequency distribution remains unchanged, making transposition resistant to basic frequency analysis.
- However, patterns in letter adjacency and structure can be exploited using anagramming and known-plaintext attacks.

2.5 Comparative Analysis

| Feature | Substitution | Transposition |
|-----------------|--------------------------|--------------------------------|
| Symbol Identity | Altered | Preserved |
| Frequency | Changed | Preserved |
| Distribution | (monoalphabetic) | |
| Vulnerability | Frequency analysis | Pattern recognition |
| Modern Usage | S-boxes in block ciphers | Permutation layers in AES, DES |

2.6 Applications in Modern Cryptography

2.6.1 Substitution

- **Advanced Encryption Standard (AES) S-box:** Non-linear substitution layer critical for confusion.
- **Stream ciphers:** Use dynamic substitution tables for keystream generation.

2.6.2 Transposition

- **DES Permutation Functions:** Initial and final permutations enhance diffusion.
- **Block cipher rounds:** Often alternate between substitution and permutation layers.

2.7 Case Study: Hybrid Classical Cipher

2.7.1 Scenario

A military cipher combines substitution and transposition:

1. Apply Caesar cipher (shift = 3)
2. Rearrange using columnar transposition (key = 3,1,2)

2.7.2 Excercise

1. Create your own hybrid classical cipher with a shift of not less than 5 and columnar transposition key

2.7.3 Result

- Enhanced security through layered transformation.
- Requires both frequency and positional analysis to break.

2.8 Summary

Substitution and transposition represent two fundamental paradigms in cryptographic transformation. While substitution alters symbol identity, transposition manipulates symbol order. Their combination—used in both classical and modern systems—provides the essential ingredients for **confusion** and **diffusion**, the twin pillars of secure cipher design.

2.9 Frequency Analysis in Classical Cryptanalysis

2.9.1 Conceptual Foundation

Frequency analysis is a cornerstone of classical cryptanalysis, exploiting the statistical regularities inherent in natural languages. In English, for instance, the letter **E** appears with the highest frequency (~12.7%), followed by **T**, **A**, **O**, **I**, and **N**. These patterns persist across large corpora and form the basis for decrypting substitution ciphers without prior knowledge of the key.

2.9.2 Historical Significance

- **Al-Kindi (9th century)**: Credited with formalizing frequency analysis in his treatise *Risalah fi Istikhraj al-Mu'amma* (“Manuscript on Deciphering Cryptographic Messages”), laying the foundation for statistical cryptanalysis.
- **European Renaissance**: Frequency analysis became a powerful tool against monoalphabetic ciphers used in diplomatic and military correspondence.

- **WWII Era:** Though classical frequency analysis was insufficient against Enigma, its principles informed early machine-based cryptanalysis.

2.10 Methodology

2.10.1 Step-by-Step Procedure:

1. **Collect Ciphertext:** Obtain a sufficiently long encrypted message.
2. **Tabulate Frequencies:** Count occurrences of each symbol.
3. **Compare with Language Models:** Use known frequency distributions (e.g., English letter frequencies).
4. **Hypothesize Substitutions:** Map high-frequency ciphertext symbols to likely plaintext equivalents.
5. **Iterate and Refine:** Use digraphs, trigraphs, and contextual clues to validate or adjust hypotheses.

2.10.2 Example Frequency Table (English):

| Letter | Frequency (%) |
|--------|---------------|
| E | 12.7 |
| T | 9.1 |
| A | 8.2 |
| O | 7.5 |
| I | 7.0 |
| N | 6.7 |

2.11 Applied Activity: Caesar Cipher Analysis

2.11.1 Ciphertext:

ZHOFRPH WR FUBSWRJUDSKB

2.11.2 Observed Frequencies:

- Z, H, O, F, R, P, M, W, etc.

2.11.3 Hypothesis:

- Likely Caesar cipher (monoalphabetic shift).
- Try common shifts (e.g., Caesar's original shift = 3).

2.11.4 Decryption Attempt (Shift = 3):

- Z → W
- H → E
- O → L
- F → C
- R → O

- $P \rightarrow M$

- $H \rightarrow E$

- $W \rightarrow T$

- $R \rightarrow O$

- $F \rightarrow C$

- $U \rightarrow R$

- $B \rightarrow Y$

- $S \rightarrow P$

- $W \rightarrow T$

- $R \rightarrow O$

- $J \rightarrow G$

- $U \rightarrow R$

- $D \rightarrow A$

- $S \rightarrow P$

- $K \rightarrow H$

- $B \rightarrow Y$

2.11.5 Result:

WELCOME TO CRYPTOGRAPHY

Successful decryption confirms Caesar cipher with shift = 3.

2.12 Cryptanalytic Insights

2.12.1 Strengths:

- Effective against monoalphabetic substitution ciphers.
- Requires no prior key knowledge.
- Can be automated for large-scale ciphertexts.

2.12.2 Limitations:

- Ineffective against polyalphabetic ciphers (e.g., Vigenère) without additional analysis.
- Requires sufficiently long ciphertext to yield statistically meaningful results.
- Vulnerable to countermeasures like homophonic substitution or nulls.

2.13 Advanced Techniques

- **Bigram/Trigram Analysis:** Examining common letter pairs (e.g., TH, HE) and triplets (e.g., THE, AND).
- **Index of Coincidence:** Measures likelihood that two randomly selected letters are the same—used to distinguish cipher types.
- **Kasiski Examination:** Identifies repeated patterns in polyalphabetic ciphers to infer key length.

2.13.1 Modern Relevance

While frequency analysis is largely obsolete against modern cryptographic algorithms (which ensure uniform ciphertext distributions), its principles remain foundational in:

- Linguistic forensics
- Steganalysis
- Machine learning for NLP
- Cybersecurity education

2.14 Activities

2.14.1 Manual Encryption/Decryption

- Encrypt your name using Caesar and Vigenère ciphers.
- Decrypt a message using frequency analysis.

2.14.2 Decoding Challenge

- Given ciphertext:
 - “GUVF VF N FRPERG ZRFFNTR”
 - Hint: ROT13 (Caesar with shift = 13)

2.15 Exercises

2.15.1 Group Discussion Prompts

- Why were classical ciphers effective in their time?
- What made them vulnerable to modern cryptanalysis?
- How do substitution and transposition differ in terms of security?

2.15.2 Cipher Challenge Worksheet

- Encrypt and decrypt messages using Caesar and Vigenère.
- Identify cipher type from given ciphertext.
- Apply frequency analysis to break a monoalphabetic cipher.

2.15.3 Group Discussion

- Present findings on strengths and weaknesses of classical ciphers.
- Debate: “Could Caesar cipher still be useful today?”