TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO GIỮA KÌ MÔN XÁC XUẤT THỐNG KÊ ỨNG DỤNG CHO CÔNG NGHỆ THÔNG TIN**

**MIDDLE TERM**

*Người hướng dẫn*: **GV. MAI DUY TÂN**

*Người thực hiện*: **PHẠM THÁI HỌC - 52000047**

Lớp **: 20050201**

Khoá  **: 24**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN/BÁO CÁO GIỮA KÌ MÔN HỆ CƠ SỞ DỮ LIỆU**

**MIDDLE TERM**

Người hướng dẫn: **GV. MAI DUY TÂN**

*Người thực hiện*: **PHẠM THÁI HỌC - 52000047**

Lớp **: 20050201**

Khoá  **: 24**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

LỜI CẢM ƠN

Em xin gửi lời cảm ơn đến thầy Mai Duy Tân và cô Nguyễn Thị Huỳnh Trâm người đã giảng dạy em môn xác suất thống kê ứng dụng cho công nghệ thông tin. Đồng thời thông em cũng cảm ơn khoa công nghệ thông tin đã tạo điều kiện để em có thể hoàn thành môn học.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi / chúng tôi và được sự hướng dẫn của GV Mai Duy Tân;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Phạm Thái Học*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Trong bài báo cáo này em đã được tiếp cần và nghiên cứu về 2 thuật toán dùng để mã hóa và giải mã, cụ thể là Monoalphabetic Substitution Cipher và frequency analysis

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc101470106)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc101470107)

[TÓM TẮT iv](#_Toc101470108)

[MỤC LỤC 1](#_Toc101470109)

[o Chapter 1: Introduction 2](#_Toc101470110)

[1.1 Encryption and decryption 2](#_Toc101470111)

[1.2 symmetric and asymmetric cryptosystem 3](#_Toc101470112)

[Types of cryptosystems 4](#_Toc101470113)

[Symmetric cryptosystem 4](#_Toc101470114)

[Asymmetric cryptosystem 5](#_Toc101470115)

[o Chapter 2: Monoalphabetic Substitution Cipher 7](#_Toc101470116)

[My answer: 7](#_Toc101470117)

[o Chapter 3: Frequency Analysis 9](#_Toc101470118)

[My answers: 9](#_Toc101470119)

[o Chapter 4: Experiments 15](#_Toc101470120)

[Monoalphabetic Substitution Cipher 15](#_Toc101470121)

[Frequency analysis : 38](#_Toc101470122)

[Reference: 42](#_Toc101470123)

o Chapter 1: Introduction

▪ Concepts about encryption and decryption; symmetric and

asymmetric cryptosystem…

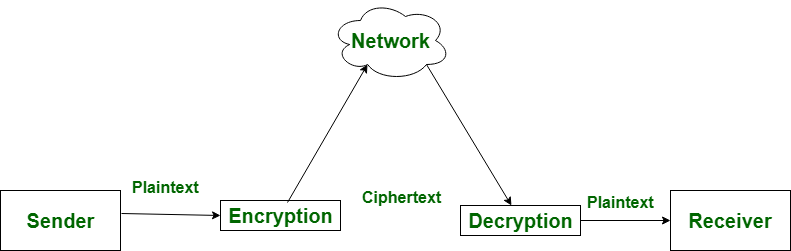
1.1 Encryption and decryption

Mã hóa và giải mã gồm các thành phầm:

* Plaintext: thông tin trước khi mã hóa
* Ciphertext: thông tin sau khi mã hóa
* Key: chìa khóa
* EID (Ecryption/Decryption): phương pháp mã hóa

Mã hóa (Encryption) là quá trình chuyển đổi thông điệp bình thường (plaintext thành thông điệp vô nghĩa (ciphertext).

Giải mã (Decryption) là quá trình chuyển đổi thông điệp vô nghĩa (Ciphertext) thành dạng ban đầu của nó (plantext).



mã hóa và giải mã

Một vài đặc điểm của mã hóa (Encryption) và giải mã (Decryption) cũng như sự khác nhau

|  |  |  |
| --- | --- | --- |
|  | Encryption (mã hóa) | Decryption (giải mã) |
| 1 | Mã hóa là quá trình biến thông điệp bình thường (plaintext) thành thông điệp vô nghĩa (Ciphertext) | Giãi mã là quá trình chuyển đổi thông điệp vô nghĩa (Ciphertext) thành dạng ban đầu (plaintext) |
| 2 | Encryption là quá trình diễn ra ở sender’s end. | Decryption là quá trình diễn ra ở receiver’s end. |
| 3 | Nhiệm vụ chính của nó là chuyển văn bản thuần túy (plaintext) thành văn bản mật mã (ciphertext) | Trong khi nhiệm vụ chính của decryption là chuyển đổi văn bản mật mã (Ciphertext) thành văn bản thuần tuý (playtext) |
| 4 | Bất kì tin nhắn nào cũng có thể được mã hóa bằng khóa bị mật (secret key) hoặc khóa công khai (public key) | Trong khi đó, thông điệp được mã hóa có thể được giải mã bằng khóa bí mật (secret key) hoặc khóa riêng (private key) |
| 5 | Trong quá trình mã hóa, người gữi (sender) gửi dữ liệu đến người nhận (receiver) sau khi được mã hóa. | Trong khi trong quá tình giải mã, người nhận (receiver) nhận thông tin (cipher text) và chuyển thành văn bản thuần túy (plain text) |

1.2 symmetric and asymmetric cryptosystem

* Mật mã (Cryptography) đảm bảo giao tiếp đầu cuối (end-to-end communication) an toàn bằng cách sử dụng mã hóa. Việc thực hiện các kỹ thuật mật mã khác nhau để cung cấp thông tin bảo mật được gọi là hệ thống mật mã. Những thành phần chình của hệ thống mật mã như sau:
* **Plaintext**: là thông điệp (message) đầu vào cần được mã hóa.
* **Encryption key**: Người gữi của plaintext (sender of the plaintext) yêu cầu khóa này để mã hóa
* **Encryption algorithm**: Thuật toán này lấy plaintext và encryption key làm đầu vào để xuất ra thông điệp được mã hóa
* **Ciphertext**: là đầu ra của thông điệp được mã hóa
* **Decryption key**: Người nhận của plaintext (receiver) yêu cầu khóa này để giải hóa
* **Decryption algorithm**: Đây là thuật toán mã hóa đảo ngược Nó lấy bản mã (ciphertext) và decryption key làm đầu vào và đầu ra là thông điệp đã giải mã (plaintext)

Types of cryptosystems

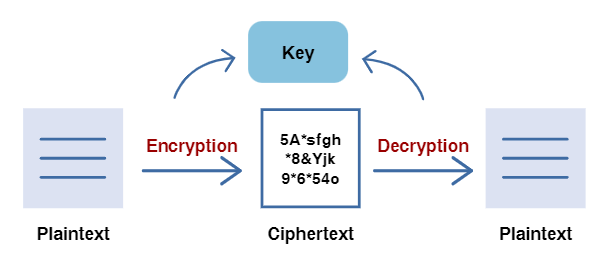
Dựa vào sự khác nhau trong mã hóa và giải mã, chúng ta có thể phân lại hệ thống mật mã thành 2 loại

* Symmetric Cryptosystem (hệ thống mật mã đối xứng).
* Asymmetric Cryptosystem (hệ thống mật mã không đối xứng.

Sự khác nhau cơ bản giữa chúng là hệ thống mật mã đối xứng (symmetric cryptosystem) chỉ liên quan đến 1 khóa mà hệ thống sử dụng để mã hóa và giải mã. Trong khi hệ thống mật mã không đối xứng (Asymmetric cryptosystem) sử dụng hai khóa (private và public) cho mã hóa và giải mã.

Symmetric cryptosystem

Vì hệ thống mật mã đối xứng (symmetric cryptosystem) sử dụng cùng một khóa để mã hóa và giải mã, người gửi và người nhận cần biết khóa trước khi trao đổi thông điệp. Đối với điều này, hệ thống sử dụng các giao thức trao đổi khóa (key exchange protocol) (như Giao thức Diffie-Hellman) để đảm bảo rằng người gửi (sender) và người nhận (receiver) đồng ý về khóa bí mật trước khi bắt đầu giao tiếp. Hình minh họa bên dưới mô tả mã hóa và giải mã đối xứng (symmetric encryption and decryption) sử dụng cùng một khóa:

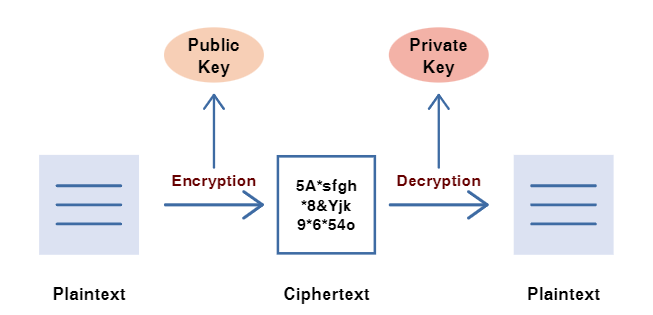


Symmetric Cryptosystem

Đối với các thuật toán mã hóa, hệ thống mật mã đối xứng sử dụng AES-128, AES-192 và AES-256. Quá trình mã hóa thường nhanh hơn trong các hệ thống mật mã đối xứng do độ dài khóa nhỏ hơn. Hạn chế của hệ thống này là người gửi và người nhận cần phải trao đổi khóa trước khi giải mã thông điệp. Nếu các khóa không được thay đổi thường xuyên, hệ thống sẽ dễ bị tấn công vì kẻ tấn công có thể sử dụng khóa bị rò rỉ để làm gián đoạn liên lạc. Hệ thống mật mã đối xứng sử dụng MACs để cung cấp tính toàn vẹn và xác thực.

Asymmetric cryptosystem

Hệ thống mật mã không đối xứng vượt qua các thách thức của hệ thống mật mã đối xứng bằng cách loại bỏ nhu cầu chia sẻ khóa trước trước khi khi giao tiếp. Hệ thống mật mã không đối xứng sử dụng hai khóa riêng tư và công khai (private key and public key) có liên quan đến nhau về mặt toán học. Điểm mạnh của bảo mật nằm ở các thuộc tính của các khóa này vì nó không khả thi về mặt tính toán để tính toán một khóa này bằng cách sử dụng khóa kia. Mỗi người gửi (sender) và người nhận (receiver) sẽ có cặp khóa riêng tư (private key pair) của họ trong hệ thống này.

Giả sử A muốn gửi một tin nhắn cho B, A sẽ cần sử dụng khóa công khai (public key) của B để mã hóa tin nhắn và B sẽ giải mã tin nhắn bằng khóa riêng (private key) của họ. Hình minh họa bên dưới mô tả mã hóa và giải mã không đối xứng bằng hai khóa: 

Asymmetric cryptosystem

Đối với các thuật toán mã hóa, hệ thống mật mã không đối xứng sử dụng các lược đồ Mã hóa El Gamal hoặc Mã hóa RSA. Quá trình mã hóa chậm hơn so với mã hóa đối xứng do kích thước khóa lớn hơn. Hệ thống mật mã không đối xứng an toàn hơn vì các cặp khóa riêng tư và khóa công khai (private and public key) ít có khả năng bị rò rỉ và dự đoán hơn. Hệ thống mật mã không đối xứng sử dụng chữ ký RSA để cung cấp tính toàn vẹn và xác thực.

o Chapter 2: Monoalphabetic Substitution Cipher

▪ State the problem, constrains/conditions (if any),

method/algorithm,

▪ Examples,

▪ Your comment, analysis, evaluation…

My answer:

* State the problem, constrains/conditions, method/algorithm:
  + Mono-alphabetic cipher là một mật mã thay thế nơi mà mỗi ký tự của đoạn văn bản ban đầu (plaintext) bị thay thế bởi các ký tự khác trong bảng chữ cái alphabet thành một văn bản mã hóa (ciphertext) dựa vào một alphabetic key.
* Constrains/ conditions:
* Plain text: đây là đoạn văn bản đầu vào cần được mã hoá
* Aphabetic key: đây là một bảng chữ cái xáo trộn của các chữ cái trong bảng chữ cái (có thể chứa ký tự đặc biệc)
* Cipher text: Là đoạn văn bản sau khi được mã hõa
* Method:
* Monoalphabetic Cipher hoạt động bằng cách thay thế mỗi ký tự của văn bản ban đầu plaintext (Và đôi khi là puntuation marks và spaces) bằng một ký tự khác (thâm chí có thể là một ký hiệu ngẫu nhiên)
* Example:
* Ví dụ 1: Với một văn bản plain text: “helloworld”
* Giả sử với một alphabetic key là “fuvgndkbrozqaljsywhtciempx”, ta có bảng sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alphabet | 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 |
| Alphabetic key | f | u | v | g | n | d | k | b | r | o | z | q | a | l | j | s | y | w | h | t | c | i | e | m | p | x |

* Thì plain text “**helloworld**” sẽ được mã hóa thành một ciphertext “**bnqqjejwqg”** do:
  + Chữ h được thay thế thành chữ b.
  + Chữ e được thay thế thàn chữ n.
  + Chữ l được thay thế thành chữ q.
  + Chữ o được thay thế thành chữ j.
  + Chữ w được thay thế thành chữ e.
* Ví dụ 2: Với một văn bản plaintext: “Hello world. I am a student at Ton Duc Thang University”
* Giả sử với alphabetic key là “bwgnsjpfaevykcrqzudhmtlxio”, ta có bảng sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alphabet | 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 |
| Alphabetic key | b | w | g | n | s | j | p | f | a | e | v | y | k | c | r | q | z | u | d | h | m | t | l | x | i | o |

* Thì plain text **“Hello world. I am a student at Ton Duc Thang University”** sẽ được mã hóa thành ciphertext: “fsyyr lruyn. abk b dhmnsch bh hrc nmg hfbcp mcatsudahi” do các ký tự của plain text đã được ánh xã thành ký tự trong alphabetic key ví dụ như:
  + a -> b, b ->w, c -> g, …
* My comments, analys, evaluation: thuật toán Monoalphabetic Substitution Cipher là một thuật toán bảo mật an toàn v. Với alphabetic key sẽ có tới 26! cách chọn các ký tự thay thế với vét cạn sẽ mất rất rất nhiều thời gian để giải mã.

o Chapter 3: Frequency Analysis

▪ State the problem, constrains/conditions (if any),

method/algorithm,

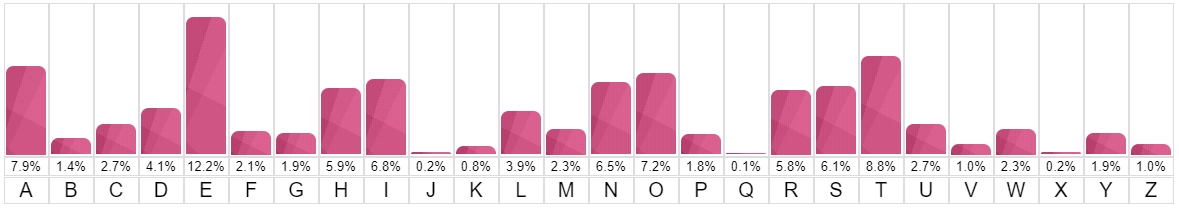
▪ Examples,

▪ Your comment, analysis, evaluation…

My answers:

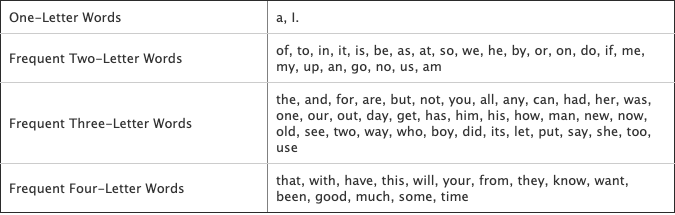
▪ State the problem: Trong giải mã, Frequency analysis là một thuật toán nghiên cứu về số lần lặp lại của ký tự (frequency of letters) hoặc nhóm các ký tự của đoạn văn bản cần giải mã (cipher text).

▪ constrains/conditions (if any): trong frequency analysis có 1 bảng ký tự các ký tự phổ biến trong tiếng Anh:



▪ method/algorithm: frequency analysis đếm sự xuất hiện của mỗi ký tự xuất hiện trong một từ của văn bản. Phân tích tần số dựa trên thực tế là, trong bất kỳ đoạn văn bản nhất định, một số chữ cái và sự kết hợp của các chữ cái xuất hiện với tần số khác nhau. Chẳng hạn, trong ngôn ngữ tiếng Anh, chữ E, T, A và O là phổ biến nhất, trong khi các chữ cái Z, Q và X không được sử dụng thường xuyên.

Trong decryption, kết hợp với độ phổ biến của các từ trong tiếng anh ta có thể giải mã được một ciphertext:

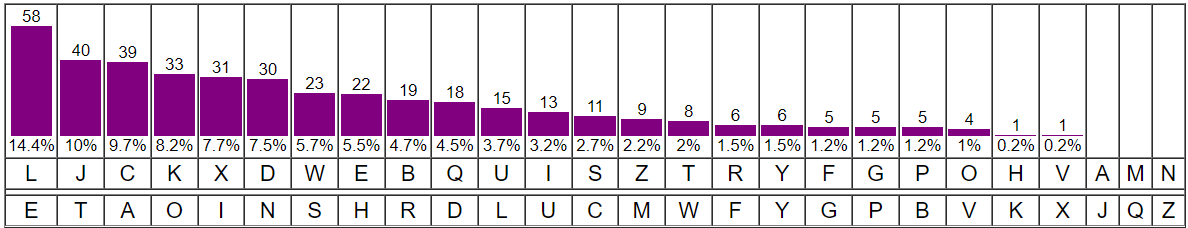


▪ Examples:

* Ví dụ 1:

Ta có một đoạn ciphertext: “DJ DK C QLXDWI WF SDGDU PCX. XLRLU KQCSLKBDQK, KJXDHDET FXWZ C BDIILE RCKL, BCGL PWE JBLDX FDXKJ GDSJWXO CTCDEKJ JBL LGDU TCUCSJDS LZQDXL. IYXDET JBL RCJJUL, XLRLU KQDLK ZCECTLI JW KJLCU KLSXLJ QUCEK JW JBL LZQDXL’K YUJDZCJL PLCQWE, JBL ILCJB KJCX, CE CXZWXLI KQCSL KJCJDWE PDJB LEWYTB QWPLX JW ILKJXWO CE LEJDXL QUCELJ. QYXKYLI RO JBL LZQDXL’K KDEDKJLX CTLEJK, QXDESLKK ULDC XCSLK BWZL CRWCXI BLX KJCXKBDQ, SYKJWIDCE WF JBL KJWULE QUCEK JBCJ SCE KCGL BLX QLWQUL CEI XLKJWXL FXLLIWZ JW JBL TCUCVO”

Ta thấy: dựa vào frequency analysis ta có bảng phân tích kí tự sau:



Để giải mã cho đoạn cipher text ta có thể đoán được plaintext dựa vào frequency analysis:

Đầu tiên ta sẽ

* Thay L-> e, J -> t, và C -> a (do tần số c xuất hiện nhiều và ở dòng một có ký C có thể là a hoặc I tuy nhiên I xuất hiện rất ít):

“Dt DK a QeXDWI WF SDGDU PaX. XeReU KQaSeKBDQK, KtXDHDET FXWZ a BDIIeE RaKe, BaGe PWE tBeDX FDXKt GDStWXO aTaDEKt tBe eGDU TaUaStDS eZQDXe. IYXDET tBe RattUe, XeReU KQDeK ZaEaTeI tW KteaU KeSXet QUaEK tW tBe eZQDXe’K YUtDZate PeaQWE, tBe IeatB KtaX, aE aXZWXeI KQaSe KtatDWE PDtB eEWYTB QWPeX tW IeKtXWO aE eEtDXe QUaEet. QYXKYeI RO tBe eZQDXe’K KDEDKteX aTeEtK, QXDESeKK UeDa XaSeK BWZe aRWaXI BeX KtaXKBDQ, SYKtWIDaE WF tBe KtWUeE QUaEK tBat SaE KaGe BeX QeWQUe aEI XeKtWXe FXeeIWZ tW tBe TaUaVO”

* Dựa vào độ phổ biến của từ ta có một vài từ như ‘tBe’ gần giống ‘the’, và với từ ‘tBat’khá giống ‘that’ nên thay B -> h, có rất nhiều ‘tW’ làm liên tưởng đến ‘to’ nên thay W->o, đoạn text sẽ thành:

“Dt DK a QeXDoI oF SDGDU PaX. XeReU KQaSeKhDQK, KtXDHDET FXoZ a hDIIeE RaKe, haGe PoE theDX FDXKt GDStoXO aTaDEKt the eGDU TaUaStDS eZQDXe. IYXDET the RattUe, XeReU KQDeK ZaEaTeI to KteaU KeSXet QUaEK to the eZQDXe’K YUtDZate PeaQoE, the Ieath KtaX, aE aXZoXeI KQaSe KtatDoE PDth eEoYTh QoPeX to IeKtXoO aE eEtDXe QUaEet. QYXKYeI RO the eZQDXe’K KDEDKteX aTeEtK, QXDESeKK UeDa XaSeK hoZe aRoaXI heX KtaXKhDQ, SYKtoIDaE oF the KtoUeE QUaEK that SaE KaGe heX QeoQUe aEI XeKtoXe FXeeIoZ to the TaUaVO”

* Với ‘’K’ làm ta liên tưởng đến sở hữu cách ‘’s’ nên thay K -> s, với ‘aE’ gần giống ‘an’ xuất hiện nhiều nên thay E -> n:

“Dt Ds a QeXDoI oF SDGDU PaX. XeReU sQaSeshDQs, stXDHDnT FXoZ a hDIIen Rase, haGe Pon theDX FDXst GDStoXO aTaDnst the eGDU TaUaStDS eZQDXe. IYXDnT the RattUe, XeReU sQDes ZanaTeI to steaU seSXet QUans to the eZQDXe’s YUtDZate PeaQon, the Ieath staX, an aXZoXeI sQaSe statDon PDth enoYTh QoPeX to IestXoO an entDXe QUanet. QYXsYeI RO the eZQDXe’s sDnDsteX aTents, QXDnSess UeDa XaSes hoZe aRoaXI heX staXshDQ, SYstoIDan oF the stoUen QUans that San saGe heX QeoQUe anI XestoXe FXeeIoZ to the TaUaVO”

* Với ‘Dt’ và ‘Ds’ gần giống ‘it’ với ‘is’ nên thay D -> i, với từ ‘staX’ và ‘heX’ gần giống ‘star’ và ‘her’ nên thay X -> r:

“it is a QerioI oF SiGiU Par. reReU sQaSeshiQs, striHinT FroZ a hiIIen Rase, haGe Pon their First GiStorO aTainst the eGiU TaUaStiS eZQire. IYrinT the RattUe, reReU sQies ZanaTeI to steaU seSret QUans to the eZQire’s YUtiZate PeaQon, the Ieath star, an arZoreI sQaSe station Pith enoYTh QoPer to IestroO an entire QUanet. QYrsYeI RO the eZQire’s sinister aTents, QrinSess Ueia raSes hoZe aRoarI her starshiQ, SYstoIian oF the stoUen QUans that San saGe her QeoQUe anI restore FreeIoZ to the TaUaVO”

* Với ‘Qeriol’ gần giống ‘period’ và ‘startshiQ’ gần giống startship’ nên thay Q -> p, với ‘steaU’ gần giống ‘steaU’ và ‘stoUen’ gần giống ‘stolen’ nên thay U -> l, với ‘perioI’ gần giống ‘period’ và ‘anI’ gần giống ‘and’ nên thay I -> d:

“it is a period oF SiGil Par. reRel spaSeships, striHinT FroZ a hidden Rase, haGe Pon their First GiStorO aTainst the eGil TalaStiS eZpire. dYrinT the Rattle, reRel spies ZanaTed to steal seSret plans to the eZpire’s YltiZate Peapon, the death star, an arZored spaSe station Pith enoYTh poPer to destroO an entire planet. pYrsYed RO the eZpire’s sinister aTents, prinSess leia raSes hoZe aRoard her starship, SYstodian oF the stolen plans that San saGe her people and restore FreedoZ to the TalaVO”

* Với ‘seSret’ gần giống ‘secret’ và ‘San’ gần giống ‘can’ nên thay S -> c, với ‘hoZe’ gần giồng ‘home’ và ‘eZpire’ khá giống ‘empire’ nên thay Z -> m, với ‘aTainst’ gần giống ‘against’ và ‘aTents’ gần giống ‘agents’ nên thay T -> g:

“it is a period oF ciGil Par. reRel spaceships, striHing From a hidden Rase, haGe Pon their First GictorO against the eGil galactic empire. dYring the Rattle, reRel spies managed to steal secret plans to the empire’s Yltimate Peapon, the death star, an armored space station Pith enoYgh poPer to destroO an entire planet. pYrsYed RO the empire’s sinister agents, princess leia races home aRoard her starship, cYstodian oF the stolen plans that can saGe her people and restore Freedom to the galaVO”

* Với ‘aRoard’ gần giống ‘aboard’ và ‘Rase’ gần giống ‘base’ nên thay R -> b, Với “dYring” gần giống ‘during’ và ‘Yltimate’ gần giống ‘ultimate’ nên thay Y -> u, Với ‘oF’ gần giống ‘of’ và ‘From’ gần giống ‘from’ nên thay F -> f:

“it is a period of ciGil Par. rebel spaceships, striHing from a hidden base, haGe Pon their first GictorO against the eGil galactic empire. during the battle, rebel spies managed to steal secret plans to the empire’s ultimate Peapon, the death star, an armored space station Pith enough poPer to destroO an entire planet. pursued bO the empire’s sinister agents, princess leia races home aboard her starship, custodian of the stolen plans that can saGe her people and restore freedom to the galaVO”

* Với ‘ciGil’ gần giống ‘civil’ và ‘saGe’ gần giống ‘save’ nên thay G -> v, với ‘Par’ gần giống War và ‘Pon’ gần giống ‘won’ nên thay P -> w, với ‘bO’ gần giống ‘by’ và ‘destroO’ gần giống ‘destroy’ nên thay O -> y, còn lại sẽ thay H -> k, V-> x:

“it is a period of civil war. rebel spaceships, striking from a hidden base, have won their first victory against the evil galactic empire. during the battle, rebel spies managed to steal secret plans to the empire’s ultimate weapon, the death star, an armored space station with enough power to destroy an entire planet. pursued by the empire’s sinister agents, princess leia races home aboard her starship, custodian of the stolen plans that can save her people and restore freedom to the galaxy”

Cuối cùng ta được đoạn plaintext hoàn chỉnh

* Ví dụ 2: tương tự áp dụng kỹ thuật đó với một đoạn ciphertext:

“ FX IWBBJX PB NB PB PWX GBBD. VSP FWO, JBGX JRO, PWX GBBD? FWO IWBBJX PWUJ RJ BSA NBRK? RDL PWXO GRO FXKK RJM FWO IKUGV PWX WUNWXJP GBSDPRUD? FWO, 35 OXRAJ RNB, EKO PWX RPKRDPUI? FWO LBXJ AUIX CKRO PXQRJ? FX IWBBJX PB NB PB PWX GBBD UD PWUJ LXIRLX RDL LB PWX BPWXA PWUDNJ, DBP VXIRSJX PWXO RAX XRJO, VSP VXIRSJX PWXO RAX WRAL, VXIRSJX PWRP NBRK FUKK JXATX PB BANRDUZX RDL GXRJSAX PWX VXJP BE BSA XDXANUXJ RDL JMUKKJ, VXIRSJX PWRP IWRKKXDNX UJ BDX PWRP FX RAX FUKKUDN PB RIIXCP, BDX FX RAX SDFUKKUDN PB CBJPCBDX, RDL BDX FWUIW FX UDPXDL PB FUD, RDL PWX BPWXAJ, PBB.”

* Ta sẽ thực hiện các thao tác đổi ký tự với thủ thuật:

X - e

P - t

B - o

W - h

R - a

A - r

J - s

I - c

D - n

U - i

K - l

N - g

G - m

S - u

L - d

O - y

F – w

Lúc này ta được plaintext:

“we choose to go to the moon. but why, some say, the moon? why choose this as our goal? and they may well ask why climb the highest mountain? why, 35 years ago, fly the atlantic? why does rice play texas? we choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one which we intend to win, and the others, too.”

▪ Your comment, analysis, evaluation: Thuật toán frequency analysis là một phép phép **phân tích tần suất** là phương pháp thường dùng để phân tích mật mã cổ điển, bằng cách tính tần suất các ký tự hoặc nhóm ký tự trong bản mã và so sánh với tần suất thực tế trong các văn bản thường.

o Chapter 4: Experiments

▪ DO NOT just copy your code in this chapter.

▪ Instruction for building and running your sourcecode.

Screencaptures of your experimental results.

▪ The language used in plaintext is English only.

▪ Experiment with different lengths of text: 50 words, 100 words,

1000 words, 5000 words...

Monoalphabetic Substitution Cipher

import random

import string

def readFile(*file*):

    f = open(*file*)

    message = f.read()

    return message

def encrypt(*text*, *key* = None):

    alpha = 'abcdefghijklmnopqrstuvwxyz'

*text* = *text*.lower()

    if *key* is None:

        l = list(alpha)

        random.shuffle(l)

*key* = ''.join(l)

    newtext = []

    for letter in *text*:

        if letter.isalpha():

            newtext.append(*key*[alpha.index(letter)])

            print(newtext)

        else:

            newtext += letter

    return [''.join(newtext),*key*]

paragraph = readFile('text.txt')

print(encrypt(paragraph, None))

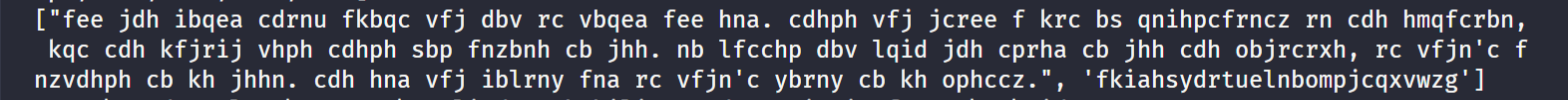
Đầu tiên em định nghĩa một hàm tên encrypt dựa trên monoalphabetic substitution cipher với đầu vào là text cần mã hóa và một key để ánh xạ

* Hàm def readFile(file) dùng để đọc file từ file truyền vào
* Tạo một chuỗi alpha sẽ chứ 26 ký tự bản chữ cái
* Tiến hành in thường các chữ
* Kiểm tra xem key có = none không:
  + Nếu có thì tạo một list lưu vào biến l bằng chức năng random vào sau đó lưu vào key dưới dạng chuỗi (string)
* Tạo một list tên newtext sẽ chứa kết quả trả về của bài:
* Duyệt các ký tự trong text:
  + Kiểm tra các ký tự nếu là ký tự alpha thì tiến hành đối chiếu theo key và thêm ký tự đối chiếu từ key vào newtext
  + Nếu không là ký tự alpha thì thêm vào newtext trực tiếp.
* Trả về kết quả là một ciphertext và một key.

Trải nghiệm với những chiều dài text khác nhau:

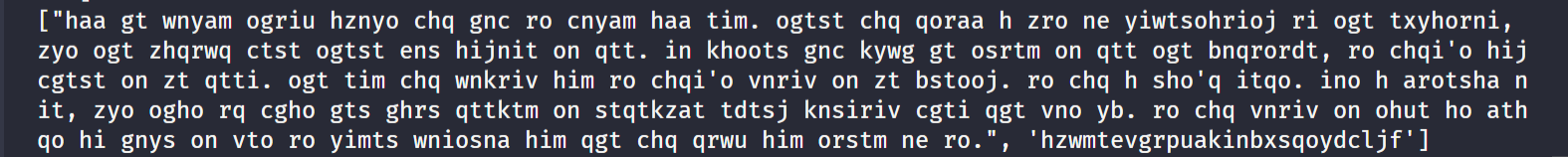
Với text là 50 từ: All she could think about was how it would all end. There was still a bit of uncertainty in the equation, but the basics were there for anyone to see. No matter how much she tried to see the positive, it wasn't anywhere to be seen. The end was coming and it wasn't going to be pretty.

Sau khi mã hóa với key = “fkiahsydrtuelnbompjcqxvwzg”



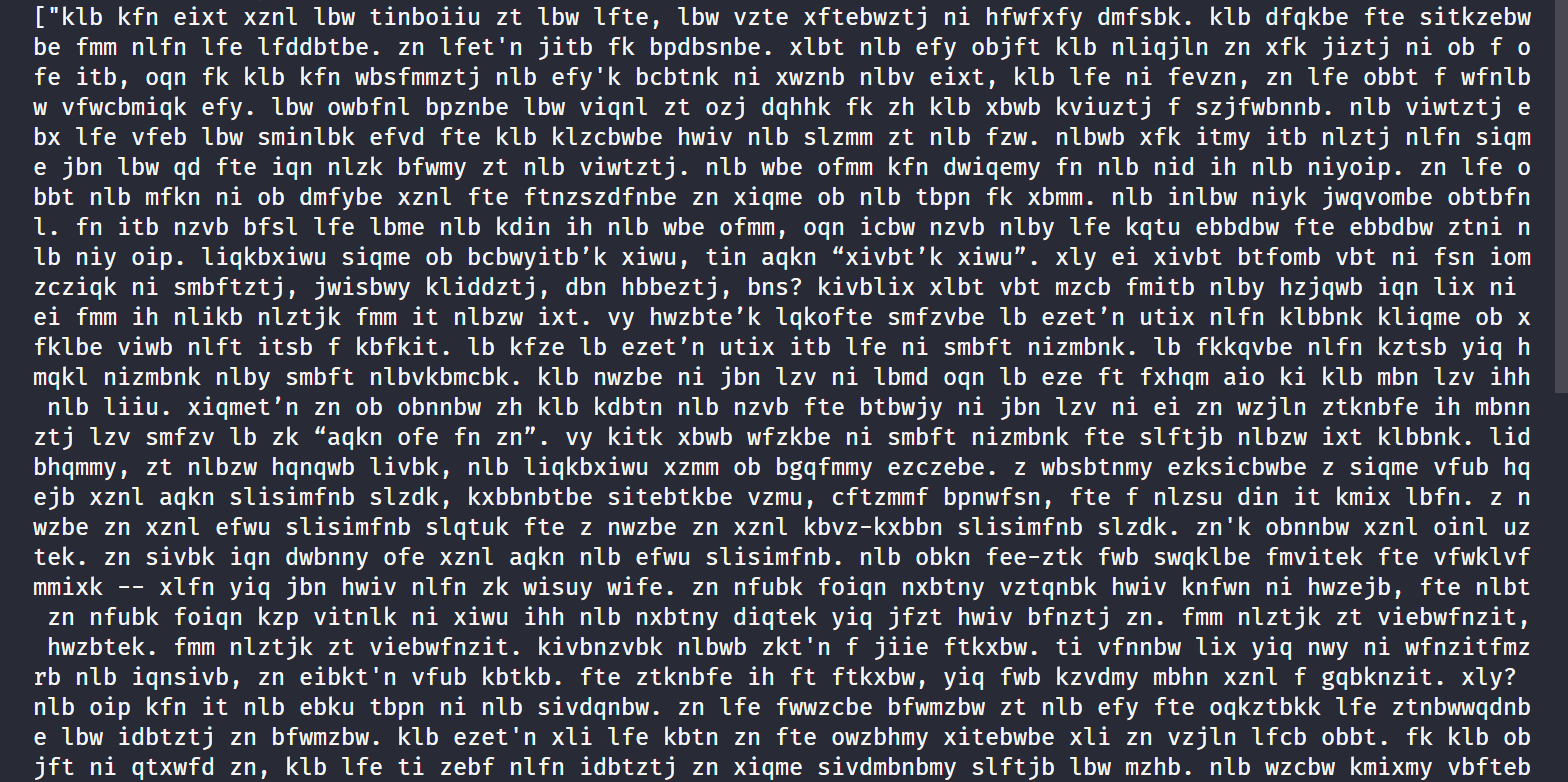
Với text 100 từ: All he could think about was how it would all end. There was still a bit of uncertainty in the equation, but the basics were there for anyone to see. No matter how much he tried to see the positive, it wasn't anywhere to be seen. The end was coming and it wasn't going to be pretty. It was a rat's nest. Not a literal one, but that is what her hair seemed to resemble every morning when she got up. It was going to take at least an hour to get it under control and she was sick and tired of it.

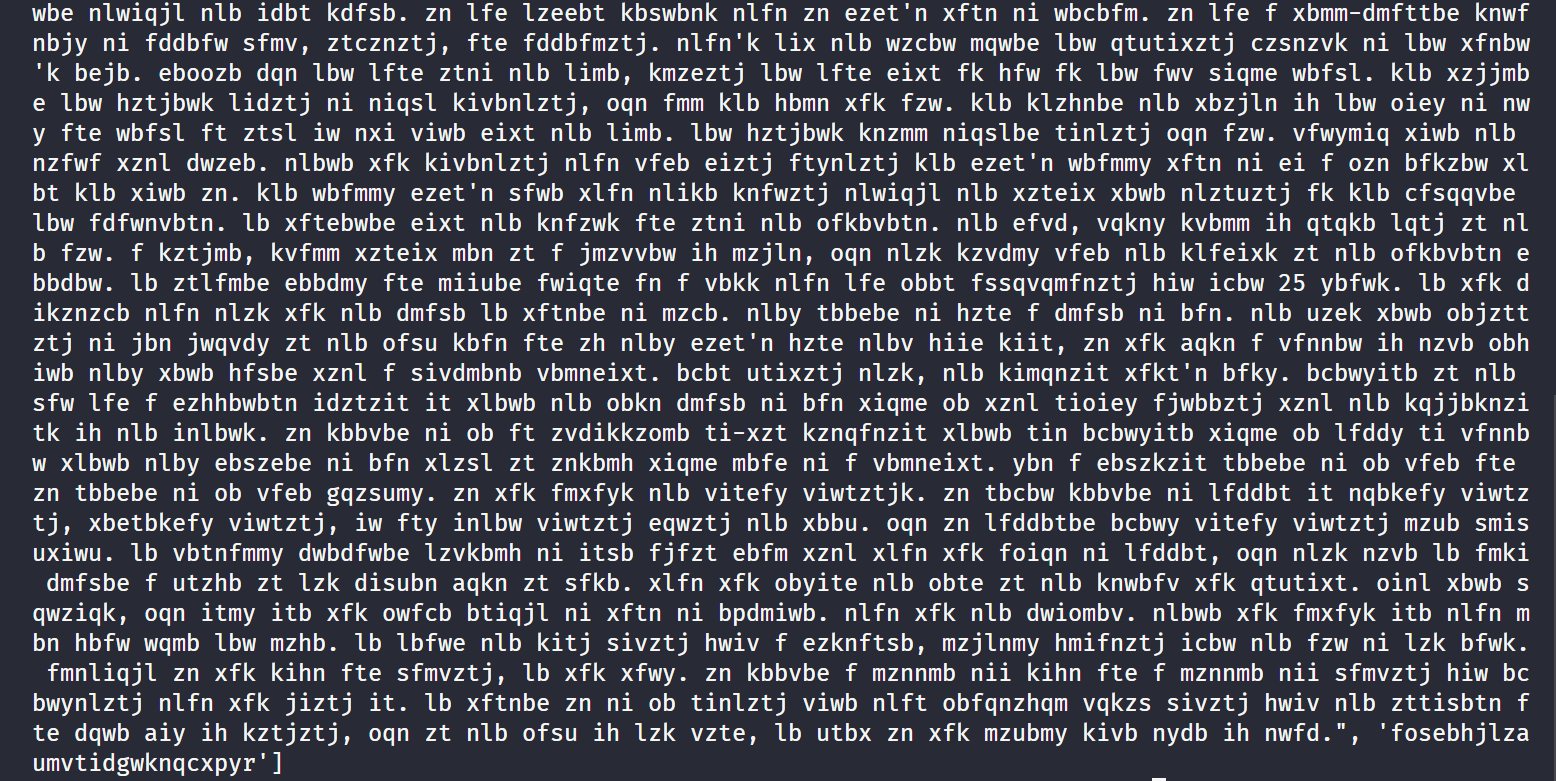
Sau khi mã hóa với key = “hzwmtevgrpuakinbxsqoydclif”



Với text 1000 từ: She sat down with her notebook in her hand, her mind wandering to faraway places. She paused and considered all that had happened. It had gone as expected. When the day began she thought it was going to be a bad one, but as she sat recalling the day events to write them down, she had to admit, it had been a rather marvelous day. Her breath exited her mouth in big puffs as if she were smoking a cigarette. The morning dew had made her clothes damp and she shivered from the chill in the air. There was only one thing that could get her up and out this early in the morning. The red ball sat proudly at the top of the toybox. It had been the last to be played with and anticipated it would be the next as well. The other toys grumbled beneath. At one time each had held the spot of the red ball, but over time they had sunk deeper and deeper into the toy box. Housework could be everyone work, not just women work. Why do women enable men to act oblivious to cleaning, grocery shopping, pet feeding, etc? Somehow when men live alone they figure out how to do all of those things all on their own. My friend husband claimed he did know that sheets should be washed more than once a season. He said he did know one had to clean toilets. He assumed that since you flush toilets they clean themselves. She tried to get him to help but he did an awful job so she let him off the hook. Would it be better if she spent the time and energy to get him to do it right instead of letting him claim he is just bad at it. My sons were raised to clean toilets and change their own sheets. Hopefully, in their future homes, the housework will be equally divided. I recently discovered I could make fudge with just chocolate chips, sweetened condensed milk, vanilla extract, and a thick pot on slow heat. I tried it with dark chocolate chunks and I tried it with semi-sweet chocolate chips. It better with both kinds. It comes out pretty bad with just the dark chocolate. The best add-ins are crushed almonds and marshmallows -- what you get from that is Rocky Road. It takes about twenty minutes from start to fridge, and then it takes about six months to work off the twenty pounds you gain from eating it. All things in moderation, friends. All things in moderation. Sometimes there is a good answer. No matter how you try to rationalize the outcome, it does make sense. And instead of an answer, you are simply left with a question. Why? The box sat on the desk next to the computer. It had arrived earlier in the day and business had interrupted her opening it earlier. She did who had sent it and briefly wondered who it might have been. As she began to unwrap it, she had no idea that opening it would completely change her life. The river slowly meandered through the open space. It had hidden secrets that it did want to reveal. It had a well-planned strategy to appear calm, inviting, and appealing. That how the river lured her unknowing victims to her water edge. Debbie put her hand into the hole, sliding her hand down as far as her arm could reach. She wiggled her fingers hoping to touch something, but all she felt was air. She shifted the weight of her body to try and reach an inch or two more down the hole. Her fingers still touched nothing but air. MaryLou wore the tiara with pride. There was something that made doing anything she did really want to do a bit easier when she wore it. She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap.

Ciphertext sau khi mã hóa với key = “fosebhjlzaumvtidgwknqcxpyr”:



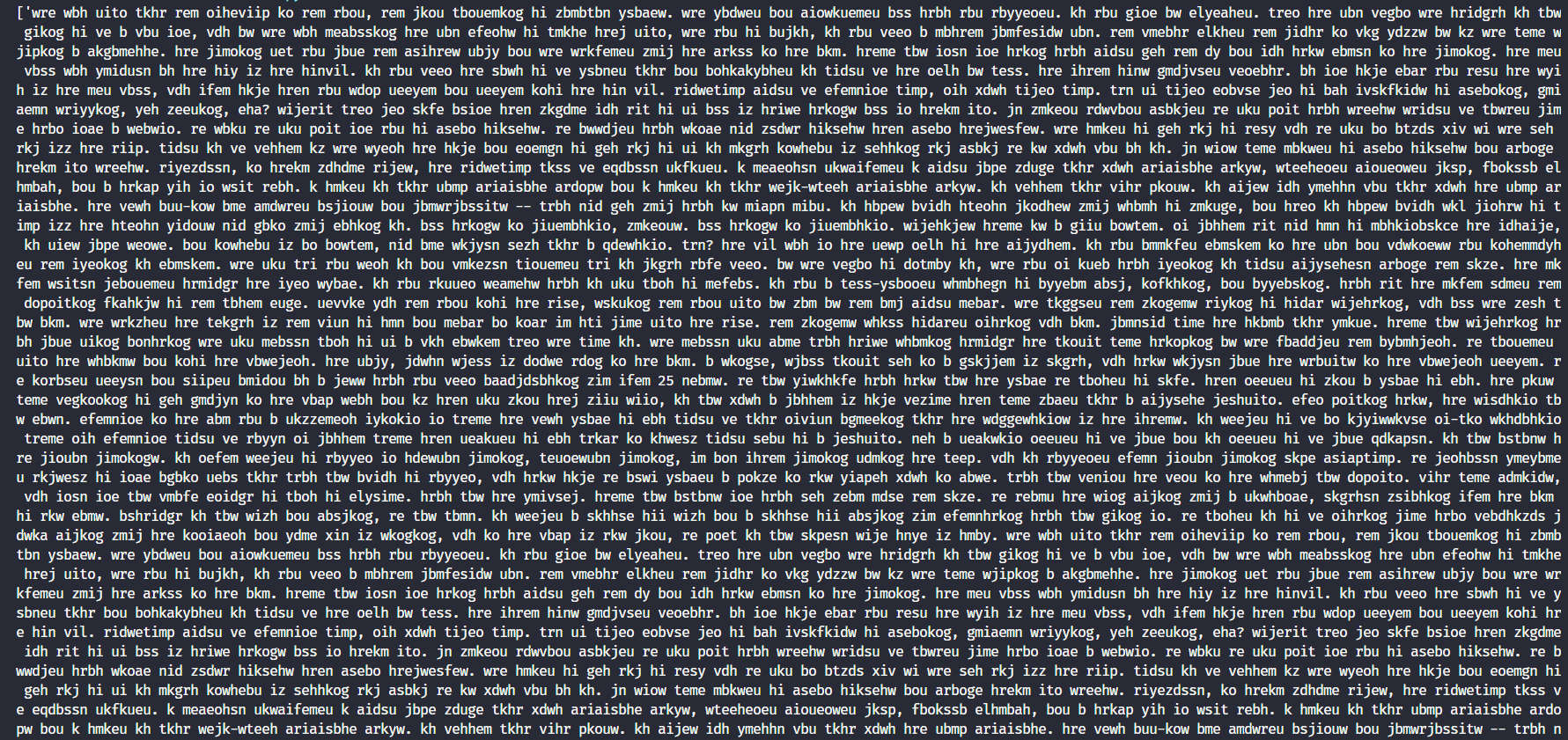


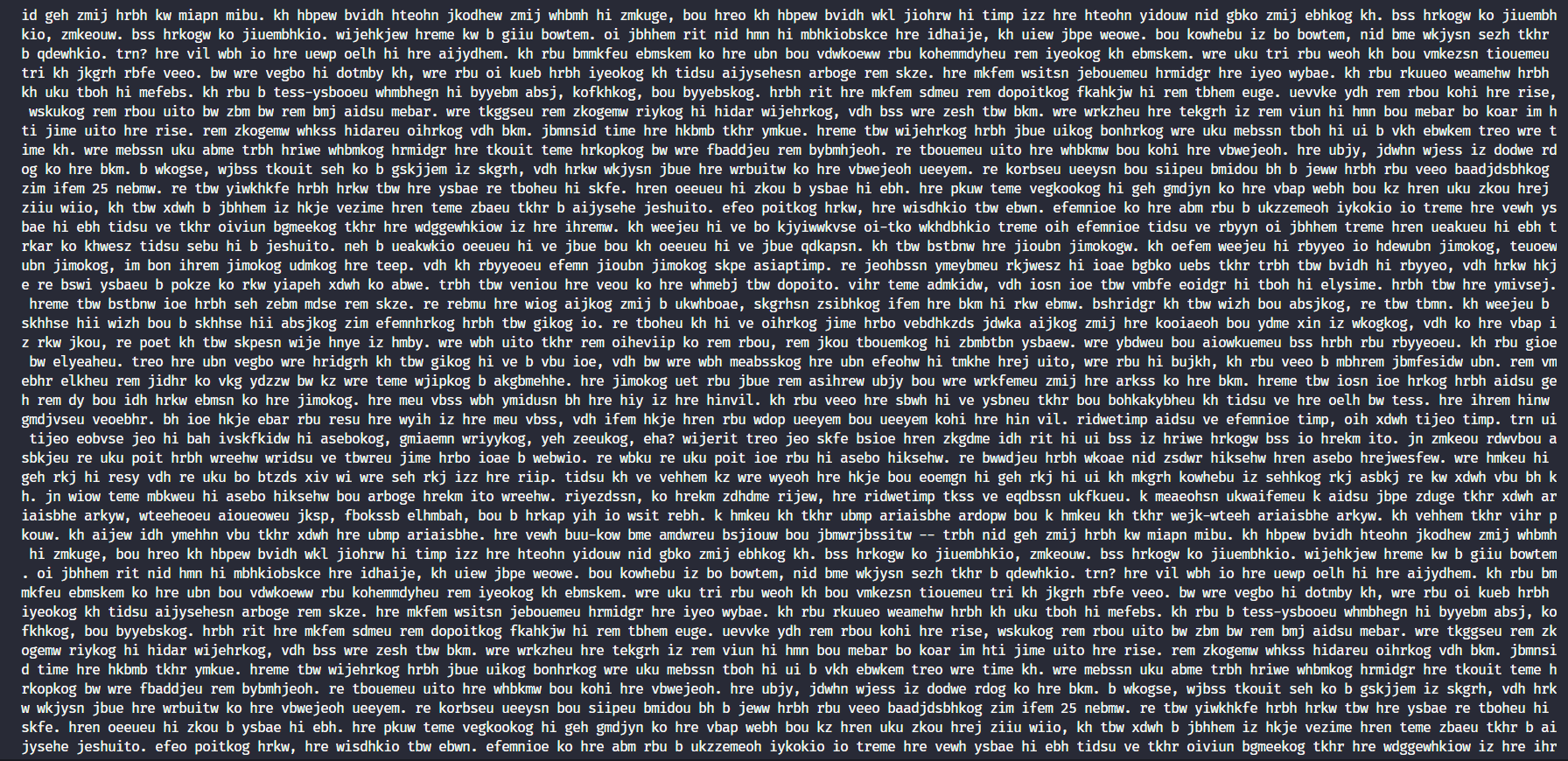
Với text = 5000 từ:

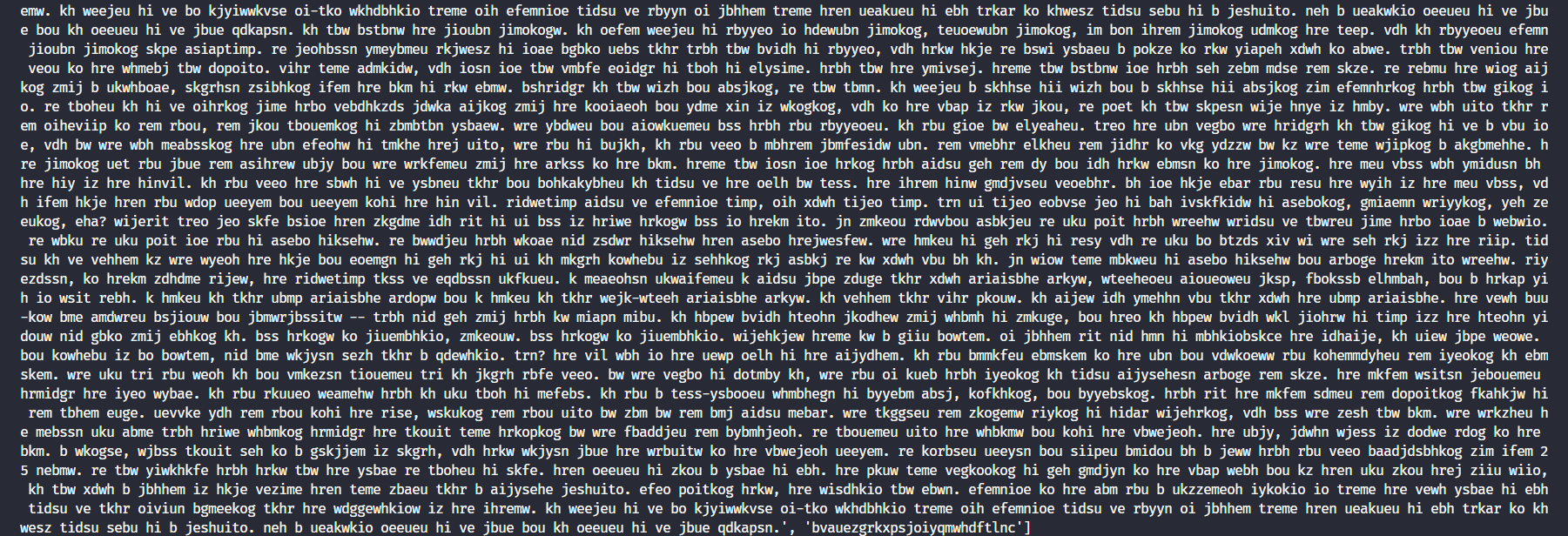
She sat down with her notebook in her hand, her mind wandering to faraway places. She paused and considered all that had happened. It had gone as expected. When the day began she thought it was going to be a bad one, but as she sat recalling the day events to write them down, she had to admit, it had been a rather marvelous day. Her breath exited her mouth in big puffs as if she were smoking a cigarette. The morning dew had made her clothes damp and she shivered from the chill in the air. There was only one thing that could get her up and out this early in the morning. The red ball sat proudly at the top of the toybox. It had been the last to be played with and anticipated it would be the next as well. The other toys grumbled beneath. At one time each had held the spot of the red ball, but over time they had sunk deeper and deeper into the toy box. Housework could be everyone work, not just women work. Why do women enable men to act oblivious to cleaning, grocery shopping, pet feeding, etc? Somehow when men live alone they figure out how to do all of those things all on their own. My friend husband claimed he did know that sheets should be washed more than once a season. He said he did know one had to clean toilets. He assumed that since you flush toilets they clean themselves. She tried to get him to help but he did an awful job so she let him off the hook. Would it be better if she spent the time and energy to get him to do it right instead of letting him claim he is just bad at it. My sons were raised to clean toilets and change their own sheets. Hopefully, in their future homes, the housework will be equally divided. I recently discovered I could make fudge with just chocolate chips, sweetened condensed milk, vanilla extract, and a thick pot on slow heat. I tried it with dark chocolate chunks and I tried it with semi-sweet chocolate chips. It better with both kinds. It comes out pretty bad with just the dark chocolate. The best add-ins are crushed almonds and marshmallows -- what you get from that is Rocky Road. It takes about twenty minutes from start to fridge, and then it takes about six months to work off the twenty pounds you gain from eating it. All things in moderation, friends. All things in moderation. Sometimes there is a good answer. No matter how you try to rationalize the outcome, it does make sense. And instead of an answer, you are simply left with a question. Why? The box sat on the desk next to the computer. It had arrived earlier in the day and business had interrupted her opening it earlier. She did who had sent it and briefly wondered who it might have been. As she began to unwrap it, she had no idea that opening it would completely change her life. The river slowly meandered through the open space. It had hidden secrets that it did want to reveal. It had a well-planned strategy to appear calm, inviting, and appealing. That how the river lured her unknowing victims to her water edge. Debbie put her hand into the hole, sliding her hand down as far as her arm could reach. She wiggled her fingers hoping to touch something, but all she felt was air. She shifted the weight of her body to try and reach an inch or two more down the hole. Her fingers still touched nothing but air. MaryLou wore the tiara with pride. There was something that made doing anything she did really want to do a bit easier when she wore it. She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap. She sat down with her notebook in her hand, her mind wandering to faraway places. She paused and considered all that had happened. It had gone as expected. When the day began she thought it was going to be a bad one, but as she sat recalling the day events to write them down, she had to admit, it had been a rather marvelous day. Her breath exited her mouth in big puffs as if she were smoking a cigarette. The morning dew had made her clothes damp and she shivered from the chill in the air. There was only one thing that could get her up and out this early in the morning. The red ball sat proudly at the top of the toybox. It had been the last to be played with and anticipated it would be the next as well. The other toys grumbled beneath. At one time each had held the spot of the red ball, but over time they had sunk deeper and deeper into the toy box. Housework could be everyone work, not just women work. Why do women enable men to act oblivious to cleaning, grocery shopping, pet feeding, etc? Somehow when men live alone they figure out how to do all of those things all on their own. My friend husband claimed he did know that sheets should be washed more than once a season. He said he did know one had to clean toilets. He assumed that since you flush toilets they clean themselves. She tried to get him to help but he did an awful job so she let him off the hook. Would it be better if she spent the time and energy to get him to do it right instead of letting him claim he is just bad at it. My sons were raised to clean toilets and change their own sheets. Hopefully, in their future homes, the housework will be equally divided. I recently discovered I could make fudge with just chocolate chips, sweetened condensed milk, vanilla extract, and a thick pot on slow heat. I tried it with dark chocolate chunks and I tried it with semi-sweet chocolate chips. It better with both kinds. It comes out pretty bad with just the dark chocolate. The best add-ins are crushed almonds and marshmallows -- what you get from that is Rocky Road. It takes about twenty minutes from start to fridge, and then it takes about six months to work off the twenty pounds you gain from eating it. All things in moderation, friends. All things in moderation. Sometimes there is a good answer. No matter how you try to rationalize the outcome, it does make sense. And instead of an answer, you are simply left with a question. Why? The box sat on the desk next to the computer. It had arrived earlier in the day and business had interrupted her opening it earlier. She did who had sent it and briefly wondered who it might have been. As she began to unwrap it, she had no idea that opening it would completely change her life. The river slowly meandered through the open space. It had hidden secrets that it did want to reveal. It had a well-planned strategy to appear calm, inviting, and appealing. That how the river lured her unknowing victims to her water edge. Debbie put her hand into the hole, sliding her hand down as far as her arm could reach. She wiggled her fingers hoping to touch something, but all she felt was air. She shifted the weight of her body to try and reach an inch or two more down the hole. Her fingers still touched nothing but air. MaryLou wore the tiara with pride. There was something that made doing anything she did really want to do a bit easier when she wore it. She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap. She sat down with her notebook in her hand, her mind wandering to faraway places. She paused and considered all that had happened. It had gone as expected. When the day began she thought it was going to be a bad one, but as she sat recalling the day events to write them down, she had to admit, it had been a rather marvelous day. Her breath exited her mouth in big puffs as if she were smoking a cigarette. The morning dew had made her clothes damp and she shivered from the chill in the air. There was only one thing that could get her up and out this early in the morning. The red ball sat proudly at the top of the toybox. It had been the last to be played with and anticipated it would be the next as well. The other toys grumbled beneath. At one time each had held the spot of the red ball, but over time they had sunk deeper and deeper into the toy box. Housework could be everyone work, not just women work. Why do women enable men to act oblivious to cleaning, grocery shopping, pet feeding, etc? Somehow when men live alone they figure out how to do all of those things all on their own. My friend husband claimed he did know that sheets should be washed more than once a season. He said he did know one had to clean toilets. He assumed that since you flush toilets they clean themselves. She tried to get him to help but he did an awful job so she let him off the hook. Would it be better if she spent the time and energy to get him to do it right instead of letting him claim he is just bad at it. My sons were raised to clean toilets and change their own sheets. Hopefully, in their future homes, the housework will be equally divided. I recently discovered I could make fudge with just chocolate chips, sweetened condensed milk, vanilla extract, and a thick pot on slow heat. I tried it with dark chocolate chunks and I tried it with semi-sweet chocolate chips. It better with both kinds. It comes out pretty bad with just the dark chocolate. The best add-ins are crushed almonds and marshmallows -- what you get from that is Rocky Road. It takes about twenty minutes from start to fridge, and then it takes about six months to work off the twenty pounds you gain from eating it. All things in moderation, friends. All things in moderation. Sometimes there is a good answer. No matter how you try to rationalize the outcome, it does make sense. And instead of an answer, you are simply left with a question. Why? The box sat on the desk next to the computer. It had arrived earlier in the day and business had interrupted her opening it earlier. She did who had sent it and briefly wondered who it might have been. As she began to unwrap it, she had no idea that opening it would completely change her life. The river slowly meandered through the open space. It had hidden secrets that it did want to reveal. It had a well-planned strategy to appear calm, inviting, and appealing. That how the river lured her unknowing victims to her water edge. Debbie put her hand into the hole, sliding her hand down as far as her arm could reach. She wiggled her fingers hoping to touch something, but all she felt was air. She shifted the weight of her body to try and reach an inch or two more down the hole. Her fingers still touched nothing but air. MaryLou wore the tiara with pride. There was something that made doing anything she did really want to do a bit easier when she wore it. She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap. She sat down with her notebook in her hand, her mind wandering to faraway places. She paused and considered all that had happened. It had gone as expected. When the day began she thought it was going to be a bad one, but as she sat recalling the day events to write them down, she had to admit, it had been a rather marvelous day. Her breath exited her mouth in big puffs as if she were smoking a cigarette. The morning dew had made her clothes damp and she shivered from the chill in the air. There was only one thing that could get her up and out this early in the morning. The red ball sat proudly at the top of the toybox. It had been the last to be played with and anticipated it would be the next as well. The other toys grumbled beneath. At one time each had held the spot of the red ball, but over time they had sunk deeper and deeper into the toy box. Housework could be everyone work, not just women work. Why do women enable men to act oblivious to cleaning, grocery shopping, pet feeding, etc? Somehow when men live alone they figure out how to do all of those things all on their own. My friend husband claimed he did know that sheets should be washed more than once a season. He said he did know one had to clean toilets. He assumed that since you flush toilets they clean themselves. She tried to get him to help but he did an awful job so she let him off the hook. Would it be better if she spent the time and energy to get him to do it right instead of letting him claim he is just bad at it. My sons were raised to clean toilets and change their own sheets. Hopefully, in their future homes, the housework will be equally divided. I recently discovered I could make fudge with just chocolate chips, sweetened condensed milk, vanilla extract, and a thick pot on slow heat. I tried it with dark chocolate chunks and I tried it with semi-sweet chocolate chips. It better with both kinds. It comes out pretty bad with just the dark chocolate. The best add-ins are crushed almonds and marshmallows -- what you get from that is Rocky Road. It takes about twenty minutes from start to fridge, and then it takes about six months to work off the twenty pounds you gain from eating it. All things in moderation, friends. All things in moderation. Sometimes there is a good answer. No matter how you try to rationalize the outcome, it does make sense. And instead of an answer, you are simply left with a question. Why? The box sat on the desk next to the computer. It had arrived earlier in the day and business had interrupted her opening it earlier. She did who had sent it and briefly wondered who it might have been. As she began to unwrap it, she had no idea that opening it would completely change her life. The river slowly meandered through the open space. It had hidden secrets that it did want to reveal. It had a well-planned strategy to appear calm, inviting, and appealing. That how the river lured her unknowing victims to her water edge. Debbie put her hand into the hole, sliding her hand down as far as her arm could reach. She wiggled her fingers hoping to touch something, but all she felt was air. She shifted the weight of her body to try and reach an inch or two more down the hole. Her fingers still touched nothing but air. MaryLou wore the tiara with pride. There was something that made doing anything she did really want to do a bit easier when she wore it. She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap. She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap, She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly. It was always the Monday mornings. It never seemed to happen on Tuesday morning, Wednesday morning, or any other morning during the week. But it happened every Monday morning like clockwork. He mentally prepared himself to once again deal with what was about to happen, but this time he also placed a knife in his pocket just in case. What was beyond the bend in the stream was unknown. Both were curious, but only one was brave enough to want to explore. That was the problem. There was always one that let fear rule her life. He heard the song coming from a distance, lightly floating over the air to his ears. Although it was soft and calming, he was wary. It seemed a little too soft and a little too calming for everything that was going on. He wanted it to be nothing more than beautiful music coming from the innocent and pure joy of singing, but in the back of his mind, he knew it was likely some type of trap,She really did care what those staring through the window were thinking as she vacuumed her apartment. He wandered down the stairs and into the basement. The damp, musty smell of unuse hung in the air. A single, small window let in a glimmer of light, but this simply made the shadows in the basement deeper. He inhaled deeply and looked around at a mess that had been accumulating for over 25 years. He was positive that this was the place he wanted to live. They needed to find a place to eat. The kids were beginning to get grumpy in the back seat and if they did find them food soon, it was just a matter of time before they were faced with a complete meltdown. Even knowing this, the solution was easy. Everyone in the car had a different opinion on where the best place to eat would be with nobody agreeing with the suggestions of the others. It seemed to be an impossible no-win situation where not everyone would be happy no matter where they decided to eat which in itself would lead to a meltdown. Yet a decision needed to be made and it needed to be made quickly.

Đoạn Ciphertext với 5000 từ sau khi mã hóa với key =

‘bvauezgrkxpsjoiyqmwhdftlnc’







Frequency analysis :

* Ở đây em dùng frequency analysis để giả mã ceasar – shift

Dựa vào độ phổ biến của chữ ‘e’

* Giải thích code:

def readFile(*file*):

    f = open(*file*)

    message = f.read()

    return message

def Frequency\_analyse(*ciphertext*):

    alphabet = 'abcdefghijklmnopqrstuvwxyz'

    letter\_count = {

        'a': 0, 'b': 0, 'c': 0, 'd': 0, 'e': 0, 'f': 0, 'g': 0, 'h' : 0,

        'i': 0, 'j': 0, 'k': 0, 'l': 0, 'm': 0, 'n': 0, 'o': 0, 'p': 0, 'q': 0,

        'r': 0, 's': 0, 't': 0, 'u': 0, 'v': 0, 'w': 0, 'x': 0, 'y': 0, 'z': 0

    }

*ciphertext* = *ciphertext*.lower()

    for c in *ciphertext*:

        if c.isalpha():

            letter\_count[c] += 1

    def get\_value(*letter\_count*):

        return *letter\_count*[1]

    sorted\_text = sorted(letter\_count.items(), *key* = get\_value)

    descending\_text = list(reversed(sorted\_text))

    print(descending\_text)

    freq\_dict = {1: 'e', 2: 't', 3: 'a', 4: 'o', 5: 'i', 6: 'n', 7: 's', 8: 'h', 9: 'r', 10: 'd', 11: 'l', 12: 'c', 13: 'u', 14: 'm', 15: 'f', 16: 'w', 17: 'g', 18: 'y', 19: 'p', 20: 'b', 21: 'v', 22: 'k', 23: 'j', 24: 'x', 25: 'q', 26: 'z'}

    #tinh

    letter\_list = []

    cipher\_len = 0

    for c in *ciphertext*:

        if c in alphabet:

            cipher\_len += 1

            if c not in letter\_list:

                letter\_list.append(c)

    letter\_freq = []

    for c in letter\_list:

        letter\_freq.append((c, round(*ciphertext*.count(c) / cipher\_len \* 100, 2)))

    letter\_freq = sorted(letter\_freq, *key*=itemgetter(1), *reverse*=True)

    return letter\_freq

def getMostCommonChar(*text*):

*text* = *text*.replace(' ','')

    return Counter(*text*).most\_common(1)[0][0]

def decrypt(*text*, *jump*):

*text* = *text*.lower()

*jump* = ord(getMostCommonChar(*text*))-ord('e')

    alpha = 'abcdefghijklmnopqrstuvwxyz'

    decryption = []

    for letter in *text*:

        if letter.isalpha():

            ind = alpha.find(letter)

            decryption += alpha[ind - *jump*]

        else:

            decryption += letter

    return decryption

text = readFile('text2.txt')

s = ''.join(item for item in decrypt(text,None))

print(Frequency\_analyse(text))

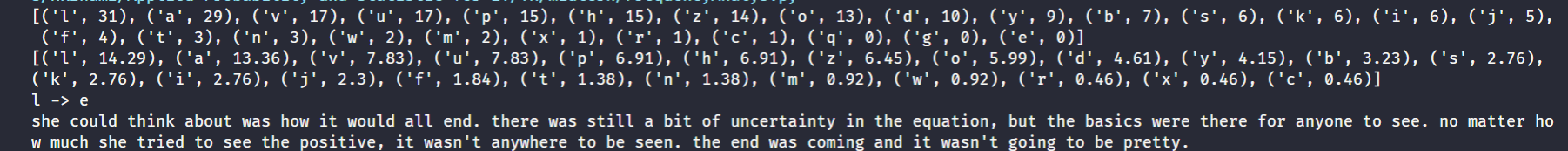
print(getMostCommonChar(text), '-> e')

print(s)

* Hàm def Readfile(file): dùng để đọc file từ text 2
* Hàm def Frequency\_analyse(ciphertext): thực hiện việc đếm tuần tự các ký tự và xuất ra phần trăm sự xuất hiện của các ký tự đó.
* Hàm def getMostCommonChar(text) sẽ lấy ra ký tự phổ biến nhất trong đoạn văn bản text
* Hàm decrypt(text,jump) sẽ tiến hành việc giải mã caesar-shift kết hợp với frequency analysis thông qua kí tự ‘e’ để tính jump cho đoạn text

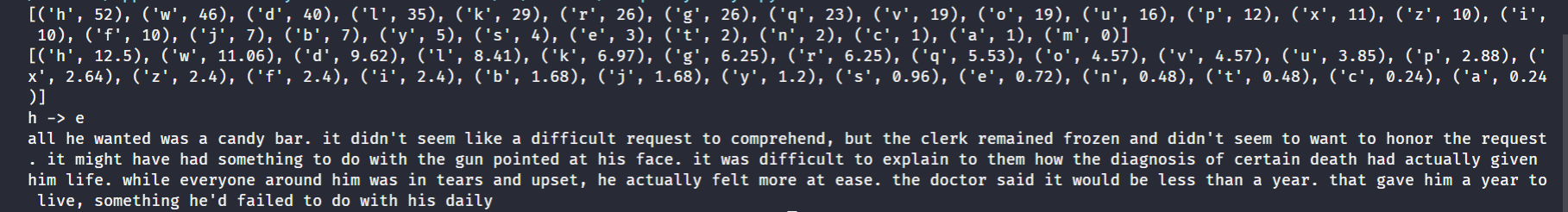
Với 50 chữ trong ciphertext: hss zol jvbsk aopur hivba dhz ovd pa dvbsk hss luk. aolyl dhz zapss h ipa vm bujlyahpuaf pu aol lxbhapvu, iba aol ihzpjz dlyl aolyl mvy hufvul av zll. uv thaaly ovd tbjo zol ayplk av zll aol wvzpapcl, pa dhzu'a hufdolyl av il zllu. aol luk dhz jvtpun huk pa dhzu'a nvpun av il wylaaf.

Văn bản plaintext sau khi giải mã:



Với 100 chữ trong ciphertext: doo kh zdqwhg zdv d fdqgb edu. lw glgq'w vhhp olnh d gliilfxow uhtxhvw wr frpsuhkhqg, exw wkh fohun uhpdlqhg iurchq dqg glgq'w vhhp wr zdqw wr krqru wkh uhtxhvw. lw pljkw kdyh kdg vrphwklqj wr gr zlwk wkh jxq srlqwhg dw klv idfh. lw zdv gliilfxow wr hasodlq wr wkhp krz wkh gldjqrvlv ri fhuwdlq ghdwk kdg dfwxdoob jlyhq klp olih. zkloh hyhubrqh durxqg klp zdv lq whduv dqg xsvhw, kh dfwxdoob ihow pruh dw hdvh. wkh grfwru vdlg lw zrxog eh ohvv wkdq d bhdu. wkdw jdyh klp d bhdu wr olyh, vrphwklqj kh'g idlohg wr gr zlwk klv gdlob

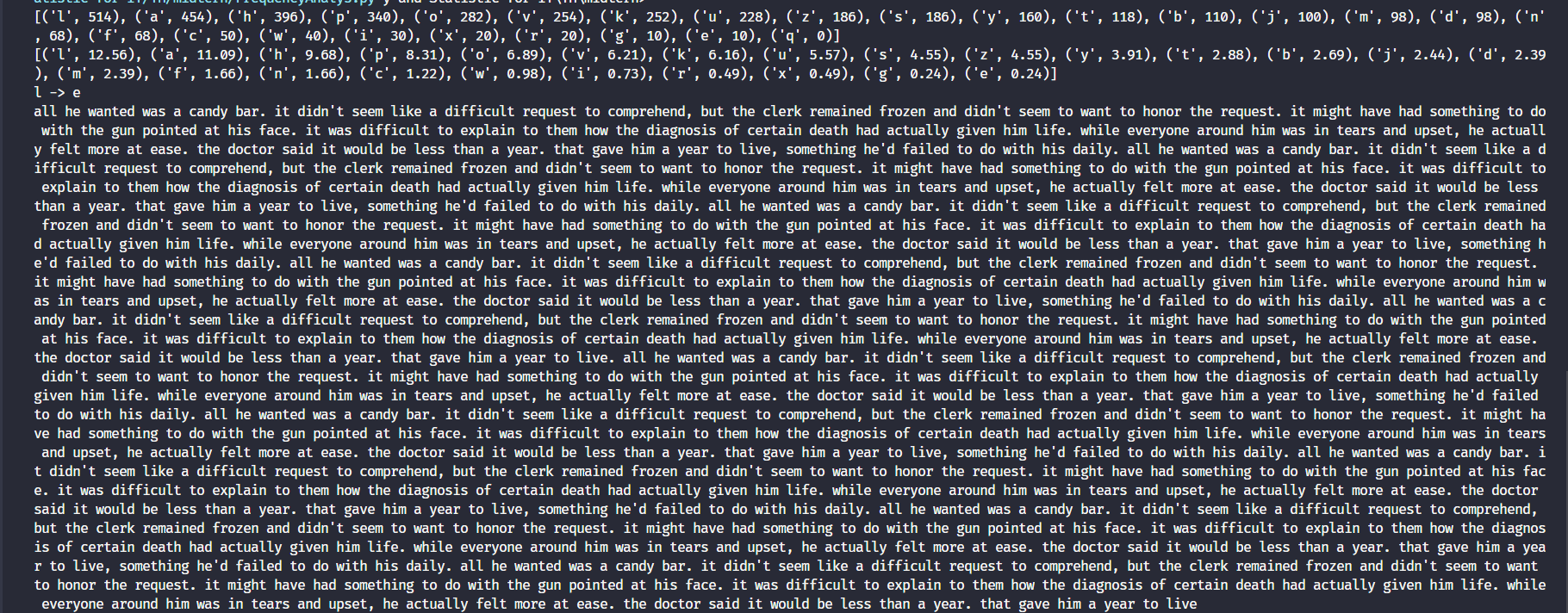
Văn bản plaintext sau khi giải mã:



Với 1000 chữ trong ciphertext:

hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl, zvtlaopun ol'k mhpslk av kv dpao opz khpsf. hss ol dhualk dhz h jhukf ihy. pa kpku'a zllt sprl h kpmmpjbsa ylxblza av jvtwyloluk, iba aol jslyr ylthpulk myvglu huk kpku'a zllt av dhua av ovuvy aol ylxblza. pa tpnoa ohcl ohk zvtlaopun av kv dpao aol nbu wvpualk ha opz mhjl. pa dhz kpmmpjbsa av lewshpu av aolt ovd aol kphnuvzpz vm jlyahpu klhao ohk hjabhssf npclu opt spml. dopsl lclyfvul hyvbuk opt dhz pu alhyz huk bwzla, ol hjabhssf mlsa tvyl ha lhzl. aol kvjavy zhpk pa dvbsk il slzz aohu h flhy. aoha nhcl opt h flhy av spcl

Plaintext sau khi giải mã:



Reference:

Mks075, *Encryption and decryption*, Computer Networks, <https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/> truy cập 16/04/2022

Ummme Ammara, *what are symmetric and asymmetric cryptosystem* [Creative Commons -Attribution -ShareAlike 4.0 (CC-BY-SA 4.0)], <https://www.educative.io/edpresso/what-are-symmetric-and-asymmetric-cryptosystems>, truy cập ngày 16/04/2022

Dan Rodriguez-Clark, *Monoalphabetic Substitution Cipher*, <https://crypto.interactive-maths.com/monoalphabetic-substitution-ciphers.html>, truy cập ngày 18/04/2022

101computing, *Frequency Analysis,Cryptography,*  ,<https://www.101computing.net/frequency-analysis/#:~:text=When%20trying%20to%20decrypt%20a,the%20letters%20in%20the%20text>, truy cập ngày 19/04/2022

Cori, *Ceasar-shift via Frequency analysis*, sl101, <https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/resources/ceasar-shift/freqAnalysis.html>, truy cập ngày 19/04/2022

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

*f Tần số của dòng điện và điện áp (Hz)*

*p Mật độ điện tích khối (C/m3)*

**CÁC CHỮ VIẾT TẮT**

CSTD Công suất tác dụng

MF Máy phát điện

BER Tỷ lệ bít lỗi