1

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

**<Classical Cryptography>**

**Môn học: An toàn mạng máy tính**

**Lớp: NT101.P21.1**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | Nguyễn Xuân Hà |
| **Sinh viên thực hiện** | Nguyễn Minh Quyền (23521325) |
| Phạm Nguyễn Tấn Sang (23521346) |
| Đỗ Hoàng Phúc (23521195) |
| **Mức độ hoàn thành** | Hoàn thành |
| **Thời gian thực hiện** | 06/03/2025 – 12/03/2025 |
| **Tự chấm điểm** | 10/10 |

* 1. **CÁC BƯỚC THỰC HÀNH**

**Gợi ý:** *Ghi rõ từng bước thực hành, chụp hình ảnh screenshot để báo cáo thêm trực quan*

* 1. **TRẢ LỜI CÁC CÂU HỎI**

## Task 1. Kickoff: Crack the code

Task 1.1. Let’s begin with a straightforward task that does not use any cipher algorithm. Try to solve the following codes:

1. We need to find the code to open the lock in Figure 4. The lock has a three-digit pin that satisfies five conditions (hints). Can you crack this code? If it’s possible, explain how.

A number padlock with numbers

AI-generated content may be incorrect.

Hình 1.1.1. Câu hỏi task 1a

1 | 9 | 3 : 1 số đúng và ở đúng vị trí

2 | 7 | 3: 1 số đúng nhưng không ở đúng vị trí

8 | 1 | 3 : 2 số đúng nhưng không ở đúng vị trí

4 | 0 | 3 : không có cái nào đúng

5 | 7 | 8 : 1 số đúng nhưng ở không ở đúng vị trí

**Giải:**

xét 4 | 0 | 3 : loại 4, 0, 3.

Xét 1 | 9 | 3 : số 1 hoặc số 9 đúng và ở đúng vị trí.

Xét 8 | 1 | 3 : chắc chắn số 1 và số 8 đúng nhưng sai vị trí => số 9 bị loại.

* Vị trí thứ nhất là số 1 => 1 | \* | \* .

Xét 5 | 7 | 8 : số 8 đã đúng nhưng sai vị trí lần 2 và số 5 với số 7 bị loại.

* Vị trí thứ hai là số 8 => 1 | 8 | \*

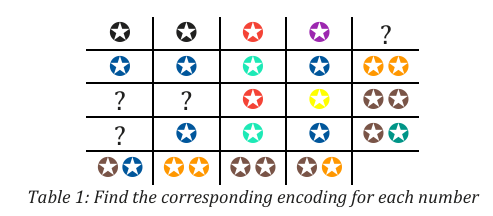
Xét 2 | 7 | 3 : số 2 đúng nhưng sai vị trí vì số 3 và số 7 đã bị loại.

* Vị trí thứ ba là số 2 => 1 | 8 | 2.

**Vậy đáp án là 1 | 8 | 2.**

1. Find the corresponding encoding for the numbers 1 to 9 according to the clues provided in Table 1:

* Each symbol in the set  unique encoding for one of the numbers from 1 to 9.
* The rightmost column is the sum of the numbers in each row.
* The bottom row is the sum of the number in each column.
* Each symbol “?” can represent either a one-digit number or a two-digit number. Thay can be different from each other.



Hình 1.1.2. Câu hỏi task 1b

**Giải:**

Để dễ hiểu và dễ trình bày, từ bảng đề bài em có bảng sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | A | B | C | ? |
| D | D | E | D | FF |
| ? | ? | B | G | HH |
| ? | D | E | D | HI |
| HD | FF | HH | HF |  |

* Xét hàng 2,3: FF, HH sẽ luôn nhỏ hơn 44 vì nó là tổng của các thành viên còn lại trong cùng 1 hàng, vì thế chỉ có thể là 11,22 hoặc 33.
* Xét cột 3: HH sẽ là 1 số chẵn vì nó là B + E + B + E = 2(B + E), do đó HH là 22 nên H = 2.
* Xét hàng 2: FF = D + D + E = 3D + E, ta thấy tổng này không thể bằng 11 được, vì thế FF = 33 nên F = 3.
* Từ kết quả ở trên ta được B + E = 11, do đó các cặp B, E có thể là 4 - 7, 5 - 6.
* Giả sử ta chọn B = 5, E = 6 thì ta được bảng mới như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | A | 5 | C | ? |
| D | D | 6 | D | 33 |
| ? | ? | 5 | G | 22 |
| ? | D | 6 | D | 2I |
| 2D | 33 | 22 | 23 |  |

* Từ bảng trên ta được D = 9 nên C + G = 5. Suy ra cặp C, G là cặp số 4, 1.
* Chọn C = 4, G = 1. Đặt ký tự cho các dấu ?. Ta được bảng mới:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | A | 5 | 4 | X |
| 9 | 9 | 6 | 9 | 33 |
| Y | T | 5 | 1 | 22 |
| Z | 9 | 6 | 9 | 2I |
| 29 | 33 | 22 | 23 |  |

* A và I chỉ có thể là cặp 7, 8.
* Giả sử chọn A = 8, I = 7, ta được:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 8 | 5 | 4 | X |
| 9 | 9 | 6 | 9 | 33 |
| Y | T | 5 | 1 | 22 |
| Z | 9 | 6 | 9 | 27 |
| 29 | 33 | 22 | 23 |  |

* X = 25, T = 7, Y = 9, Z = 3. Đối chiếu lại với các hàng và cột đều hợp lí.
* Suy ra ta kết luận được:

A close-up of a game

AI-generated content may be incorrect.

Hình 1.1.3. Bảng kết quả task 1b

## 2. Caesar cipher

Task 2.1 In this task, you must write an application using your chosen programming language to encrypt and decrypt a message using Caesar cipher. Your application should satisfy the following requirements:

Allow to input a key and a plaintext to encrypt or ciphertext to decrypt using a given key.

Allow brute-force all possible keys k to find the plaintext of given ciphertext without its key.

Test your program with a message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify. Then use your program to crack the following ciphertext:

Max NBM bl t extwbgz bglmbmnmbhg ngwxk OGN-AVF, lixvbtebsbgz bg max ybxew hy bgyhkftmbhg mxvaghehzr. Xlmtueblaxw pbma t fbllbhg mh yhlmxk bgghotmbhg tgw xqvxeexgvx bg BM xwnvtmbhg tgw kxlxtkva, NBM hyyxkl t pbwx ktgzx hy ngwxkzktwntmx tgw ihlmzktwntmx ikhzktfl tbfxw tm ikhwnvbgz abzaer ldbeexw ikhyxllbhgtel. Max ngboxklbmr bl kxvhzgbsxw yhk bml vnmmbgz-xwzx kxlxtkva bg tkxtl ebdx vruxklxvnkbmr, tkmbybvbte bgmxeebzxgvx, tgw lhymptkx xgzbgxxkbgz. Pbma lmtmx-hy-max-tkm ytvbebmbxl tgw t lmkhgz xfiatlbl hg vheetuhktmbhg pbma bgwnlmkr, NBM xjnbil lmnwxgml pbma uhma maxhkxmbvte dghpexwzx tgw iktvmbvte ldbeel mh makbox bg max ktibwer xoheobgz mxva bgwnlmkr.

Do you find any special concerning the key used to encrypt this ciphertext?

**Giải:**

A screenshot of a computer program

AI-generated content may be incorrect.

Hình 2.1.1. Code Caeser Cipher (1)

A screen shot of a computer program

AI-generated content may be incorrect.

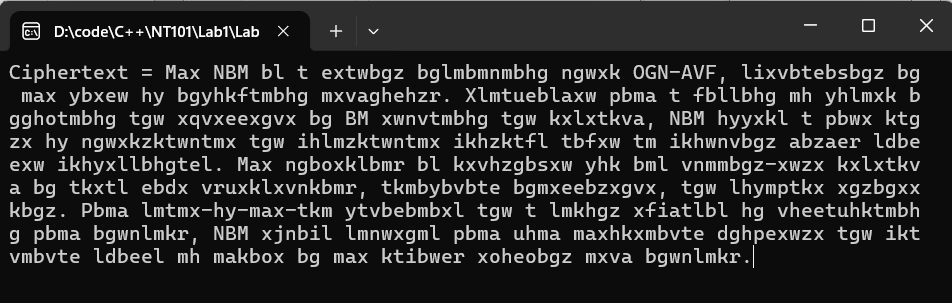
Hình 2.1.2. Code Caeser Cipher (2)

Giải thích code:

* Hàm EnCrytion được dùng để mã hóa ký tự và hàm DeCrytion được dùng để giải mã ký tự theo thuật toán Caeser Cipher.
* Đầu tiên kiểm tra ký tự có viết hoa hay không viết hoa, còn không thì sẽ là các ký tự đặc biệt, sau đó trả về 1 ký tự theo biểu thức sau: 'A' + (input - 'A' - key + 26) % 26.
* Input – ‘A’ : lấy ra thứ tự của input trong bảng chữ cái.
* input - 'A' – key : dịch chuyển input về trước 1 khoảng key hay lấy khoảng cách từ ‘A’ tới chữ cái mới khi chuẩn bị dịch chuyển.
* input - 'A' - key + 26 : cộng thêm 26 để kết quả luôn dương.
* % 26 : lấy dư để số luôn nằm trong khoảng [0, 25].
* ‘A’ + : để chuyển từ chỉ số qua lại ký tự chữ cái.
* Tương tự cho các biểu thức khác.
* Dòng 39: Nhập vào 1 chuỗi văn bản (s).
* Dòng 40: Lấy độ dài chuỗi.
* Dòng 42 – 47: Người dùng chọn phương thức mã hóa (Encryt) hoặc giải mã (Decryt).
* Dòng 49 – 59: Nhập key, sau đó duyệt và mã hóa tuần tự từng ký tự của chuỗi văn bản theo key vừa nhập để cho ra chuỗi mã hóa (Ciphertext).
* Dòng 61 – 72: Để giải mã thì duyệt qua từng key (1 - 25) với chuỗi văn bản, với từng key thì duyệt tuần tự từng ký tự để giải mã và cho ra chuỗi giải mã (Plaintext). Từ đây kiểm tra từng đáp án để tìm ra đáp án chính xác.

**Quá trình chạy chương trình:**

Nhập chuỗi ciphertext:



Hình 2.1.3. Chạy chương trình code Caeser Cipher (1)

Chọn giải mã (Decryt) và tìm kiếm kết quả đúng với từng key (1 - 25) được duyệt: 

A screenshot of a computer screen

AI-generated content may be incorrect.

Hình 2.1.4. Kết quả chạy code Caeser Cipher

Kết quả sau khi tìm kiếm tại key = 19:

Tương tự cho việc mã hóa (Encryt):

A screenshot of a computer

AI-generated content may be incorrect.

Hình 2.1.5. Chạy chương trình code Caeser Cipher (2)

## 3. Mono-alphabetic substitution cipher and frequency analysis

Task 3.1 See the attached file “3\_1\_cipher\_text” in the Courses for cypher text.

Your job is to find out the original text using the frequency analysis technique. It is known that the original text is an English article. Describe how to find the plaintext in detail (step-by-step).

**Giải:**

Giả sử: v – e, r – t, m – a, g – o (kí tự xuất hiện nhiều nhất)

j – x, a – q, c – z, q – j (kí tự xuất hiện ít nhất)

OhE Hliib KzOOEi sEiTEs, uiTOOEA yb YiTOTsh lfOhzi J.P. IzuoTAt, Ts zAE zd OhE nzsO kzkfoli lAw TAdofEAOTlo dlAOlsb sltls zd nzwEiA oTOEilOfiE.

* Xét từ “seites” có 6 kí tự có thể viết lại dưới dạng 0.1.2.3.1.0 (với mỗi kí tự thay thế bằng một số và kí tự giống nhau có số giống nhau). Kí tự 0, 5 giống nhau là ‘s’, kí tự 1, 4 giống nhua là ‘e’, kí tự 2 là ‘i’ và kí tự 3 là ‘t’. Trong tiếng anh chỉ có “series” là phù hợp.
* Vậy : s ~ s , i ~ r , t ~ i 🡪 s ~ s, i ~ r , r ~ i.
* OhE HlRRb KzOOER SERIES, uRIOOEA yb YRIOISh lfOhzR J.P. RzuoIAt, IS zAE zd OhE nzSO kzkfolR lAw IAdofEAOIlo dlAOlSb SltlS zd nzwERA oIOERlOfRE.
* Xét từ “uRIOOEA” có 7 kí tự, viết lại dưới dạng số 0.1.2.3.3.4.5. Kí tự 3 giống nhau ‘O’, kí tự 0 là ‘u’, kí tự 1 là ‘r’, kí tự 2 là ‘i’, kí tự 4 là ‘e’ và kí tự 5 là ‘a’. Trong tiếng anh ta thấy từ “written” là phù hợp.
* Vậy : u ~ w, o ~ t, a ~ n🡪 u ~ w, g ~ t, m ~ n.
* ThE HlRRb KzTTER SERIES, WRITTEN yb YRITISh lfThzR J.P. RzWoINt, IS zNE zd ThE nzST kzkfolR lNw INdofENTIlo dlNTlSb SltlS zd nzwERN oITERlTfRE.

-Xét từ “ThE” tương tự, ta thấy trong tiếng anh chỉ có chữ “the” là phù hợp.

* Vậy h ~ h.
* THE HlRRb KzTTER SERIES, WRITTEN yb YRITISH lfThzR J.P. RzWoINt, IS zNE zd THE nzST kzkfolR lNw INdofENTIlo dlNTlSb SltlS zd nzwERN oITERlTfRE.
* Xét từ “zNE” tương tự, ta thấy trong tiếng anh chỉ có chữ “one” là phù hợp.
* Vậy z ~ o.
* THE HlRRb KOTTER SERIES, WRITTEN yb YRITISH lfThOR J.P. RzWoINt, IS ONE Od THE nOST kOkfolR lNw INdofENTIlo dlNTlSb SltlS Od nOwERN oITERlTfRE
* Xét từ “YRITISH” tương tự, ta thấy trong tiếng anh chỉ có chữ “BRITISH” là phù hợp.
* Vậy y ~ b.
* THE HlRRb KOTTER SERIES, WRITTEN Bb BRITISH lfThOR J.P. RzWoINt, IS ONE Od THE nOST kOkfolR lNw INdofENTIlo dlNTlSb SltlS Od nOwERN oITERlTfRE
* Xét từ “Bb” tương tự chỉ có từ “by” là phù hợp.
* Vậy b ~ y.
* THE HlRRY KOTTER SERIES, WRITTEN BY BRITISH lfThOR J.P. ROWoINt, IS ONE Od THE nOST kOkfolR lNw INdofENTIlo dlNTlSY SltlS Od nOwERN oITERlTfRE
* Xét từ “Od” và “nOST” chỉ có “of” và “most” là phù hợp.
* Vậy d ~ f, n ~ m.
* THE HlRRY KOTTER SERIES, WRITTEN BY BRITISH lfThOR J.P. ROWoINt, IS ONE OF THE MOST kOkfolR lNw INFofENTIlo FlNTlSY SltlS OF MOwERN oITERlTfRE
* Tương tự ta suy ra: w ~ d, l ~ a, k ~ p, p ~ k.
* THE HARRY POTTER SERIES, WRITTEN BY BRITISH AfTHOR J.K. ROWoINt, IS ONE OF THE MOST POPfoAR AND INFofENTIAo FANTASY SAtAS OF MODERN oITERATfRE
* Tương tự, ta suy ra: f ~ u, o ~ l, t ~ g.
* THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.K. ROWLING, IS ONE OF THE MOST POPULAR AND INFULENTIAL FANTASY SAGAS OF MODERN LITERATfRE
* Còn lại: e ~ v, x ~ c.
* Bảng giải mã kí tự :

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

* Đoạn văn hoàn chỉnh là:

The Harry Potter Series, Written By British Author J.K. Rowling, Is One Of The Most Popular And Influential Fantasy Sagas Of Modern Literature. Spanning Seven Books, The Series Follows The Life Of A Young Boy, Harry Potter, Who Discovers On His 11th Birthday That He Is A Wizard. He Is Invited To Attend Hogwarts School Of Witchcraft And Wizardry, Where He Learns About His Magical Heritage, Develops Close Friendships, And Confronts The Dark Forces That Threaten The Wizarding World.

The Central Plot Revolves Around Harry's Ongoing Battle With Lord Voldemort, A Dark Wizard Intent On Conxuering Both The Magical And Non-Magical Worlds. As Harry Grows Older, He Learns More About His Own Mysterious Past, His Connection To Voldemort, And The Prophecy That Ties Their Fates Together. Throughout The Series, Themes Of Friendship, Loyalty, Bravery, And The Power Of Love Are Explored, With A Rich World Filled With Magical Creatures, Spells, And Deep Mythology.

The Books, Starting With Harry Potter And The Philosopher's Stone (1997) And Concluding With Harry Potter And The Deathly Hallows (2007), Have Sold Over 500 Million Copies Worldwide, Been Translated Into More Than 80 Languages, And Adapted Into A Successful Film Series. The Series Is Known Not Only For Its Enchanting World-Building But Also For Addressing Darker, Complex Themes Such As Mortality, Prejudice, And The Abuse Of Power. The Harry Potter Series Has Left An Indelible Mark On Popular Culture, Fostering A Global Fan Base, Inspiring Countless Spin-Offs, And Cementing Its Place As A Literary Phenomenon.

Vietnam National University, Ho Chi Minh City (Vnu-Hcm) Is One Of The Most Prestigious And Comprehensive Higher Education Institutions In Vietnam, Known For Its Excellence In Research, Innovation, And Education. Founded In 1995 By The Vietnamese Government, Vnu-Hcm Was Established As A Key Center For Training, Research, And Technology Transfer With The Mission Of Contributing To The Country’s Socio-Economic Development. As A Flagship University, It Has Played A Pivotal Role In Producing Highly Skilled Professionals, Scientists, And Leaders Across Multiple Fields.

Vnu-Hcm Operates Under A Distinctive Structure As A Multi-Disciplinary And Multi-Campus System, Comprising Several Member Universities And Research Institutes. These Include Some Of The Most Well-Established Institutions In The Region, Such As The University Of Science, University Of Technology, University Of Social Sciences And Humanities, International University, University Of Economics And Law, And Others. Each Of These Member Institutions Operates Semi-Independently But Collaborates Under The Umbrella Of Vnu-Hcm, Making It A Unique Higher Education Model In Vietnam That Promotes Interdisciplinary Learning And Research.

Located In Ho Chi Minh City, The Country's Economic And Cultural Hub, Vnu-Hcm Benefits From Close Ties With Industries, Businesses, And Government Agencies. This Proximity Fosters Collaboration In Research, Internships, And Job Placement, Ensuring That Its Graduates Are Well-Prepared To Meet The Demands Of An Evolving Workforce. The University Is Committed To Producing Graduates Who Are Not Only Academically Proficient But Also Equipped With Practical Skills And A Global Outlook.

Vnu-Hcm Is Renowned For Its Strong Emphasis On Scientific Research And Technological Innovation. It Houses Numerous Research Centers, Institutes, And Labs That Focus On Various Areas Of Science, Engineering, Social Sciences, Economics, And More. The University's Research Agenda Is Aligned With National Priorities, Focusing On Areas Such As Information Technology, Biotechnology, Renewable Energy, And Environmental Sustainability. Vnu-Hcm Also Actively Engages In International Cooperation, Partnering With Leading Universities And Research Institutions Worldwide To Enhance Its Academic Programs, Foster Joint Research Projects, And Promote Student And Faculty Exchanges.

The University Is Also Deeply Involved In Addressing Global Challenges Through Its Research And Educational Programs. Vnu-Hcm Places A Strong Emphasis On Sustainable Development, Environmental Conservation, And Technological Innovation, Aligning Its Goals With The United Nations’ Sustainable Development Goals (Sdgs). The Institution Encourages Its Faculty And Students To Pursue Research That Has A Meaningful Impact On Both The Local And Global Community.

In Terms Of Student Life, Vnu-Hcm Offers A Vibrant And Dynamic Environment. With A Student Body Of Over 60,000 And A Faculty Of Highly Qualified Professors And Researchers, The University Provides A Rich Academic And Social Experience. The Campuses Are Equipped With Modern Facilities, Including Libraries, Laboratories, Sports Complexes, And Dormitories, Creating A Supportive Learning Environment. Students Also Have Access To A Variety Of Extracurricular Activities, Clubs, And Organizations, Allowing Them To Engage In Cultural, Social, And Professional Development Alongside Their Studies.

In Conclusion, Vietnam National University - Ho Chi Minh City Stands As A Leading Educational Institution In Vietnam, Contributing Significantly To The Country’s Intellectual, Scientific, And Economic Progress. Its Commitment To Academic Excellence, Research Innovation, And Societal Impact Has Positioned It As A Crucial Player In Shaping The Future Of Vietnam And The Broader Region. As It Continues To Evolve And Expand, Vnu-Hcm Remains Dedicated To Fostering The Next Generation Of Leaders And Innovators Who Will Drive Sustainable Growth And Global Progress.

Advanced Task 3.2 See the attached file “3\_2\_cipher\_text” in the Courses for cypher text.

Decrypt the cypher text and explain how to do It is known that:

* The original text is an English article.
* The cypher text does not include “,”,”.” and spaces.
* Each symbol corresponds to a letter in the English alphabet.

**Giải:**

Giả sử :

\* ~ e

6 ~ t

+ ~ a

8 ~ o

2 ~ z

9 ~ x

# ~ j

‘ ~ q

T7E 7-OO1 0ATTEO %EO$E%, &O$TTE= \_1\_O$T$%7 -5T7AO Q.@. OA&!$=^, $% A=E A3 T7E ~A%T 0A05!-O -=( $=3!5E=T$-! 3-=T-%1 %-^-% A3 ~A(EO= !$TEO-T5OE...

* Xét từ “%EO$E%” có 6 kí tự có thể viết lại dưới dạng 0.1.2.3.1.0 (với mỗi kí tự thay thế bằng một số và kí tự giống nhau có số giống nhau). Kí tự 0, 5 giống nhau là ‘%’, kí tự 1, 4 giống nhau là ‘e’, kí tự 2 là ‘o’ và kí tự 3 là ‘$’. Trong tiếng anh chỉ có “series” là phù hợp.
* Vậy % ~ s, o ~ r, $ ~ i 🡪 % ~ s, 8 ~ r, $ ~ i.
* T7E 7-RR1 0ATTER SERIES, &RITTE= \_1 \_RITIS7 -5T7AR J.@. RA&!I=^, IS A=E A3 T7E ~AST 0A05!-R -=( I=3!5E=TI-! 3-=T-S1 S-^-S A3 ~A(ER= !ITER-T5RE...
* Xét từ “&RITTE=” có 7 kí tự, viết lại dưới dạng số 0.1.2.3.3.4.5. Kí tự 3 giống nhau ‘T’, kí tự 0 là ‘&’, kí tự 1 là ‘r’, kí tự 2 là ‘i’, kí tự 4 là ‘e’ và kí tự 5 là ‘=’. Trong tiếng anh ta thấy từ “written” là phù hợp.
* Vậy & ~ w, = ~ n.
* T7E 7-RR1 0ATTER SERIES, WRITTEN \_1 \_RITIS7 -5T7AR J.@. RAW!IN^, IS ANE A3 T7E ~AST 0A05!-R -N( IN3!5ENTI-! 3-NT-S1 S-^-S A3 ~A(ERN !ITER-T5RE...
* Tương tự, ta thấy từ “T7E” chỉ có từ “The” trong tiếng anh là phù hợp
* Vậy 7~h.
* THE H-RR1 0OTTER SERIES, WRITTEN \_1 \_RITISH -5THOR J.@. ROW!IN^, IS ONE O3 THE ~OST 0O05!-R -N( IN3!5ENTI-! 3-NT-S1 S-^-S O3 ~O(ERN !ITER-T5RE...
* Tương tự, ta thấy “ANE” gần giống với từ “one”.
* Vậy a ~ o 🡪 + ~ o.
* Tương tự, các từ “~OST”, “O3” lần lượt giống với các từ “MOST”, “OF”
* Vậy ~ ~ m, 3 ~ f.
* THE H-RR1 0OTTER SERIES, WRITTEN \_1 \_RITISH -5THOR J.@. ROW!IN^, IS ONE OF THE MOST 0O05!-R -N( IN3!5ENTI-! 3-NT-S1 S-^-S O3 MO(ERN !ITER-T5RE...
* Xét từ “MO(ERN” ta thấy tương tự với từ “modern”.
* Vậy ( ~ d.
* THE H-RR1 0OTTER SERIES, WRITTEN \_1 \_RITISH -5THOR J.@. ROW!IN^, IS ONE OF THE MOST 0O05!-R -ND IN3!5ENTI-! 3-NT-S1 S-^-S O3 MODERN !ITER-T5RE...
* Tương tự, các từ “\_RITISH”, “-ND” lần lượt giống với các từ “BRITISH”, “AND”.
* Vậy \_ ~ b, - a.
* THE HARR1 0OTTER SERIES, WRITTEN B1 BRITISH A5THOR J.@. ROW!IN^, IS ONE OF THE MOST 0O05!AR AND INF!5ENTIA! FANTAS1 SA^AS OF MODERN !ITERAT5RE...
* Với các từ “A5THOR” 🡪 “author”, “HARR1 0OTTER” 🡪 “HARRY POTTER”.
* Vậy 5 ~ u, 1 ~ y, 0 ~ p.
* THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.@. ROW!IN^, IS ONE OF THE MOST POPU!AR AND INF!UENTIA! FANTASY SA^AS OF MODERN !ITERATURE...
* Tương tự, xét từ “!ITERATURE” giống với từ “literature”.
* Vậy ! ~ l.
* THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.@. ROWLIN^, IS ONE OF THE MOST POPULAR AND INFLUENTIAL FANTASY SA^AS OF MODERN LITERATURE..
* Các từ còn lại: @ ~ K, ^ ~ G.
* THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.K. ROWLING, IS ONE OF THE MOST POPULAR AND INFLUENTIAL FANTASY SAGAS OF MODERN LITERATURE...
* Bảng mã hoàn chỉnh:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ~ | ! | @ | # | $ | % | ^ | & | \* | ( | ) | \_ | - | + | = | ` | ‘ |
| p | y | z | f | v | u | t | h | r | x | m | l | k | j | i | s | g | w | e | d | c | b | a | o | n | q |  |

* Đoạn văn hoàn chỉnh là:

The Harry Potter Series, Written By British Author J.K. Rowling, Is One Of The Most Popular And Influential Fantasy Sagas Of Modern Literature. Spanning Seven Books, The Series Follows The Life Of A Young Boy, Harry Potter, Who Discovers On His 11th Birthday That He Is A Wizard. He Is Invited To Attend Hogwarts School Of Witchcraft And Wizardry, Where He Learns About His Magical Heritage, Develops Close Friendships, And Confronts The Dark Forces That Threaten The Wizarding World.

The Central Plot Revolves Around Harry's Ongoing Battle With Lord Voldemort, A Dark Wizard Intent On Conxuering Both The Magical And Non-Magical Worlds. As Harry Grows Older, He Learns More About His Own Mysterious Past, His Connection To Voldemort, And The Prophecy That Ties Their Fates Together. Throughout The Series, Themes Of Friendship, Loyalty, Bravery, And The Power Of Love Are Explored, With A Rich World Filled With Magical Creatures, Spells, And Deep Mythology.

The Books, Starting With Harry Potter And The Philosopher's Stone (1997) And Concluding With Harry Potter And The Deathly Hallows (2007), Have Sold Over 500 Million Copies Worldwide, Been Translated Into More Than 80 Languages, And Adapted Into A Successful Film Series. The Series Is Known Not Only For Its Enchanting World-Building But Also For Addressing Darker, Complex Themes Such As Mortality, Prejudice, And The Abuse Of Power. The Harry Potter Series Has Left An Indelible Mark On Popular Culture, Fostering A Global Fan Base, Inspiring Countless Spin-Offs, And Cementing Its Place As A Literary Phenomenon.

## 4. Playfair cipher

Task 4.1 Encrypt and decrypt using Playfair cipher. You are able to use public tools or your own tool that was developed in the advanced task 4.2. Given the cipher text:

ARYWYPHCBVEBYGMPNCYGCNTDNCWTMGRMFTQPLEWTMLREFBEBQEBIYGBFLPHVOAEHKDHEUNGQFEROLEWTMLOPHEQGOSBEROQDWTLCMTHBWLNRKXRYLORYYPHCBVEBYRLGYDMKYGGWKLROANDBWGNERMNGYRLGHEWRTRLMBRHMUDGVODVTEGMCHLGWCMTFODNRRYCMZKODDUTDXGEOPOYRMFRMGUKXRYGHABROVTGQMCEHPRPEOTSEGEQLARYWYPOTMGQDOEXGOAUDHGUTULTNEHFTFHPGXGVPHGURBDMEGWKLETCBOTNTFQLTAEHMTUGEOAHEVEROXGVPHGDEWTEWGQIEDLPILERWPMOATNGQKQEAHBMVRFKBRMKLXODXFREBHMNUKXRYKLRMFLWDDNCN

The key used was Harry Potter. Let’s decrypt the message.

**Giải:**

A screenshot of a computer

AI-generated content may be incorrect.

Hình 4.1.1. Chạy và cho ra kết quả của chương trình code PlayFair

Advanced Task 4.2 In this extra task, you have to write an application using your own programming language to encrypt and decrypt a message using Playfair cypher. Your application should satisfy the following requirements:

* Allow you to input a key and the plain text to encrypt or a cypher text to decrypt.
* Display the Playfair matrix (5x5) corresponding with the given key.

Test your program with a message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify.

**Giải:**

A screen shot of a computer screen

AI-generated content may be incorrect.

Hình 4.2.1. Code chương trình thuật toán mã hóa/mã hóa Playfair (1)

A computer screen shot of a program code

AI-generated content may be incorrect.

Hình 4.2.2. Code chương trình thuật toán mã hóa/mã hóa Playfair (2)

A computer screen shot of a program

AI-generated content may be incorrect.

Hình 4.2.3. Code chương trình thuật toán mã hóa/mã hóa Playfair (3)

A screenshot of a computer program

AI-generated content may be incorrect.

Hình 4.2.4. Code chương trình thuật toán mã hóa/mã hóa Playfair (4)

A screen shot of a computer program

AI-generated content may be incorrect.

Hình 4.2.5. Code chương trình thuật toán mã hóa/mã hóa Playfair (5)

**Giải thích code:**

1. Hàm fillMatrix:

* Hàm dùng để điền 1 ma trận kích thước 5x5 với khóa key đầu vào và sau đó điền các ký tự chữ cái còn thiếu ( ‘I’ và ‘J’ là một) dựa trên thuật toán Playfair.
* Sử dụng set<char> used để lưu các ký tự chữ cái đã điền và ma trận nhằm tránh trùng lặp ký tự.
* Tiếp theo điền các ký tự của khóa key vào ma trận khóa, ký tự sẽ được viết hoa để đồng bộ dữ liệu khóa.
* Tiếp đến thay ký tự ‘J’ thành ‘I’ để đủ 25 ký tự chữ cái cho ma trận 5x5, kế đến kiểm tra xem ký tự này đã được điền hay chưa bằng cách sử dụng used để kiểm tra.
* Sau khi đã điền xong khóa thì sẽ điền các ký tự chữ cái còn thiếu vào ma trận, cũng thay ‘J’ bằng ‘I’ và kiểm tra chữ cái đã được sử dụng hay chưa.

1. Hàm printMatrix: dùng để in ma trận khóa.
2. Hàm processString:

* Hàm dùng để biến chuỗi văn bản thành 1 chuỗi có từng cặp 2 ký tự liền nhau và từng cặp cách nhau bởi 1 khoảng trắng, với mỗi 1 cặp ký tự giống nhau thì sẽ tách ra và thêm ‘X’ vào sau ký tự đầu tiên đó, còn ký tự còn lại sẽ liên kết với các ký tự sau của chuỗi văn bản theo thuật toán của Playfair.
* Dòng 46 – 49: Loại bỏ khoảng trắng trong văn bản và biến chuỗi thành chuỗi in hoa.
* Dòng 51: chia chuỗi thành từng cặp ký tự.
* Dòng 52 – 53: lấy ký tự đầu của cặp và ký tự sau của cặp, nếu mà cặp cuối của chuỗi chỉ có 1 ký tự thì sẽ thêm ‘X’ vào sau ký tự đó để thành 1 cặp hoàn chỉnh.
* Dòng 54 – 58: xử lý 2 ký tự trùng nhau, chèn thêm ‘X’ vào giữa chúng, i-- để nó lặp lại ở cặp tiếp theo.
* Dòng 59 – 62: nếu 2 ký tự không trùng thì giữ nguyên cặp đó.
* Dòng 63 – 64: sau đó thêm khoảng trắng vào giữa mỗi cặp.
* Cuối cùng trả về chuỗi đã chỉnh sửa.

1. Struct Point: Tạo 1 kiểu biến Point để lưu giữ tọa độ của ký tự trong ma trận khóa.
2. Hàm EnCrytion và DeCrytion:

* Hàm EnCrytion và DeCrytion dùng để mã hóa và giải mã ký tự theo thuật toán Playfair.
* Dòng 78 – 79: Khai báo biến Point nhằm lưu trữ tọa độ cho 2 ký tự cần mã hóa.
* Dòng 81 – 96: tìm kiếm tọa độ 2 ký tự mã hóa trong ma trận khóa.
* Dòng 97 – 101: nếu 2 ký tự mã hóa cùng hàng (row) thì cả 2 sẽ dịch qua phải 1 đơn vị, nếu ký tự ở cuối hàng (row) thì sẽ quay lại từ ký tự đầu hàng (row).
* Dòng 102 – 106: nếu 2 ký tự mã hóa cùng cột (col) thì cả 2 sẽ dịch xuống 1 đơn vị, nếu ký tự ở cuối cột (col) thì sẽ quay lại từ ký tự đầu cột (col).
* Dòng 107 – 108: Trường hợp cuối là khi 2 ký tự mã hóa tọa nên 1 hình chữ nhật trong ma trận khóa, khi đó cả 2 sẽ trao đổi tọa độ cột cho nhau.
* Dòng 109 – 110: 2 ký tự mã hóa sẽ lấy ký tự mới dựa trên tọa độ mới của mình.
* Tương tự cho DeCrytion nhưng ngược lại so với EnCrytion.

1. Hàm main:

* Nhập vào chuỗi văn bản, sau đó chuỗi văn bản sẽ được chỉnh sửa dựa vào hàm processString.
* Sau đó nhập chuỗi khóa (key), khi đó sẽ tạo ra ma trận khóa dựa vào hàm fillMatrix.
* Chọn các phương thức Encryt hoặc Decryt để mã hóa hoặc giải mã chuỗi văn bản.
* Với mỗi phương thức thì sẽ duyệt qua từng cặp ký tự để mã hóa hoặc giải mã.

**Quá trình chạy chương trình:**

Với văn bản “*Doan trich Xuan Toc Do cuu quoc la mot phan quan trong trong tac pham So Do cua nha van Vu Trong Phung Khong chi la mot cau chuyen no con la mot buc tranh song dong ve cuoc song va thoi dai Voi chi tiet va su sac net tac gia da tao ra mot buc tranh chan thuc ve xa hoi Viet Nam trong giai doan lich su day bien dong Tac pham khong chi tap trung vao nhan vat chinh ma con phan anh sau sac ve tinh hinh chinh tri xa hoi va tam ly con nguoi Su tuong tac giua cac nhan vat cung voi nhung hinh anh ve cuoc song hang ngay voi nhung rac roi trong quan he con nguoi da khien doc gia dam chim trong the gioi ma tac gia tao ra Dieu nay lam noi bat kha nang cua tieu thuyet trong viec phan anh va lam sang to nhung khia canh sau sac cua xa hoi va con nguoi Qua doan trich chung ta co the thay duoc kha nang sang tao da dang cua van hoc va ky thuat viet de mo ta cuoc song phong phu va da chieu cung voi thong diep tu tuong ma tac gia muon truyen dat qua nhung trang van*” thành chuỗi mã hóa với Key = “maytinh”:

A screenshot of a computer

AI-generated content may be incorrect.

Hình 4.2.6. Chạy chương trình thuật toán Playfair (1)

A black and white screen with white letters

AI-generated content may be incorrect.

Hình 4.2.7. Chạy chương trình thuật toán Playfair (2)

## 5. Polyalphabetic ciphers – Vigenère

Task 5.1 In this task, your job is to write an application using your chosen programming language to encrypt and decrypt a message using Vigenère cipher.

Test your program with a message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify.

**Giải:**

A screen shot of a computer program

AI-generated content may be incorrect.

Hình 5.1.1 Code chương trình theo thuật toán mã hóa/giải mã Vigenère Cipher (1)

A computer screen shot of a program code

AI-generated content may be incorrect.

Hình 5.1.2 Code chương trình theo thuật toán mã hóa/giải mã Vigenère Cipher (2)

**Giải thích code:**

* Hàm EnCrytion và DeCrytion được dùng để mã hóa và giải mã ký tự ứng dụng theo thuật toán Vigenère cipher.
* Đầu tiên kiểm tra ký tự có viết hoa hay không viết hoa, còn không thì sẽ là các ký tự đặc biệt, sau đó trả về 1 ký tự theo biểu thức sau: 'A' + (input - 'A' - key + 26) % 26.
* Input – ‘A’ : lấy ra thứ tự của input trong bảng chữ cái.
* Key – ‘A’ : lấy ra thứ tự của key trong bảng chữ cái.
* input - 'A' + (key – ‘A’) : dịch chuyển input về trước 1 khoảng shift hay lấy khoảng cách từ ‘A’ tới chữ cái mới khi chuẩn bị dịch chuyển.
* input - 'A' + (key – ‘A’) + 26 : cộng thêm 26 để kết quả luôn dương.
* % 26 : lấy dư để số luôn nằm trong khoảng [0, 25].
* ‘A’ + : để chuyển từ chỉ số qua lại ký tự chữ cái.
* Tương tự cho DeCrytion.
* Dòng 41 – 43: Nhập chuỗi văn bản (s) và lấy độ dài chuỗi.
* Dòng 45 – 47: Nhập chuỗi key và lấy độ dài key.
* Dòng 50 – 55: Người dùng chọn phương thức mã hóa (Encryt) hoặc giải mã (DeCryt).
* Dòng 49: Biến j dùng để duyệt qua từng ký tự của chuỗi key, nếu j = độ dài chuỗi key thì sẽ qua trở lại bằng 0.
* Dòng 56 – 68: Duyệt qua từng ký tự của chuỗi văn bản và tương ứng với đó là ký tự của chuỗi key để mã hóa từng ký tự, sau đó cho ra chuỗi mã hóa (Ciphertext).
* Dòng 69 – 81: Duyệt qua từng ký tự của chuỗi văn bản và tương ứng với đó là ký tự của chuỗi key để giải mã từng ký tự, sau đó cho ra chuỗi giải mã (Plaintext).

**Quá trình chạy chương trình:**

Mã hóa chuỗi văn bản “hello world” với key = “maytinh”:

A screenshot of a computer program

AI-generated content may be incorrect.

Hình 5.1.3. Chạy chương trình code thuật toán Vigenère Cipher (1)

Giải mã lại chuỗi mã hóa vừa rồi “tejew jvdlb” với cùng key = “maytinh”:

A screenshot of a computer program

AI-generated content may be incorrect.

Hình 5.1.4. Chạy chương trình code thuật toán Vigenère Cipher (2)