CRYPTHONOLOGY

AN INTEGRATION OF PYTHON PROGRAMMING IN MESSAGE ENCRYPTION AND DECRYPTION

INTRODUCTION

PROBLEM STATEMENT

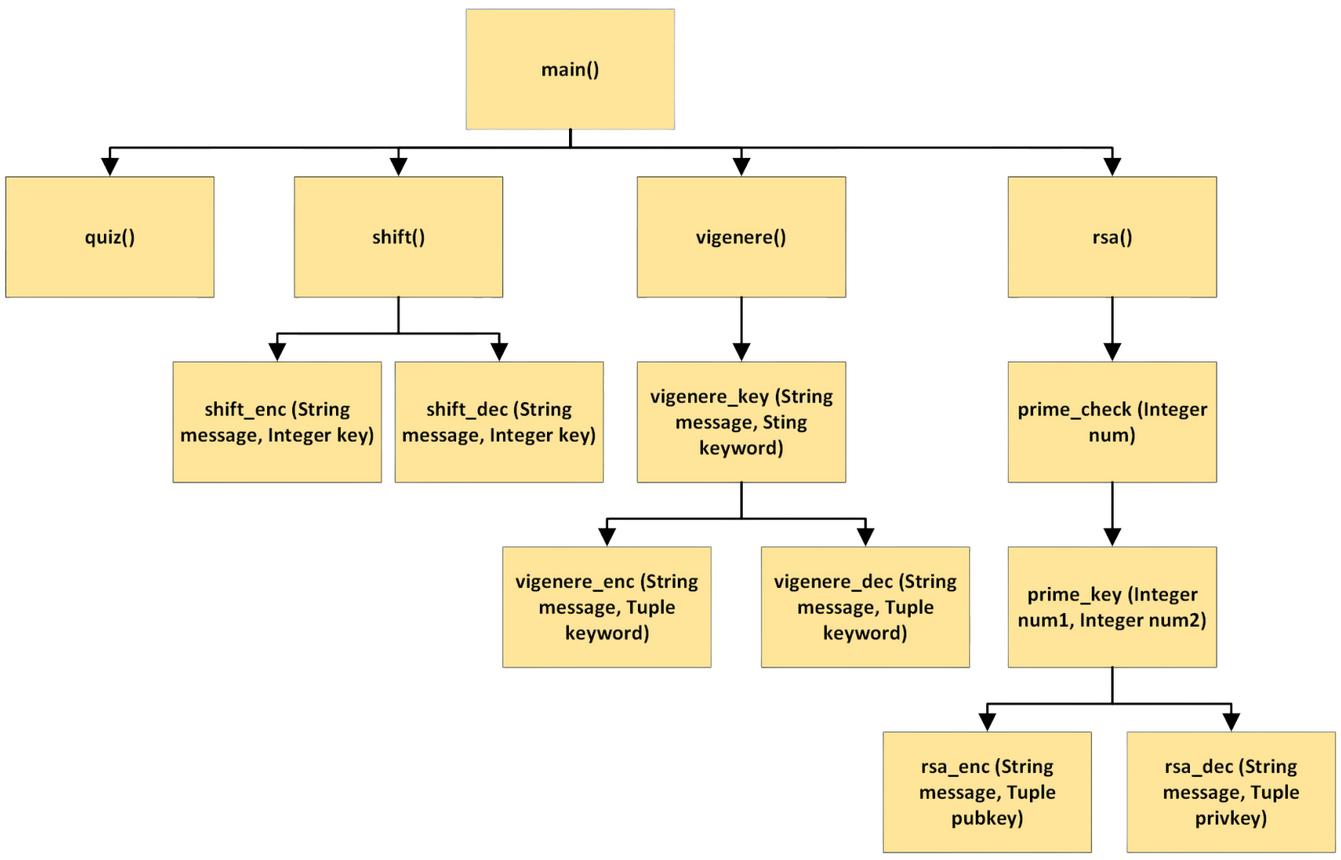
THIS PROJECT AIMS TO PROVIDE AND ASSESS BASIC CRYPTOGRAPHY KNOWLEDGE THROUGH SIMULATING THE VARIOUS ENCRYPTION AND DECRYPTION PROCESSES OF SELECTED CRYPTOGRAPHIC METHODS AND A KNOWLEDGE-ASSESSMENT TEST.

OBJECTIVES

- TO DEVELOP EFFECTIVE AND EFFICIENT ALGORITHMS FOR EACH CRYPTOGRAPHIC METHOD
- TO ENSURE THE FUNCTIONALITY OF THE PROGRAM BY CORRECTLY DISPLAYING THE ENCRYPTED AND DECRYPTED MESSAGE
- TO OPTIMIZE THE PROGRAM'S PERFORMANCE BY IMPLEMENTING APPROPRIATE AND EFFICIENT DATA STRUCTURES
- TO ESTABLISH AN OPERATIVE SCORE TRACKING SYSTEM FOR THE PROGRAM 'QUIZ' COMPONENT
- TO IMPLEMENT AND UTILIZE BUILT-IN PYTHON MODULES IN THE OVERALL PROGRAM DEVELOPMENT

METHODOLOGY

HIERARCHY CHART



MATERIALS/TOOLS USED

- JUPYTER NOTEBOOK
- MS VISIO AND MS WORD
- INSTRUCTOR'S NOTES (LABORATORY MANUAL)
- TEXTBOOK ON CRYPTOGRAPHY (ESSENTIAL MATHEMATICS IN THE MODERN WORLD, 2018)
- ONLINE GUIDES AND TUTORIALS ON PROGRAMMING LANGUAGES

RESULTS

RESULTS OF ALL COMPONENTS

SHIFT CIPHER

```
shift()


Input message: LBYCPA
Input key: 8
Encrypt (1) or Decrypt (2)
Input number: 1
The encrypted message is TJaKXI
Change message? (1)
Change key? (2)
Exit(3)
Input number: 1
Input message: TJaKXI
Encrypt (1) or Decrypt (2)
Input number: 2
The decrypted message is LBYCPA
Change message? (1)
Change key? (2)
Exit(3)
Input number: 3
```

RSA CRYPTOGRAPHY

```
rsa()


Input message: HELLO
Input a large prime number: 43
Input another large prime number: 11
Your public key is  [473, 11]
Your private key is  [473, 191]
The encrypted text is  248 234 329 329 178
Change message? (1)
Decrypt the message? (2)
Exit(3)
Input number: 2
The decrypted text is  72 69 76 76 79
Change message? (1)
Exit(2)
Input number: 2
```

VIGENERE CIPHER

```
vigenere()


Input message: HELLO
Input keyword: HI
The modified keyword is  ['H', 'I', 'H', 'I', 'H']
Encrypt (1) or Decrypt (2)
Input number: 1
The encrypted text is OMSTV
Change message? (1)
Change key? (2)
Exit(3)
Input number: 1
Input message: OMSTV
The modified keyword is  ['H', 'I', 'H', 'I', 'H']
Encrypt (1) or Decrypt (2)
Input number: 2
The decrypted text is HELLO
Change message? (1)
Change key? (2)
Exit(3)
Input number: 3
```

QUIZ COMPONENT

```
quiz()

What is the process of using an algorithm to transform information into a format that cannot be read?
ENCRYPTION
Correct!
Is Vigenere Cipher monoalphabetic or polyalphabetic?
POLYALPHABETIC
Correct!
If the encrypted message is PFCGTE from LBYCPA, what is the key of the shift cipher?
4
Correct!
What key is used to decrypt in RSA cryptography?
PRIVATE
Correct!
Which of the following cryptographic methods uses a keyword?
Vigenere
Correct!
Quiz completed! You scored 5/5 points.
```

REFERENCES

COGHLAN, N., VAN ROSSUM, G., & WARSAW, B. (2001). PEP 8 - STYLE GUIDE FOR PYTHON CODE. PYTHON ENHANCEMENT PROPOSALS. HTTPS://PEPS.PYTHON.ORG/PEP-0008/

NOCON, E. & NOCON, R. (2018). ESSENTIAL MATHEMATICS FOR THE MODERN WORLD. C & E PUBLISHING, INC.

REITER, R. (N.D.). INTRO TO PYTHON TUTORIAL. INTERACTIVE TUTORIALS. HTTPS://WWW.LEARNPYTHON.ORG/

THE ASIA FOUNDATION (2022). CYBERSECURITY IN THE PHILIPPINES: GLOBAL CONTEXT AND LOCAL CHALLENGES. HTTPS://ASIAFOUNDATION.ORG/WP-CONTENT/UPLOADS/2022/03/CYBERSECURITY-IN-THE-PHILIPPINES-GLOBAL-CONTEXT-AND-LOCAL-CHALLENGES-.PDF

W3SCHOOLS. (2023). PYTHON TUTORIAL. REFSNES DATA. HTTPS://WWW.W3SCHOOLS.COM/PYTHON/

CONCLUSION/ RECOMMENDATIONS

- INCORPORATE MORE CRYPTOGRAPHIC METHODS TO ESTABLISH A DIVERSIFIED LEARNING PLATFORM FOR CRYPTOGRAPHY
  - CRYPTOGRAPHIC METHODS HAVE ITS LIMITATIONS
  - ESSENTIAL IN TACKLING TOPICS SUCH AS CYBERSECURITY AND DATA PRIVACY
- DISPLAY A COMPARISON BETWEEN CRYPTOGRAPHIC METHODS BASED ON THEIR STRENGTHS AND WEAKNESSES