ENCRYPTION KEY

Encryption Key

Third Semester -2023

Cyber Security

Group: Four

Edit by:

Abdullah Alsalem

Hamad Altawab

Naif Alsubaie

Habeeb Almarai

info@encryption-key.netlify.app

www.encryption-key.netlify.app

PROJECT OVERVIEW

Encryption key platform is a free platform concerned with teaching the method of encryption and decryption for many old and new Ciphers, and its developers are very interested in facilitating the learning method, and its supervisors aspire to be an integrated platform for everyone who wants to learn encryption and decryption for many of ciphers, what distinguishes this platform is that it works in both Arabic and English and shortens a lot of the learner's time in terms of research and investigation in the required code, and we aspire that our platform will be a destination for all trainers and trainees in all educational commission, So that it is a curriculum for learning and knowledge, and we will plan in the future to provide academic training courses on the platform, and we will also apply user experience (UX) rules on our platform so that all users can use all the tools of our platform because it will be easy to use for adults, children, learners and uneducated and will be our target audience with different abilities through the use of icons that will help people who suffer from the inability to read or understand Arabic and English and we will take into account the blind by observing how to read the browser The idea of the platform will be similar to Google Translate, which is used by an infinite number of people around the world so that the user can paste or write the phrase he wants to encrypt and then choose the cipher from the drop-down list and type the key from then the platform will give him the ciphertext with ease and ease, and in order not to distract the user, we will put a link at the bottom of each tool to go to the detailed explanations for each cipher and there will be a box in the lower right corner of the screen with an explanation Simplified for each cipher.

As a group, we believe that our platform will solve the problem of the great challenges faced by male and female students in understanding many ciphers, and we also expect the number of users of our platform to increase with the obsolescence of years in light of the direction of our dear Kingdom in activating cybersecurity sciences in the intermidate and secondary stages.

This platform will contribute to gaining a lot of visitors' integrated knowledge of encryption methods, and this will be a free social contribution and free learning for a party to encrypt and decrypt the most important old or new cyphers.

TABLE OF CONTENTS

PROBLEM STATEMENT

The meaning of cryptography is general

Encryption in cybersecurity means converting data from a readable format to an encrypted one. Encrypted data can be read or processed only after it has been decrypted. Encryption is the basic building block of data security. It is the simplest and most important way to ensure that computer system information is not stolen or read by someone who wants to use it for malicious purposes.

What is problem?

The problem for establishing this project lies around the lack of Arab resources that help and contribute to understanding Applied Cryptography and conducting encryption operations automatically, quickly and accurately, and collecting many ciphers in one place, and this project will contribute, with the grace and power of God, to increasing society's awareness of cryptography and scientific excellence among students of cybersecurity at the level of the Kingdom of Saudi Arabia in particular and at the level of the Arab world in general.

Why there is a problem?

Usually, the methods of education in the Applied Cryptography course differ from one trainer to another, and this distracts the focus of male and female students in understanding this important course in the specialty of cybersecurity in particular and in other disciplines in general, so we as a group will strive to unify trainers to take information from our platform, which we will enter accurate and value-added information to it, and we will facilitate the method of education so that the target audience for this platform is the entire community, whether they are young or old This platform will not be limited to a specific category.

How you are going to address the problem?

We will seek as a group to provide globally approved sources that deal with cryptography in one platform, this platform will support Arabic and English languages, and also we will facilitate the understanding of Applied Cryptography, and we will start at the beginning of our project by adding 5 ciphers through which the user can encrypt plaintexts and also can decrypt ciphertext, and then we will add a lot of codes through continuous updates on the platform.

Expected result and its significance :

We expect this project to be pioneering in the future, as we believe that it will contribute very significantly to the development of cryptography and will serve as a social service for students and everyone who wants to learn how to encrypt and decrypt using many Ciphers, whether old or new.

PROJECT IMPACT

WHAT IS THE IMPACT OF YOUR PROJECT ON SOCIETY OR ENVIRONMENT

Impacted persons of project:

Encryption Teachers

Students

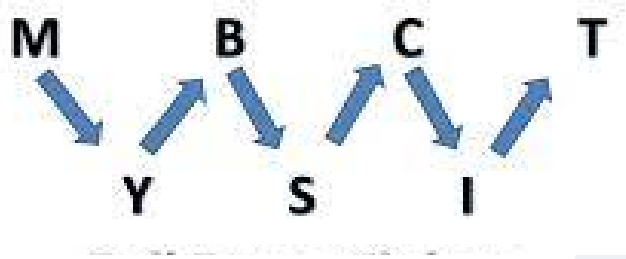
People of different abilities

Non-native Arabic and English speakers

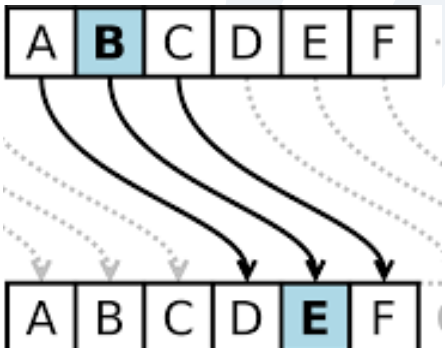
PROJECT SCOPE

Describe what work is in scope for your project and what is out of its boundaries

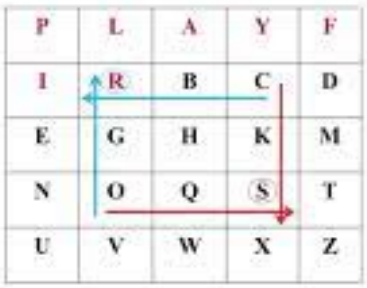
With this site we will cover the following ciphers:



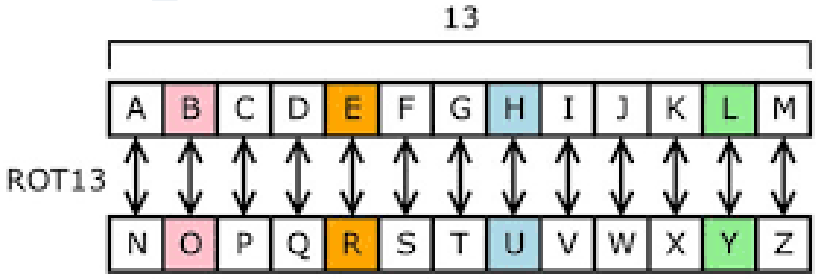
RAIL FENCE CIPHER [3,4]



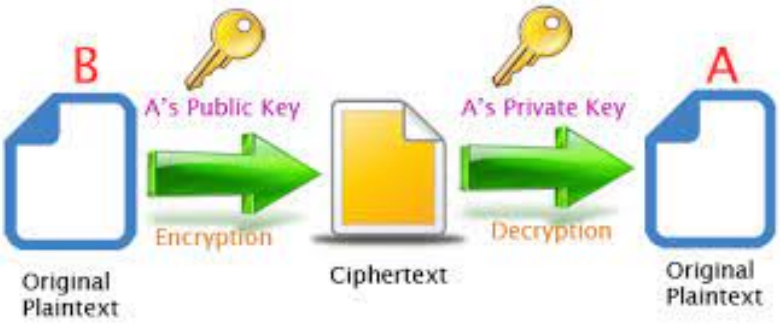
CAESAR CIPHER [1,2]



PLAYFAIR CIPHER [7,8]



MONO-ALPHABETIC CIPHER [5,6]



AES ALGORITHM [11,12]

RSA ALGORITHM [9,10]

Things that are outside the limits of the project:

1. Hashing algorithms will not be discussed.
2. Video training sessions but may be a futuristic idea.
3. Support languages other than Arabic and English.

AIMS AND OBJECTIVES

- Overall goal
- High level description
- A concise and precise objectives

The overall goal of the project:

The community, led by male and female students and teachers, gained basic concepts in cryptography in the easiest and most enjoyable way possible.

The goals and objectives of the Encryption Key platform are:

1. Draw a clear and easy way to encrypt and decrypt many ciphers.
2. Provide a clear curriculum for many ciphers.
3. Contribute to the dissemination of cryptography among the general public of society and make it a science of great importance.
4. Collect educational content for many ciphers on one site.
5. The strategic goal of the platform is for there to be free digital training courses on the platform.
6. Learning applied cryptography is a difficult and complex topic, but our site makes this task easy for you. Here you'll find different learning methods, including video lessons and practical examples that help you understand the basics quickly and easily.
7. We aspire to make our platform a destination for many users, whether they are trainees or teachers.
8. Provide all the necessary tools to encrypt and decrypt most of the encryption algorithms.
9. This platform aims to provide comprehensive and detailed educational resources on encryption algorithms. Here you will find interactive lessons and practical exercises that will help you understand the basics of cryptography and improve your encryption comprehension skills.
10. Whether you are a beginner in cryptography or have previous experience, this platform will help you gain the skills you need to develop yourself and join the modern technology industry.

EXISTING SOLUTIONS AND THEIR LIMITATIONS

What are other existing solutions :

PLANETCALC

A site with a lot of calculators for everything and from the calculators on this site (Playfair cipher) that are very important for cybersecurity professionals and learners in the field of cryptography.

Click Here for visit it

MYMATHTABLES

A site with a lot of calculators for everything and from the calculators on this site (Cryptography Caesar Cipher Converter) that are very important for cybersecurity professionals and crypto learners.

Click Here for visit it

how did they solve the problem; and their limitations:

1. Their sites do not support the Arabic language.
2. Their sites are general for all calculators while ours is for ciphers.
3. There are no details of the encryption and decryption processes at other sites.
4. There is a great difficulty when dealing with other sites because they do not care completely about the user experience (UX).
5. On other sites, there is no training curriculum for each cipher, as on our site, because it is not intended for encryption and decryption, but rather general for all sciences.
6. Other sites are full of annoying ads

EXISTING SOLUTIONS AND THEIR LIMITATIONS

Clarify how we will address or solve the problems? (Generally):

We will solve these problems by making our site support Arabic and English and support people with different abilities and non-native speakers of Arabic and English through symbols, and we will make our platform directed to users who wish to develop their capabilities in the specialty of cryptography, and we will take care of the smallest details about user experience (UX), we will provide specialized curricula In encryption, our site is completely free and ad-free.

Suggested solution to address the issue:

Applied cryptography is one of the most important skills that individuals must acquire in this digital age, as it facilitates many things for them and saves time and effort.

However, many have difficulty learning this science, whether because of the lack of available lessons or the difficulty of understanding concepts. Therefore, we offer a proposed solution to teach the community applied cryptography through a website.

The site includes educational content covering all levels, from beginners to professionals. The content includes illustrated lessons and a detailed explanation of the concepts and tools needed to advance in understanding applied cryptography.

The content is characterized by an easy and clear style that makes it easier for individuals to understand and apply concepts correctly.

With this proposed solution, the community can learn applied cryptography in an easy, organized, anytime, anywhere, helping them improve their skills and achieve their goals in this scientific field.

We hope that this solution will be beneficial to society and contribute to the development of the digital and technical skills of individuals and educational institutions.

REFERENCES

1- GOYAL, K., & KINGER, S. (2013). MODIFIED CAESAR CIPHER FOR BETTER SECURITY ENHANCEMENT. INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS, 73(3), 0975-8887.

2- MISHRA, A. (2013). ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT METHODS. INTERNATIONAL JOURNAL OF RESEARCH IN ENGINEERING AND TECHNOLOGY, 2(09), 327-332.

3- SIAHAAN, A. P. U. (2017). RAIL-FENCE-CRYPTOGRAPHY-IN-SECURING-INFORMATION.

4- GODARA, S., KUNDU, S., & KALER, R. (2018). AN IMPROVED ALGORITHMIC IMPLEMENTATION OF RAIL FENCE CIPHER. INTERNATIONAL JOURNAL OF FUTURE GENERATION COMMUNICATION AND NETWORKING, 11(2), 23-31.

5- AUNG, T. M., NAING, H. H., & HLA, N. N. (2019). A COMPLEX TRANSFORMATION OF MONOALPHABETIC CIPHER TO POLYALPHABETIC CIPHER:(VIGENÈRE-AFFINE CIPHER). INTERNATIONAL JOURNAL OF MACHINE LEARNING AND COMPUTING, 9(3), 296-303.

6-OMRAN, S. S., AL-KHALID, A. S., & AL-SAADY, D. M. (2010, DECEMBER). USING GENETIC ALGORITHM TO BREAK A MONO-ALPHABETIC SUBSTITUTION CIPHER. IN 2010 IEEE CONFERENCE ON OPEN SYSTEMS (ICOS 2010) (PP. 63-67). IEEE.

7- RAHIM, R., & IKHWAN, A. (2016). CRYPTOGRAPHY TECHNIQUE WITH MODULAR MULTIPLICATION BLOCK CIPHER AND PLAYFAIR CIPHER. INT. J. SCI. RES. SCI. TECHNOL, 2(6), 71-78.

8- SRIVASTAVA, S. S., & GUPTA, N. (2011). A NOVEL APPROACH TO SECURITY USING EXTENDED PLAYFAIR CIPHER. INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS, 20(6), 0975-8887.

REFERENCES

9- MILANOV, E. (2009). THE RSA ALGORITHM. RSA LABORATORIES, 1-11.

10- KALPANA, P., & SINGARAJU, S. (2012). DATA SECURITY IN CLOUD COMPUTING USING RSA ALGORITHM. INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER AND COMMUNICATION TECHNOLOGY, IJRCCT, ISSN, 2278-5841.

11- ABDULLAH, A. M. (2017). ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM TO ENCRYPT AND DECRYPT DATA. CRYPTOGRAPHY AND NETWORK SECURITY, 16, 1-11.

12 - KUMAR, P., & RANA, S. B. (2016). DEVELOPMENT OF MODIFIED AES ALGORITHM FOR DATA SECURITY. OPTIK, 127(4), 2341-2345.