CryptoCal: A tool to Understand and Implement Cryptographic Algorithms

1st, Vinita Vikram Bhandiwad
Phd Research Scholar
Department of Electronics and Telecommunication Engineering
Terna Engineering College, University of Mumbai
Vidyalankar Institute of Technology, Wadala
vinita.bhandiwad@gmail.com

2nd, Lakshmappa K Ragha
PhD Research Supervisor
Department of Electronics and Telecommunication Engineering
Terna Engineering College, University of Mumbai
lkragha@ternaengg.ac.in

***Abstract*—In today's digital age, safeguarding data holds paramount importance, as it encompasses a wide range of stored digital information. Ensuring the security of these assets is imperative, and data security mechanisms are employed to thwart unauthorized access to personal databases, computers, and websites. This research paper introduces " CryptoCal: A tool to Understand and Implement Cryptographic Algorithms" an integrated platform poised to revolutionize the landscape of cryptography. Serving as a comprehensive hub, CryptoCal offers a singular destination for cryptography enthusiasts, practitioners, and researchers. The platform amalgamates a repository of diverse cryptography algorithms**

Keywords— Data Encryption, Compression, Cryptography, Information Security, AES Encryption, Confidentiality, Integrity, Authentication

1. INTRODUCTION

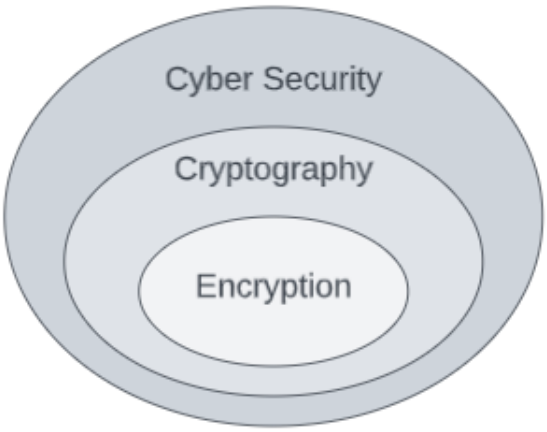
This project aims to create a space where anyone who wants to acquire knowledge about various cryptographic techniques can do so. In a world where everything is available online, there is a lot of data flow happening over the internet. To protect this data, Cyber security has come into picture.

Cyber security is a practice of securing data, data which is confidential and prone to data breach can lead to long-term consequences. With the increase in technology, any third party can gain unauthorized access over the shared network. Thus, the importance of cybersecurity grows, requiring a proactive and adaptive approach to stay ahead of evolving threats. One of the key pillars of Cyber security that encompasses the use of techniques like Encryption is Cryptography.

Cryptography is a foundational component of cybersecurity. It provides the techniques and tools used to secure data and communication within the broader field of cybersecurity. It involves designing and analyzing algorithms for encrypting and decrypting data to protect it from unauthorized access or modification. Cryptography provides the mathematical techniques used in encryption to secure data.

Encryption is a specific application of cryptography. It involves the process of converting plaintext (readable data) into ciphertext (encoded data) using an encryption algorithm and an encryption key. The goal of encryption is to ensure that even if unauthorized individuals gain access to the ciphertext, they cannot decipher it without the appropriate decryption key. Thus, Encryption is a specific application of cryptographic techniques to protect data, which is an integral part of both cryptography and the larger field of cybersecurity.

Below Figure(i) shows how Cyber security, cryptography and encryption are related and work hand in hand.



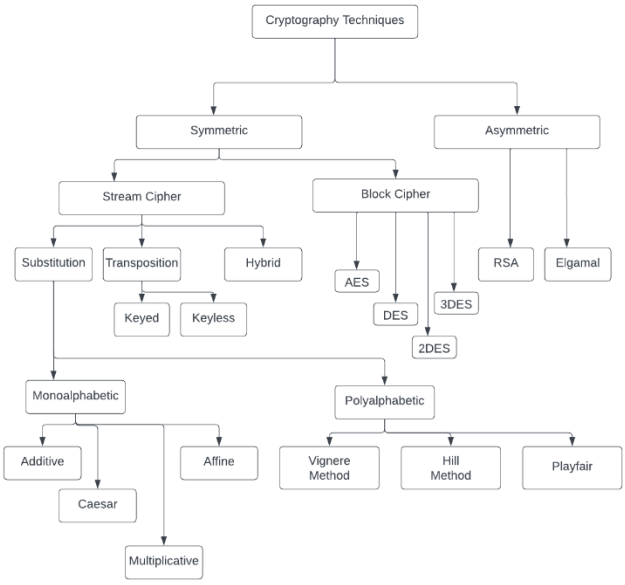
Figure(i)

Encryption can be done using various cryptography algorithms. Cryptography is classified into two types- (i) Symmetric Cryptography (It uses single key for encryption and decryption process) (ii) Asymmetric Cryptography (It uses pair of keys- Public and Private key for encryption and decryption respectively)

Symmetric Cryptography is further divided into two types- (i) Stream Cipher (Encrypt data one bit at a time or in small units) (ii) Block Cipher (Encrypt data in fixed-size blocks). Stream cipher technique is further divided into three types- (i) Substitution (ii) Transposition and (iii) Hybrid. Substitution stream cipher is further divided into two types- (i) Monoalphabetic (Uses single bit key) (ii) Polyalphabetic (Uses multiple bit key) while Transposition stream cipher has two types- (i) Keyed (ii) Keyless. Figure(ii) shows the brief classification of cryptography techniques.

Students who wish to learn these techniques can have a hands-on experience on our website. The website even provides additional services like Mod Calculator, Euclidean Inverse Calculator, blogs and trending videos related to cyber security as a whole.

A review of various existing methodologies and their limitations has been presented in section 3. In Section 4, we provide the real time applications of the proposed system, how our system works, what services we provide. In section 5 we present conclusions and the scope of future work.



Figure(ii)

2. EXISTING METHODOLOGIES

SEED Labs:

- SEED Labs offers a set of lab exercises that allow students to experiment with cryptographic algorithms, protocols, and techniques in a controlled environment. The cryptography labs typically cover a range of topics, such as encryption, digital signatures, key exchange, and cryptographic attacks.
- SEED Labs often present scenarios that reflect real-world security challenges. Students can explore how cryptography is used to secure communication, authenticate users, and protect sensitive data.
- Some labs also include simulations of cryptographic attacks, allowing students to understand vulnerabilities and weaknesses in cryptographic systems.
- The labs typically come with instructions and guidelines, helping students navigate through the exercises and learn step-by-step.
- Depending on the availability of physical resources (such as specific hardware for cryptographic experiments), SEED Labs have limitations in providing certain types of hands-on experiences.

vlabs:

- vlabs is offered by MoE of India which provides hands-on exercises, simulations, and interactive modules for learning about cryptographic concepts, algorithms, and applications.
- It is a virtual lab that deals with virtual experiments to understand the basic mathematical foundations of cryptography to gain insightful experience by working with fundamental cryptographic applications and to train in the art of design and analysis of information security protocols.
- It supports a calculator-like platform where students can gain hands-on experience while learning about cryptography algorithms and techniques.
- While it a great platform for students beginning to explore the world of cryptography, it does not provide tools for advanced cryptography.
- It also lacks the visual simulation and dynamic interaction that may limit the scope of learning and understanding.

Dcode:

- Dcode.fr is a popular online platform that offers a wide range of tools and resources related to cryptography, ciphers, and codebreaking. The website serves as an interactive hub for individuals interested in exploring and learning about various cryptographic techniques.
- Dcode.fr provides a collection of online tools that allow users to encrypt and decrypt messages using different types of ciphers and cryptographic algorithms. Users can input their own text and apply various encryption methods gaining hands-on experience.
- It also offers tools to help users identify unknown ciphers or encoding methods. Users can submit encrypted texts, and Dcode.fr attempts to identify the cipher type and provide a decrypted version of the message.
- The website includes educational resources wherein the users can access tutorials and explanations on topics such as frequency analysis, substitution ciphers, transposition ciphers, and more.
- While the website offers a variety of tools, the depth of documentation for certain tools or techniques are insufficient for users who require comprehensive understanding and implementation guidance.
- As cryptography evolves, new encryption techniques and methods are developed to address emerging security challenges which Dcode.fr might not cover limiting its relevance for users seeking up-to-date information.
- Its interactivity might not be as dynamic or engaging as dedicated cryptographic software or platforms, potentially limiting user engagement and exploration.

3. PROPOSED SYSTEM

The project contains an interactive GUI and includes most cyber security related materials hence making the proposed system a convenient and user-friendly website when itcomes to cryptography.
The proposed system gives the following features:

- Interactive GUI.
- Detailed information on Symmetric and asymmetric encryption algorithms.
- Blogs and News related to cyber security.
- Reference videos about cryptography techniques.
- Additional calculators for mod and Euclidean inverse.

The below Figure(iii) is the block diagram of our system, it has detailed overview of how our system works and the services we are providing to the user.

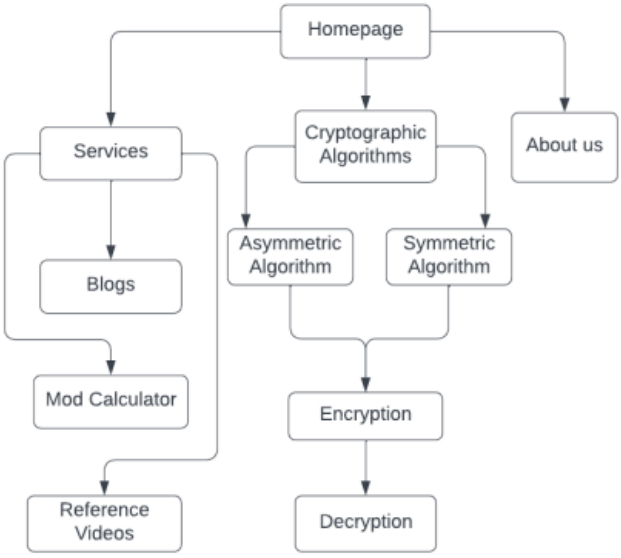
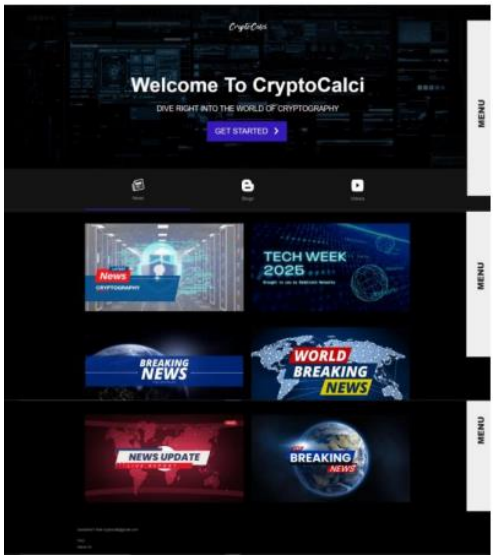


Figure (iii)

A. Landing Page

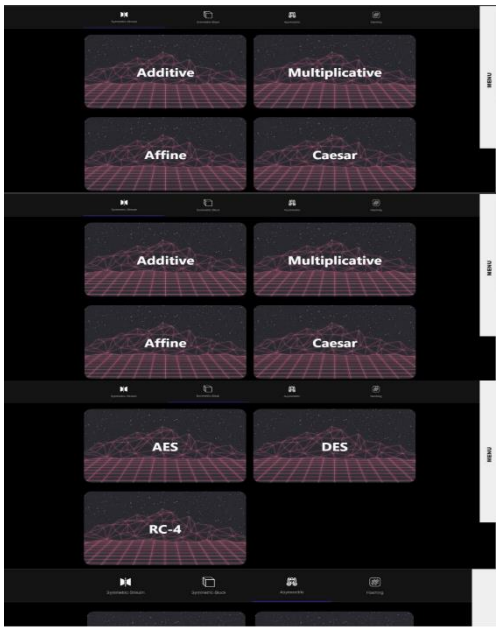
Below figure(iv) shows the landing page of our system, where user can get latest information on cryptography and cyber security through recent blogs and news over the internet and reference videos from YouTube.



Figure(iv)

B. Home Page

In the home page we have all the symmetric, asymmetric algorithms. It provides information about the algorithm and hands-on experience for encryption and decryption.

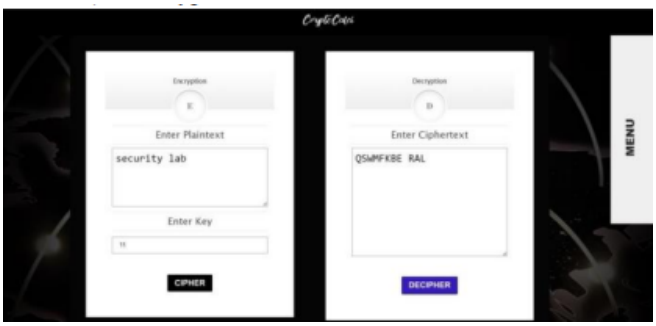


Figure(v)

C. Encryption Algorithms

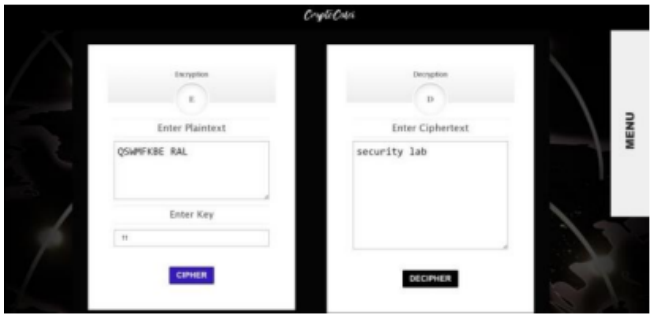
i. Multiplicative

- Encryption



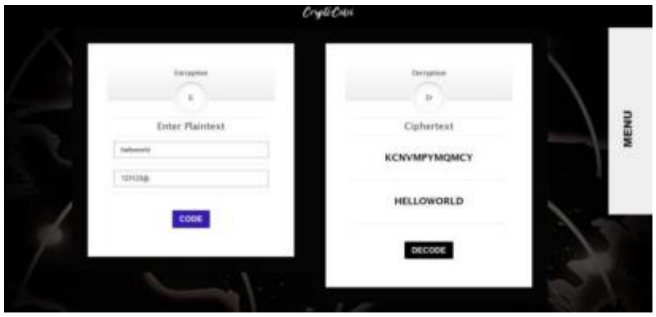
Figure(vi)

b) Decryption Figure



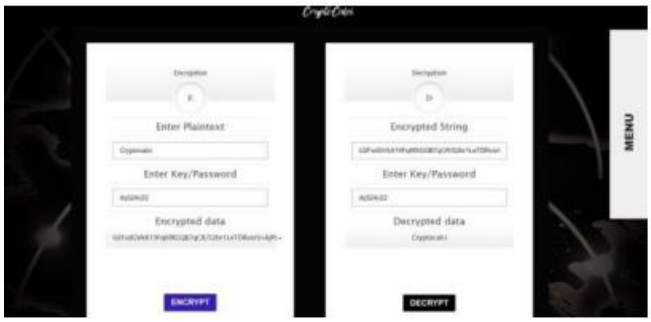
Figure(vii)

(ii) Playfair



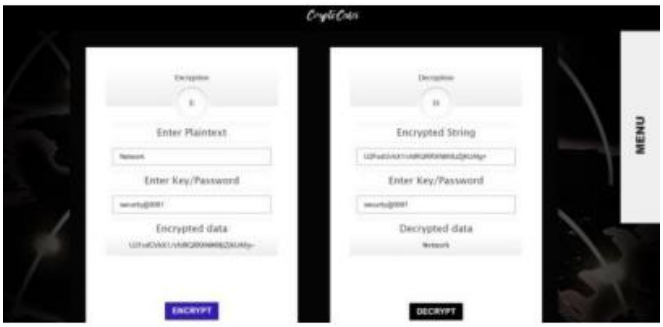
Figure(viii)

(iii) AES



Figure(ix)

(iv) RC4



D. Services

The additional services available on the website is: a) Mod Calculator. b) Euclidean Inverse (Mod Inverse) Calculator. Figure(xi) & (xii) shows the same

FIGURE(XI)

Figure(xii)

4. CONCLUSION AND FUTURE WORK

The platform's ability to house a diverse collection of cryptographic algorithms, ranging from classical to modern, underscores its commitment to serving as a one-stop hub for cryptographic knowledge. This enables users to access a wide spectrum of encryption and decryption, fostering a deeper understanding of the intricacies and nuances within cryptography.
Additionally, we plan to implement these features in future:

a) Addition of more cryptography algorithms like Hashing.
b) Providing security services for third parties.
c) Introducing database and securely storing user's data for their future use.
d) Introduction of additional services like Matrix Calculator.
e) Using Web Scraping to give users dynamic and latest knowledge on cyber security.
f) Introduce PDF Generation option for each algorithm, users can download the PDF and understand how the algorithm worked for their plain text or encrypted text.

REFERENCES

[1] Diffie, W., & Hellman, M. (1976). "New Directions in Cryptography." IEEE Transactions on Information Theory, 22(6), 644-654.

[2] Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key

[3] Cryptosystems." Communications of the ACM, 21(2), 120-126.

[4] Goldwasser, S., Micali, S., & Rackoff, C. (1985). "The Knowledge Complexity of Interactive Proof-Systems." SIAM Journal on Computing, 18(1), 186-208.

[5] Boneh, D., & Franklin, M. (2001). "Identity-Based Encryption from the Weil Pairing." SIAM Journal on Computing, 32(3), 586-615.

[6] Bellare, M., Rogaway, P., & Wagner, D. (1993). "Confoundingly Weak Notions of Security for Public-Key Encryption." In Advances in Cryptology – CRYPTO '93 (pp. 394-413).

[7] Paillier, P. (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes." In Advances in Cryptology – EUROCRYPT '99 (pp. 223-238).

[8] Bellare, M., Desai, A., Jokipii, E., & Rogaway, P. (1997). "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation." In Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS '97) (pp. 394-403).

[9] Boneh, D., & Shoup, V. (2000). "A Graduate Course in Applied Cryptography." Available online: https://crypto.stanford.edu/~dabo/cryptobook/

[10] Koblitz, N. (1987). "Elliptic curve cryptosystems." Mathematics of Computation, 48(177), 203-209.

[11] Miller, V. S. (1986). "Use of elliptic curves in cryptography." Advances in Cryptology — CRYPTO '85 (pp. 417-426).

[12] Peikert, C., & Waters, B. (2013). "Lossy trapdoor functions and their applications." Advances in Cryptology — EUROCRYPT '08 (pp. 455-475).

[13] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). "Post-Quantum Key Exchange — A New Hope." Advances in Cryptology — EUROCRYPT '16 (pp. 166-195).