INDIAN REGIONAL LANGUAGES ENCRYPTER

Mr Prajwal Balasaheb Yadav
Student,
Walchand College of Engineering, Sangli,Maharashtra,India.
prajwal.yadav@walchandsangli.ac.in

Mrs A.M.Chimanna(Umrani)
Asst.Professor
Walchand College of Engineering,
Sangli,Maharashtra,India.
amruta.umrani@walchandsangli.ac.in

Ms Smital Rajendra Patil
Student,
Walchand College of Engineering,
Sangli,Maharashtra,India.
smital.patil@walchandsangli.ac.in

Mr Yash Dilip Kalam
Student,
Walchand College of Engineering Sangli,Maharashtra,India.
yash.kalam@walchandsangli.ac.in

Mr Udaykumar Sanjay Gadikar
Student,
Walchand College of Engineering.
Sangli,Maharashtra,Indiaudaykumar.gad
ikar@walchandsangli.ac.in

***Abstract*— The rapid growth of the internet in recent days and the widespread availability of networks have led to the development of various creative applications. Almost all software applications are becoming online. But the increasing use of the internet has raised security concerns for private and confidential data. As technology has involved a lot, it has also led to malpractices like stealing personal or organizational private information. To avoid this, the information must be stored and transferred safely. To maintain the privacy of data, data can be stored in encrypted form.**

Today Indian government is shifting towards digitalization. This means every work that used to be done using traditional pen-paper mode is done using smart technologies and the internet. As government data is very confidential, it is necessary to protect that data from intruders. But in India, every single piece of paper from small scale to advanced documentary such as Aadhar card or PAN card information, Household Bills to Income tax returns, Property Documents, and also various GRs of government is written in regional languages. But there are no data encryption tools to encrypt regional languages to keep data safe. So, to overcome this problem and provide more security to Government confidential data, we have come up with an idea to develop an algorithm that will encrypt Regional Languages.

Keywords—Digitalization, Regional Language,Encrypter

I. INTRODUCTION

There is a need of developing encryption algorithm for Indian regional languages along with English. While researching an encryption algorithm for the Marathi language we came across an existing algorithm to encrypt the Devnagari language, but it is similar to Ceaser Cipher algorithm and provides very less security. Simple guessing or cryptanalysis attack can easily compromise confidential data encrypted using that algorithm. So, we realized that traditional symmetric key algorithms are not secure, and using those can cause security threats for important data. So, used the AES encryption algorithm for regional language. It can't be used directly for encryption of languages other than English due to differences in ASCII values of English characters and characters of regional languages. So, making necessary changes, developed a generalized encryption algorithm which can encrypt multiple regional languages like English, Hindi, Marathi, Kannada, Tamil, Telugu, Gujrati, and more. There has been a great increase in the usage of the internet in the past few years. With the increase in internet consumption, security threats are also arising. The confidentiality and security of personal data have been taken into consideration and many cryptographic algorithms are developed to secure data. Most of the algorithms are built considering the English language only. But, in countries like India which have many languages and some of which are being used for official government work, there's a need to secure regional languages also. Existing cryptographic encryption algorithms that are widely used for encrypting English language data do not work well for regional languages. So, developing a new encryption algorithm for regional languages or changing existing algorithms in order to work well for languages other than English is necessary. So, we come up with the idea to develop a Cryptographic Encryption Algorithm for Indian Regional Languages. The primary goal is to keep CIA triads intact while protecting the secrecy of government information. Government officials must send sensitive material via mail, but there is no assurance that it will be secure. Consequently, developing an encryption method is necessary to assure security. In this project, we have implemented a cryptographic algorithm that encrypts Indian regional languages as well as English. If someone has to encrypt data in any regional language or communicate sensitive information in encrypted form, this encryption algorithm can be helpful. Additionally, this program includes a Chrome extension to initiate encryption and decryption whenever necessary.

II Literature Survey

There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for security experts. Cryptography is the best technique to nullify this threat.

MULET: A Multilanguage Encryption Technique

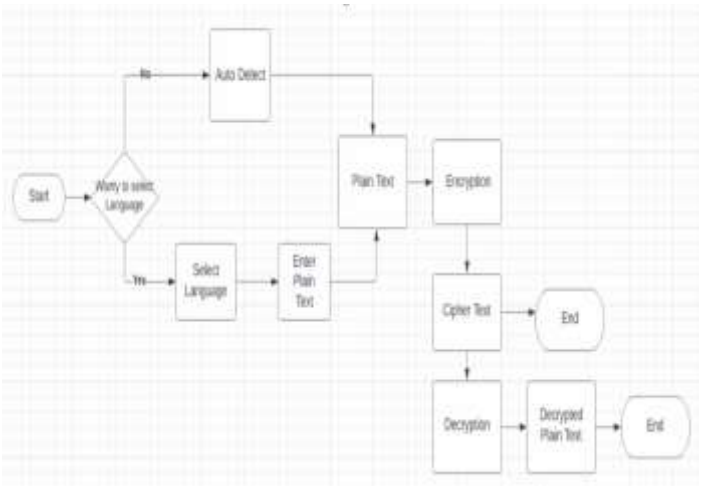
In this MULET technique, Hindi characters are encrypted using a simple algorithm. A wide variety of techniques have been employed for encryption and decryption, but the use of a

multilingual approach for the same is not prevalent. Motivated by this, here, they proposed a novel algorithm that focuses on the encryption of plain text over a range of languages supported by Unicode. The text to be encrypted is read character by character and the Unicode value of each is obtained. This value is then divided by the mapping constant. The remainder and quotient are calculated. The remainder obtains the encrypted character and the quotient has the key for the decryption of the corresponding character. The MULET algorithm uses a very simple and direct mapping technique. As it encrypts only by mapping plain text with some key to produce cipher text, it is not very secure and can compromise important data.

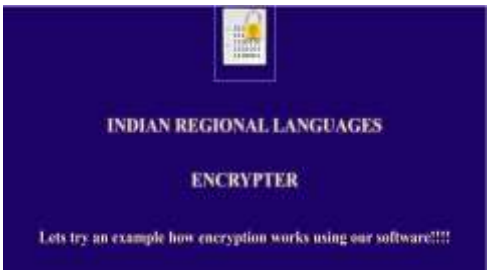
III Methodology

The application is regarding asymmetric cryptography encryption which use symmetric key for encryption and decryption process. So depending on our algorithm requires any kind of plain text along with symmetric key ,the novelty of application is the text may in any kind of language the algorithm is not specific to english language For regional languages, Unicode values are defined. While encrypting, plain text is taken character by character and taken its Unicode value .to achieve novelty character entered may have ASCII value in any range of values it can be more than 1000 in number and the arandard AES algorithm supports an ASCII of range for 0-256 which means maximum of 8 bit character can be stored as a character ,therefore this ASCII is firstly converted into 8 bits (range 0-255) using any kind of hash function which can be de-hashed ,this hash value is given to the AES encryption and it converts this hash value into cipher text.T he key is taken and the plain text is encrypted using the AES Encryption algorithm. The algorithm is modified to work well with hashed values. The encrypted text will be in the form of hex values.The same key is used for decryption, the cipher text is passed for decryption, and decryption is performed where we get the hashed value and it is the unhashed to get the plaintext again to get the original plain text.After that, developed UI and then integrated encryption and decryption methods with it.Added functionality to automatically send a mail with cipher text to a specified email id from the application itself .

1. For regional languages, Unicode values are defined. While encrypting, plain text is taken character by character and taken its Unicode value. The Unicode value of each character is hashed and converted in a specific range.
2. Then the key is taken and the plain text is encrypted using the AES Encryption algorithm. The algorithm is modified in order to work well with hashed values. The encrypted text will be in the form of hex values.
3. For decryption also, the same key is used, the cipher text is passed for decryption, and decryption is performed to get the original plain text.
4. After that, developed UI and then integrated encryption and decryption methods with it.
5. Added functionality to automatically send a mail with cipher text to specified email id from the application itself.



1. For regional languages, Unicode values are defined. While encrypting, plain text from entered text or from selected file is taken character by character and taken its Unicode value. But these Unicode values of languages other than English cannot be directly used in AES Encryption Function. As required Unicode range for AES to work well is 0 to 255. But Unicode values of regional languages say Marathi is between 2304 to 2431. So, the Unicode value of each character in regional text is hashed and converted in a specific range i.e., 0 to 255.
2. Then the key is taken and the plain text is encrypted using the AES Encryption algorithm. The algorithm is modified in order to work well with hashed values. For hash values, AES will work well as the values will be in the range of 0 to 255 The encrypted text will be in the form of hex values. That hex text is given as output.
3. For decryption also, the same key is used, the cipher text is passed for decryption, and decryption is performed to get the original plain text. This decrypted text will be having Unicode values in the range of 0 to 255. To get the original text, reverse hashing is done. Then the original text in the same language is given as output.
4. Apart from simple encryption and decryption, as important files need to be sent over mail, added functionality to send an encrypted text to entered mail id directly via the application. So that privacy can be achieved while transferring confidential information via mail.



Encryption

Decryption

Encryption File

Sent encrypted text via mail—application and mail both screenshots

In this work, we deal with the concepts of security of digital data communication across the network. This project is designed by using the AES algorithm for better performance and security. We performed a new cryptography method by modifying AES. The method proposed has proved successful for encrypting and decrypting inputted text or text file. And also provided an email sending facility.

Conclusion:

Data encryption is a crucial technique for safeguarding government data because it encodes confidential material into an encrypted message that can only be decoded by authenticated persons with the appropriate encryption key. These are a few ways that encryption process might improve government data.

Encryption can serve to safeguard sensitive information against unauthorized access, theft, and other types of cybercrime. This includes information about national security, public safety, financial activities, and personal data.

Encryption assists to the confidentiality of government data by preventing unauthorized parties from reading or accessing it. This is extremely critical for classified or sensitive material that should only be available to authorized persons.

Numerous laws and regulations compel government organizations to encrypt sensitive information. Government entities can assure compliance with these requirements by employing encryption techniques.

Encryption can aid in data breach prevention by making it far more difficult for thieves to access and take private information. Even if data is taken, encryption can help prevent unauthorized parties from reading or using it.

Government entities may show their dedication to securing sensitive data and retaining public confidence by installing strong encryption techniques. This can serve to boost confidence in government and enhance transparency.

In this research, we will examine at the integrity of digital data transfer through a network. For improved performance and security, the AES algorithm was used in the creation of this project. By altering AES, we created a new cryptographic approach. The proposed approach has shown to be effective for encrypting and decrypting inputted text or text files. In addition, an email sending function was given.

REFERENCES

[1] G. Praveen Kumar; Arjun Kumar Murmu; Biswas Parajuli; Prasenjit Choudhury, On certain “MULET: A Multilanguage Encryption Technique” , https://doi.org/10.1109/ITNG.2010.105

[2] Ross and J. Anderson, "Why Cryptosystems Fail" in Communications of the ACM, New York, USA, pp. 32-40, 1994.

[3] Francois-Xavier Standaert, Gilles Piret and Jean-Jacques Oui squater, "Cryptanalysis of Block Ciphers: A Survey" in , UCL Crypto Group, 2003..

[4] R. L. Rivest, "The RC5 encryption algorithm", *Proceedings of the 1994 Leuven Workshop on Fast Software Encryption*, pp. 86-96, 1995.

[5] "Elliptic Curve Cryptography" in , Certicom Research, 2000.

[6] William C. Barker, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" in , National Institute of Standards and Technology, NIST Special Publication 800–67, 2008.