PrasathSrinivasan Sushmitha Algorithm for String Encryption and Decryption

Dr. J.S.Prasath, Ms. Sushmitha G S
Department of Computer Science and Engineering,
Sapthagiri NPS University, Bengaluru, India
jsprasath@gmail.com, sushmithags884@gmail.com

Abstract

Security is essential for communication of messages, data, and private information. Security threats and vulnerabilities increases rapidly due to the wide usage of wireless medium for data transmission. The sensitive data and private information transmitted across internet can be accessed and altered by the intruders. The security algorithms are important to ensure the communication of messages without unauthorized access and modification as well as to achieve data security. This proposed work is the development of novel cryptography suitable for encryption of text messages. This proposed algorithm encrypts the input string into ciphertext through series of mathematical operations. The inverse operation of encryption is performed at the receiver to obtain the original string from the ciphertext. This proposed cryptography can be utilized for preventing the theft and fraud in online money transactions, securing the email messages, file encryption, securing the web information, ensuring data confidentiality across internet, assuring data security in remote access, securing the patients information transmitted across wireless networks, enabling secure communication of country's border information, preventing the credit card fraud, securing the industrial continuous varying process parameters, encryption of whatsapp messages, and securing the individual's private information.

Keywords: Cryptography, Encryption, Decryption, Security, String

1. Introduction

Cryptography is closely related to cryptology and cryptanalysis. Cryptology is the concept which involves both cryptography and cryptanalysis. Cryptology includes a wider extent than cryptography. In addition, it includes examining the numerical structures, computations, and conjectural cryptographic proportion. Cryptology reads the input plain text and converts it into equivalent ciphertext as well as it reads the ciphertext and converts it into plain text. Cryptology is the process of encryption and decryption of data. It performs analysis and breaking of existing encryption algorithms. The expansion of a cryptographic id-mechanism based on Compact Knapsack problem is presented [1]. This scheme ensures security against active attacks. Cryptology is widely used in our daily applications including financial transactions, medical services, legal operations, and electronic banking systems in order to maintain the data secret and protect the private information from various attacks. It is used in ATM (Automated Teller Machine) where the customers can deposit or withdrawal the money using the personal identity number (PIN). The ciphertext of PIN is stored in the database maintained by the bank and in the credit and debit cards. This type of storing the PIN details of customers is called one-way cryptography. The ciphertext can be generated using customer's PIN and bank's key. Mathematically, it is not possible to recover the plaintext of PIN from the ciphertext even though the key is known. The encryption algorithm should be as simple as possible, perform less computations, and to consume less power. A low-energy data encryption algorithm is proposed which is based on the Advanced Encryption Standard (AES) for enhancing security in data communication and consuming less in performing encryption [2]. This data encryption algorithm enhances the performance of Internet of Things (IoT) devices. The Assessment of Elliptic Curve Cryptography (ECC) methods are done for ensuring security and data privacy in IoT-based devices [3]. The variety of security threats and concerns should be taken into consideration. The optimal secure defense mechanism for Distributed Denial of Service (DDoS) attacks in IoT network utilizing feature optimization and intrusion detection system [4]. An improved

quantum query optimization algorithm is used for choosing the feature that selects optimal best among many features which decreases the data dimensionality problems.

Figure 1 shows the components of cryptology. Cryptology involves different ways of converting the input plaintext into unreadable ciphertext and different ways of breaking the ciphertext and to identify the plaintext. Cryptology deals with secure communication of messages and data storage with confidential.

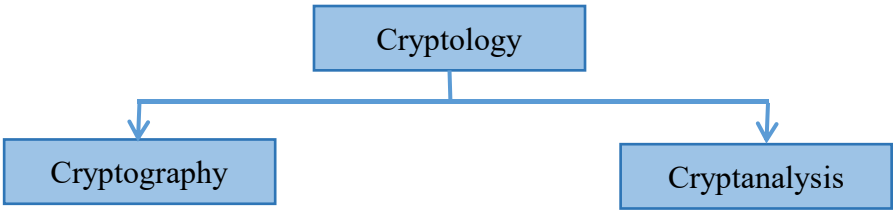

Figure 1 Components of Cryptology

Cryptography is a method of protecting the messages and communications so that only authorized parties can access the confidential information transmitted across internet. Now-a-days, cryptography methods are likely be unalterable, confirming the data security. It is essential to secure and protect the information transmitted across the medium from various attacks than developing the strong cryptography techniques. The conventional cryptographic methods are less efficient and it is easy for attackers to hack the messages and alter the data. Modern cryptographic algorithms involves complex mathematical computations and the intruders need more number of years and decades to identify the exact data, information or even a single message. Researchers are still working towards developing the efficient, optimized, and strong encryption algorithms since the variety of attacks increases. The preferable security properties and existing attacks against the Industrial IoT is addressed [5]. The traditional cryptographic tools used to secure the recent development in Industrial IoT networks are discussed. The segregation of various security mechanisms including symmetric encryption, asymmetric encryption for signature and access control is done [6]. It gives the amenities of data security and information gathered by Wireless Sensor Networks. An optimized hybrid encryption algorithm is proposed which integrates Elliptic Curve Cryptography with Advanced Encryption Standard [7]. It strengthens the data security and efficiency and it is used for smart home healthcare systems. The investigation of quantum communication and cryptography is done which aims to create strong encryption techniques acts against attacks from quantum computers [8]. The quantum technology in different applications including quantum machine learning, and quantum block chain are explored. The trends in lightweight cryptography and various encryption algorithms are compared using real-time data [9]. The key parameters taken for consideration are encryption time, memory utilization, and CPU utilization. The two Dynamic Searchable Symmetric Encryption algorithm is proposed to attain forward and Type-1 backward security while maintaining strength when incoherent queries are issued [10]. This work reduces the information leakage of encryption. The various cryptographic algorithms such as elliptic curve, hybrid, lightweight, and novel techniques are evaluated [11]. The Elliptic Curve Cryptography (ECC) is suitable for safe communication and it is the choice of lightweight cryptography for Internet of Things (IoT) devices. A secure and effective cloud-based data-sharing system is proposed [12]. The dual timestamp management scheme is introduced to manage the timestamp in each ciphertext to assist dynamic user groups. The framework is proposed to accomplish privacy-preserving statistical investigation on an encrypted database [13]. A cryptosystem based on binary vectors to accomplish complex logic expressions for statistical analysis on ciphertext. The ciphertext evaluation mechanism is designed which permits the edge to clean the encrypted value to be uploaded [14]. The public-key encryption algorithm is investigated to implement the secure data evaluation mechanism. The multi-key searchable encryption scheme is proposed which is efficient and secures data search algorithm that allows the owner to grant users to acquire data from the ciphertext [15]. This novel multi-key data search mechanism is strong against unauthorized queries. The updated version of the Menezes-Vanstone elliptic curve

cryptography scheme is proposed to perform text, image, audio, and video data security [16]. It is inferred that the ciphertext file size is smaller than alternative methods. The novel method is proposed for creating stochastic and undeterminable keys for symmetric One Time Pad cryptosystems [17]. The publicly available DNA sequences stored in genetic databases are used as a source. The Encryption stage of the cyber kill chain and its detection methods is discussed [18]. The system calls, I/O monitoring, and file system operations are performed using encryption-related activities. The characteristics of homomorphic transform are utilized to make it more suitable for text encryption [19]. The simple union and symmetric difference operators are used for converting plaintext to ciphertext. A novel cryptography has been formulated that utilizes both Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) further with clustering through standard LEACH protocol for enhancing energy efficiency, data security, and network lifetime [20]. It rectifies the problem in key exchange, simpler than ECC, and more reliable than AES.

Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it. Cryptography involves a set of procedure which contains mathematical calculations called algorithms. Figure 2 shows the input plaintext is converted into ciphertext which is called as encryption. The function of cryptography is to convert the input messages into unreadable text that are difficult for attackers to identify or to obtain the original information. These algorithms are utilized to maintain the private data secret, securing the web information, protecting the data and transactions on credit card and debit card.

Figure 2 Cryptography

The objectives of cryptographic algorithms are confidentiality, integrity, non-repudiation, and authentication. The raw data and the information is encrypted to produce the ciphertext. This ciphertext is unreadable and it assures confidentiality of information during transmission over internet. Cryptography is also exploited to assure data integrity in which the information cannot modified during communication. Cryptography provides non-repudiation in which the information generated by someone cannot deny at a later stage their intentions in the transmission of data. Non-repudiation is a sequential, judicial concept that proves the genuineness of information or data communication by providing indisputable proof of both authenticity and integrity. Cryptography is used to provide authentication of messages which involves identification and validation of information sender. Authentication is the procedure for identifying the individuals who creating and sending the information. Authentication mechanisms enable access control for devices by testing the user's information match the information given in the database of authorized parties or a data authentication server. Authentication guarantees that devices, operations and organization information are secret. User authentication is achieved through the validation of user ID and password. In addition, users need to authenticate through face recognition, thumb print or biometric signature. The security scheme is proposed that utilize the Improved Elliptic Key Cryptography to attain data encryption and decryption [21]. The source codes keep the private keys which preserve other keys in non-volatile memories and it prevents replay, Denial of Service and Sybil attacks. The optimized quantum network is proposed which integrates the Whale optimization algorithm with the feed-forward and back propagation algorithms [22]. The administrator keeps erogenous data on a server, and the document is encrypted using the encryption technique. An enhanced S-box based Advanced Encryption Standard is proposed along with Runge-Kutta Optimization scheme to attain the confidentiality and integrity of medical information [23]. The level of security is validated using non-linearity, Strict Avalanche Criterion, Differential Probability, Bit Independence Criterion, and Linear Probability parameters. The lightweight elliptic curve cryptographic algorithm for safeguarding resource-constrained devices such as IoT is proposed [24]. The elliptic curve cryptography strengthens the level of security as compared to RSA algorithm for the identical key size. A ground-breaking hybrid cryptographic scheme is proposed for securing the data storage of cloud computing [25]. This algorithm utilizes the variety of features include time-limited access control, adaptive key management, and dual security algorithms which are RSA and Advanced

Encryption Standard. An enhanced elliptical curve cryptography and chaotic mapping is proposed to achieve data transmission security [26]. Cryptography and steganography are united to improve the data security. The provable Fuzzy multi-keyword search mechanism is proposed along with the adaptive security [27]. It utilizes locality based hashing to hash the wrong words and correct keywords to the identical point. The effective privacy-preserving scheme for ciphertext traffic detection is proposed [28]. This mechanism utilizes lightweight cryptographic operations to attain both privacy and security. The broad range of cryptographic algorithms designed for protecting sensitive information in the cloud computing is proposed [29]. The research areas involved in the cryptographic scheme in cloud computing is addressed. The symmetric encryption is designed to protect the cloud server information, as well as to secure the transmission and reception of cloud server data [30]. A dual encryption algorithm is implemented to transmit data in a secure format.

Cryptography is classified into symmetric key, asymmetric key, and hash function. In symmetric key cryptography, the transmitter and the receiver utilizes the identical key for encryption and decryption of data or text messages. The symmetric key mechanisms are faster and it is not so complex to use, but the major challenge is secure transmission of key between transmitter and receiver. The commonly used symmetric key cryptography is Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms. Asymmetric key cryptography utilizes two keys for encryption and decryption of data and messages. The sender utilizes the public key to convert the input plaintext into unreadable ciphertext. The receiver utilizes the private key to convert the unreadable ciphertext into original plaintext. This asymmetric key encryption strengthens the security through the pair of keys. The commonly used asymmetric cryptography are RSA algorithm, Elliptic Curve Cryptography (ECC), and Secure Shell Protocol (SSH). The algorithm and computational complexity of asymmetric cryptography is higher than symmetric cryptography. Cryptography is also used to ensure the integrity of data. Data integrity is achieved through hash functions. Hash functions are a kind of cryptographic algorithm that creates finite length of hash value. Hash algorithm reads the set of input data and converts it into a specific hash value. Hash functions are more effective since the variation of one alphabet or blank space in the plaintext would generate a distinct value. Applications, websites, or receivers can test integrity of data by differentiating the obtained hash value with the standard hash, and they can validate that data has not been modified during communication. Hash functions are also widely used to guarantee user passwords without demand to generate an insecure client-side database of confidential passwords. The online banking system only gathers and stores the hash value of customer passwords. When the intruder tries to steal the bank customer's database, they should not able to retrieve any passwords from the hash value. The main purpose of cryptography is to protect the data, information, and messages during transmission across internet. The security between web browsers and web servers can be achieved through cryptographic protocols. The transmission of data between browser and website takes place through secure channel and the attackers cannot eavesdrop the information. Cryptography is also utilized to achieve security of email and whatsapp communication. It provides end to end encryption and keep the privacy of user's data secret. The importance and maintenance of data secrecy is addressed [31]. The various security algorithms are discussed and the parameters are compared. The opinion about cryptography, history of cryptography, and the modern cryptography is addressed [32]. The various computations involved in cryptographic algorithms are explored. The modern hardware security component is proposed for generation of cryptographic key generation [33]. The designed hardware module removes the deposited cryptographic keys and avoiding attacks against stored keys. The dynamic QR code payment system is presented to rectify the security issues [34]. The hardware section of the security component employs the algorithm flow and enhances the payment performance. The security schemes applied for internal usage in the Android Operating System is discussed [35]. This work investigates the security mechanisms and validates the cryptographic schemes in terms of energy efficiency derived from computation time. The forward search privacy scheme is proposed to strengthen the security [36]. It involves search operations over recently added documents do not leak any data about past queries. A flexible lightweight encryption algorithm is designed and implemented [37]. It performs simple substitution, and transposition process to encrypt and decrypt data that offers fewer computations within IoT devices. The modern lightweight cryptographic algorithm is proposed for improving data security on cloud computing [38]. This algorithm is based on 128-bit block cipher and 128-bit key size used for data encryption.

A smart residential load management scheme is designed by three-fold together with the provisioning of consumer security [39]. The computation of home load confirms to manage the load either to switch off the load or intimate extra usage of electricity. The privacy protection mechanism is proposed with the use of improved Honeypot algorithm [40]. It maintains and provides data security against intrusion or any other attack.

Cryptanalysis is the art and science of retrieving the plaintext from the ciphertext. It is the process of analyzing the weaknesses of cryptographic algorithms and the plaintext is identified using these weaknesses without the knowledge of secret key. Figure 3 shows the input ciphertext is converted into plaintext. It reads the ciphertext, analysis it and recovers the plaintext without using the key.

Figure 3 Cryptanalysis

Cryptanalysis is the process of analyzing and decoding ciphers, codes, and encrypted data without using the real key. Cryptanalyst tries to crack or break the encryption codes to identify the plaintext. The major job and responsibilities of cryptanalyst is to gather, process, and analyze the information in ciphertext, perform debugging of software codes, examine the deficiency of cryptographic algorithms, developing modern tools for cryptanalysis, and developing techniques for exploiting shortcomings in the computer networks. Cryptanalyst serves in various sectors including government, private organizations, legal and criminal cases, academic institutions, banking and finance, military, and medical fields. Cryptanalyst should have vast knowledge in advanced mathematical operations, encryption process, programming languages, and data structures. Public sectors utilize cryptanalysis to decode the encrypted information of other countries. Industries and enterprises use the cyber security goods and services to evaluate their security features. Usually, cyber-terrorists use cryptanalysis to root out cryptosystem vulnerabilities rather than a brute force attack. Hackers may be categorized into black-hat hackers and white-hat hackers. Black-hat hackers utilize cryptanalysis to involve in cybercrimes whereas the white-hat hackers use cryptanalysis to perform penetration testing to verify the strength of security. The research work is done in cyber security related to big data [41]. The big data tools and its protection for cyber security are addressed. The modified security algorithm together with the dedicated hardware key using embedded system is proposed [42]. This algorithm produces large key size of 1024-bit for asymmetric encryption and 256-bit key size for symmetric encryption. An identity-based encryption transformation scheme is proposed which combines two well-established encryption algorithms, namely identity-based encryption (IBE) and identity-based broadcast encryption [43]. A concrete identity-based encryption transformation is designed which is based on bilinear groups and verify its security against powerful attacks. A secure ciphertext duplication mechanism based on data popularity is proposed [44]. Ciphertext policy attribute-based encryption is applied to preserve the tags. The homomorphic encryption encapsulated difference expansion technique is proposed for reversible data hiding in ciphertext [45]. Key-switching and bootstrapping methods are presented to control the ciphertext expansion and decryption failure of homomorphic encryption. The security mechanism is implemented for monitoring of waste-water using embedded system and internet [46]. The value of dissolved oxygen and pH is encrypted using embedded system and sent through wireless medium. The experimental and the numerical approach of an optical key distribution quantum cryptography using BB84 protocol has been achieved [47]. The security of quantum cryptography is improved using one-time pad scheme and chaotic signal. The key generation algorithms of conventional cryptography and the need of strong security is discussed [48]. The different ways of attaining rigid security in public-key cryptography is addressed. The selection of identity-based asymmetric encryption is addressed [49]. This identity based cryptography offers end-to-end security of information across IoT-enabled industrial operations. The modern encryption scheme based on coupled map lattice is proposed for image security [50]. This encryption method utilizes randomly generated secret key, sub-keys based substitution, confusion algorithm to improve the security, sensitivity and robustness. The modern technique is incorporated

for securing the data storage [51]. In this scheme, biometric based statistical features are explored to create code word of a user.

Cryptanalytic Attacks

Cryptanalysis are categorized into three types which are analysis of ciphertext alone, analysis of known pairs of ciphertext/plaintext, and analysis of selected plaintext or selected ciphertext. Cryptanalytic attack is performed to identify the weakness of the cryptographic algorithms. This attack is based on the quality of the algorithms and the intelligence about the plaintext characteristics. The plaintext can be a string, group of strings, or it can be a code written using any programming languages. The knowledge about the plaintext is essential prior to attack testing. The various types of cryptanalytic attacks are shown in the figure 4. These are known plaintext attack, chosen plaintext attack, ciphertext only attack, man in the middle attack, and adaptive chosen plaintext attack. Besides these attacks, the other types of attacks are birthday attacks, side channel attacks, brute force attacks, dictionary attacks, hybrid attacks, reverse brute force attacks, credential stuffing, and differential cryptanalysis attacks.

Known-Plaintext Attack (KPA)

This type of attack is based on the known pairs of plaintext and ciphertext. Intruders map the plaintext with the ciphertext to identify the secret key. Intruders examine the correlation between the recognized plaintext and ciphertext to classify patterns or consistencies that might expose the key or the algorithm. Attackers can easily gather the known data and messages. Attackers can use frequency analysis to determine the most repeated characters or symbols in the ciphertext and match them to their corresponding plaintext

Chosen-Plaintext Attack (CPA)

This type of attack is based on selection of random plaintext and retrieves the related ciphertext and tries to determine the secret key. This attack is not so complicated as compared to known plaintext attacks but the failure rate is high.

Ciphertext-Only Attack (COA)

Attackers try to identify the secret key and the plaintext from the known ciphertext. The success rate of this attack is entirely depends on the cryptanalysis knowledge of the intruders. This type of attack is difficult to implement, more time consuming, and the attackers should utilize large number of combinations to determine the plaintext.

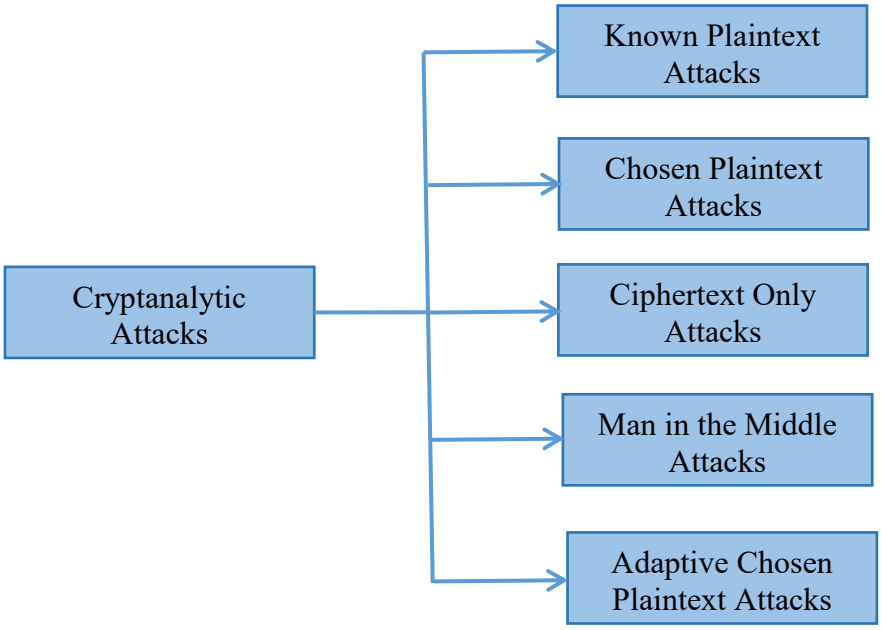

Figure 4 Types of Cryptanalytic Attacks

Man-In-The-Middle (MITM) attack

This type of attack allows intruders to listen the information on the communication between sender and receiver through a secured channel. The fake website may be created in the middle between the customer and the actual bank webpage. The various types of Man in the Middle attacks are eavesdropping the messages transmitted through Wi-Fi, hacking of electronic mail messages, spoofing of Internet Protocol (IP), Hyper Text Transfer Protocol Secure (HTTPS), Domain Name System (DNS), Address Resolution Protocol (ARP), and removal of Secure Socket Layer (SSL).

MITM attack is difficult to detect without utilizing the suitable mechanisms. Authentication and authorization is essential to determine the attacks. and it requires additional investigation. Organizations and enterprises should have standard procedure and preventive measures to nullify the MITM attacks. The MITM attack can be protected by encrypting the Wireless Access Point (WAP), authenticating the public key, ensuring the data security during communication, avoiding the usage of public Wi-Fi, utilization of Virtual Private Network (VPN), and ensuring network security through intrusion detection system.

Adaptive Chosen-Plaintext Attack (ACPA)

Attackers choose the plaintext and encrypts the plaintext multiple number of times. The plaintext is divided into smaller text and performs encryption to obtain the ciphertext. Based on the ciphertext, select another text for encryption and this process is repeated until all plaintext is converted into ciphertext.

In addition to these cryptanalytic attacks, there are other attacks generated by the intruders. These are birthday attacks, side channel attacks, brute force attacks, and differential cryptanalysis attacks.

Birthday Attack

This attack utilizes the probability of two or more individuals sharing the same birthday in a group of people. The birthday attack is a cryptographic attack based on the birthday paradox. This type of attack is used to identify the collisions in a hash function.

Side-Channel Attacks

This type of attack is enabled by leakage of information from a physical cryptosystem. Intruders gather information by analyzing indirect information, such as power consumption, electromagnetic leaks, or even sound, to reveal sensitive data like cryptographic keys or personal information. The various side-channel attacks are timing attacks, power analysis attacks, electromagnetic attacks, and others.

Brute-Force Attacks

Attackers utilize the trial and error method to identify the login details, password, and secret key. Intruders perform testing of passwords randomly until the exact password is determined. A brute force attack is very simple way of gathering the secret information and the success rate becomes high. This type of attack takes more time to guess the password, and it is complex as well as expensive in determining the longer key length. Hackers can easily identify the private information since many persons create weak passwords. Many users generate passwords without using combination of numerical value, special characters, upper case and lower case letters as they difficult to remember.

Brute-force attacks takes place in different ways. A simple brute force attack occurs when the hacker maintaining the list of usernames and tries to guess the passwords for different usernames. Attacker repeats this process until the exact combination of username and password is retrieved. Brute-force attacks are classified into dictionary attacks, hybrid attacks, reverse brute-force attacks, and credential stuffing.

Dictionary Attacks

Dictionary attack is a kind of brute-force attack where the intruder uses public and easily recognizable words plus phrases from a dictionary to guess passwords and personal identification numbers (PINs). It is frequent to see that user maintain less complexity in password combinations and easy to recall passwords. This helps intruders to handle the dictionary attacks easily as

identifying easier passwords does not consume time for skilled dictionary attackers. But dictionary attack efforts may lead to unsuccessful where individuals have a sophisticated set of passwords and not use mere alphabets or numbers as their passwords. The effects of dictionary attacks can be reduced by frequently changing the passwords, and utilizing two-factor authentication mechanisms. It can also be prevented by using strong passwords which includes random combination of lowercase and uppercase letters, numbers, and special characters.

Hybrid Attacks

It is a type of attack which integrates conventional brute force attacks with dictionary attacks. Attackers maintain the list of known words and try to match the combinations. This attack begins with dictionary words and then numbers, special characters, or change letter cases to those words are added. It also considers patterns such as appending or prepending numbers or symbols to dictionary words. Hybrid attacks are faster than brute-force attacks because it narrows down the possibilities using common password variations. The success rate of the hybrid attack is high since the individuals use common words or patterns as password. Hybrid attacks can be prevented by utilizing strong passwords including numbers, special characters, uppercase, and lowercase letters. In addition, multi-factor authentication mechanism should be incorporated along with the password to strengthen the security. The lockout scheme should also be implemented after a particular number of failed attempts.

Reverse Brute Force Attacks

A reverse brute-force attack is a kind of brute-force attack in which an intruder utilizes a common password against multiple usernames in an attempt to gain access to a network. The objective of this attack is to gather user account details without authorization by forcing the identical password for all persons. Reverse brute-force attacks often target enterprises with identification of account names, leaked account databases, or commonly accessible account lists. Reverse brute-force attacks starts with the intruder having the password as a known data, but not the username. Attackers verify these passwords against several possible usernames or encrypted files until the exact combination is recovered. The best method to preserve the reverse brute-force attacks is to maintain passwords well secured. Industries should have a standard rules and policy in creating, updating, and securing the passwords. Enterprises can also incorporate two-factor authentication or multi-factor authentication.

Credential Stuffing

Credential stuffing is a kind of cyber-attack where cybercriminals utilize hijacked login details from one system to try to approach an uncorrelated system. Credential stuffing attacks serve on the preface that people use the identical user ID and password frequently across several accounts. Maintaining the login details of one account may provide access to other unrelated account. When an illegitimate parties gathers the exact username and password, credential stuffing creates a quick attack to log in to other computers that may utilize the identical user data.

Differential Cryptanalysis Attack

This type of attack involves examining pairs of plaintexts and their related ciphertext to identify the patterns in the security algorithm. It can be efficient against block ciphers with specified characteristics.

PrasathSrinivasan Sushmitha Algorithm for Text Encryption and Decryption

This proposed novel encryption and decryption is named as Prasath Srinivasan Sushmitha algorithm. This proposed algorithm is used for text encryption through the series of mathematical operations. The various steps involved in text encryption is described in the algorithm. The text encryption reads the string as input and converts it into ciphertext.

PrasathSrinivasan Sushmitha Encryption Algorithm

Step 1: Read the input text.

Step 2: Assign the number from '1' to '26' for the alphabets in uppercase letters from 'A' to 'Z' or in lowercase letters from 'a' to 'z' and write the corresponding number for the given input string.
Step 3: Compute the cube of the individual decimal number.
Step 4: Represent the cubed decimal digit into its equivalent Binary Coded Decimal (BCD) form.
Step 5: Compute 1's complement of the obtained BCD.
Step 6: Convert the resultant 1's complement into equivalent hexadecimal.
Step 7: Represent the hexadecimal value in the form of square matrix. Number of rows and columns in the square matrix depends on the number of digits obtained in hexadecimal.
Step 8: After forming the square matrix, if there is any unfilled elements, assign the value as zero.
Step 9: Exchange diagonal elements.
Step 10: Shift rows towards bottom one time for 2x2 matrix, shift rows twice towards bottom for 3x3 matrix, shift rows bottom three times for 4x4 matrix, shift rows bottom four times for 5x5 matrix and so on.
Step 11: Shift columns one time towards left for 2x2 matrix, twice towards left for 3x3 matrix, shift columns left three times for 4x4 matrix, shift columns left four times for 5x5 matrix and so on.
Step 12: Represent each element into its equivalent BCD form.
Step 13: The resultant BCD value is the ciphertext.

The initial step of this proposed encryption algorithm is to read the string. The alphabets in lowercase letters from 'a' to 'z' or in uppercase letters from 'A' to 'Z' are assigned the value from numbers '1' to '26' respectively. The assigned numbers for the alphabets is to write separately for the given input string. The next step is to compute the cube of the individual decimal number. After cubed, the resultant value is represented in Binary Coded Decimal (BCD) form. The 1's complement is computed for this obtained BCD value. The value obtained after 1's complement is converted into hexadecimal value. This hexadecimal value is represented in square matrix. The number of rows and columns depends on the number of hexadecimal digits. For unfilled elements in square matrix, assign the value as zero and exchange the diagonals of square matrix. Then, shift rows towards bottom one time for 2x2 matrix, shift rows twice towards bottom for 3x3 matrix, shift rows three times towards bottom for 4x4 matrix, and so on. After rows shifted, columns to be shifted one time towards left for 2x2 matrix, shift columns twice towards left for 3x3 matrix, shift columns three times towards left for 4x4 matrix and so on. After shifting rows and columns of square matrix, represent each element into equivalent BCD form. This BCD value obtained is the ciphertext.

PrasathSrinivasan Sushmitha Decryption Algorithm

Step 1: Receive the ciphertext in BCD form.
Step 2: Convert the BCD value to equivalent hexadecimal.
Step 3: Represent the hexadecimal values in the form of square matrix.
Step 4: Shift columns one time towards right for 2x2 matrix, shift columns twice towards right for 3x3 matrix, shift columns right three times for 4x4 matrix, shift columns right four times for 5x5 matrix and so on.
Step 5: Shift rows one time towards top for 2x2 matrix, shift rows twice towards top for 3x3 matrix, shift rows top three times for 4x4 matrix, shift rows top four times for 5x5 matrix and so on.
Step 6: Exchange diagonal elements.
Step 7: Discard the last element if it is zero.
Step 8: Compute 1's complement for the obtained hexadecimal value.
Step 9: Represent the resultant 1's complement in its equivalent decimal number.
Step 10: Compute the cube root of decimal value separately.
Step 11: Assign the equivalent alphabet from the resultant cube root separately.
Step 12: Combine the alphabets to form the string which is the original input text.

The decryption is the reverse process of encryption. The ciphertext received in the BCD form. This BCD value is converted into equivalent hexadecimal value. The next step is to represent this hexadecimal value in square matrix. In this square matrix, shift columns one time towards right for 2x2 matrix, shift columns twice towards right for 3x3 matrix, shift columns right three times for 4x4

matrix, shift columns right four times for 5x5 matrix and so on. The next step is to shift rows one time towards top for 2x2 matrix, shift rows twice towards top for 3x3 matrix, shift rows top three times for 4x4 matrix, shift rows top four times for 5x5 matrix and so on. After shifting columns and rows, exchange the diagonal elements. Discard the last element if it is zero. Compute 1's complement for the obtained hexadecimal value and represent in equivalent decimal value. Then, compute the cube root of obtained decimal value individually. The next step is to assign the equivalent alphabet from the resultant cube root separately and combine the alphabets to form the string which is the original input text.

Result and Discussion

This proposed novel encryption and decryption algorithm is simulated using python. This algorithm involves series of mathematical operations which includes conversion, complement, shifting rows and columns of matrix, and representation of ciphertext in BCD format.

Figure 5 shows the python output of proposed cryptographic algorithm with input string named "KARTHIKEYAN" is capital letters. The encrypted text obtained from the proposed encryption algorithm is a combination of several zeros and ones shown in the output. The decrypted text obtained through the proposed decryption algorithm is "KARTHIKEYAN" shown in the output which is similar to the input string. The input characters in a string and the decrypted text is all in capital letters. This proposed cryptographic algorithm performs encryption and decryption of input string with capital letters.

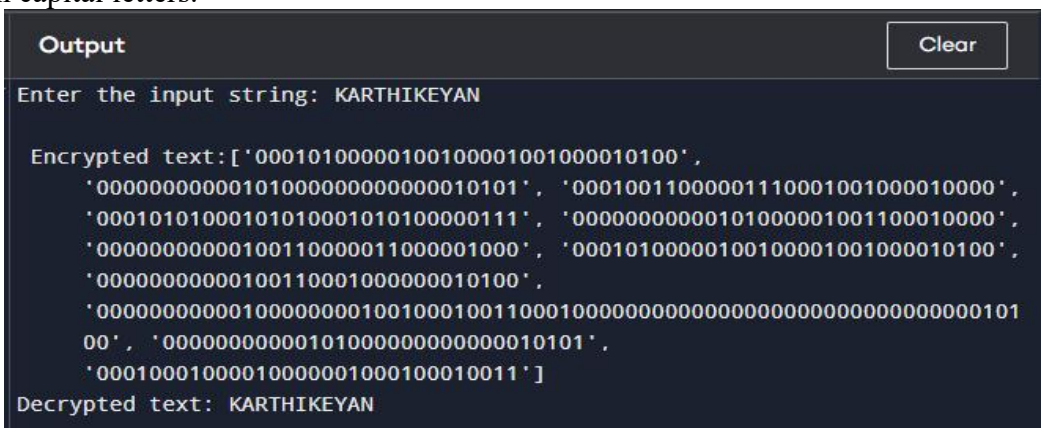

Figure 5 Output of Proposed Cryptographic Algorithm with input string given capital letters

Figure 6 shows the python output of proposed cryptographic algorithm with only first character of input string is capital letter. The input string given is "Ganesan" and the encrypted text obtained from the proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through the proposed decryption algorithm is "Ganesan" shown in the output which is similar to the input string. This proposed cryptographic algorithm accepts both capital letters and small letters, and perform encryption and decryption.

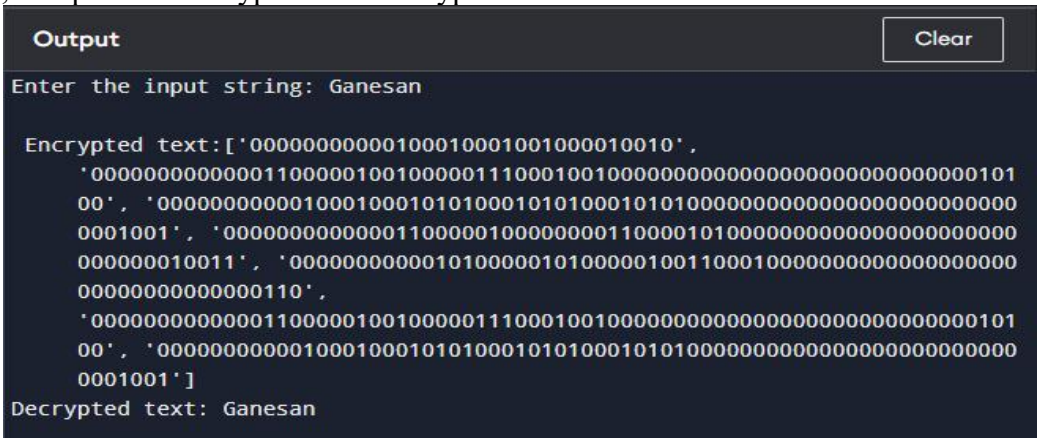

Figure 6 Output of Proposed Cryptographic Algorithm with only the first character of input string given capital letter

Figure 7 shows the python output of proposed cryptographic algorithm with input string is small letters. The input string given is “sangeetha” and the encrypted text obtained from the proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through this proposed decryption algorithm is “sangeetha” shown in the output which is similar to the input string. This proposed cryptographic algorithm can also perform encryption and decryption of input string with only small letters.

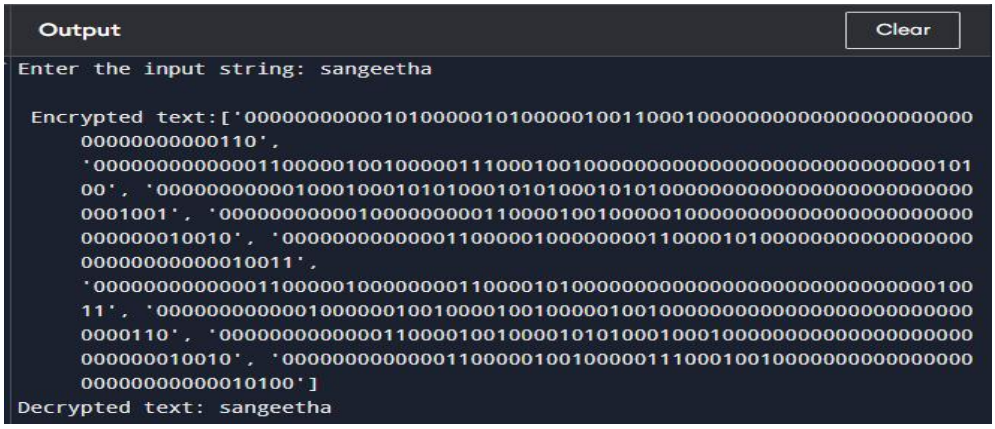

Figure 7 Output of Proposed Cryptographic Algorithm with input string given small letters

Figure 8 shows the python output of proposed cryptographic algorithm with input contains both letters and numbers. The input string given is “Rajesh 537268” and the encrypted text obtained from this proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through this proposed decryption algorithm is “Rajesh 537268” shown in the output which is similar to the input string. This proposed cryptographic algorithm can also perform encryption and decryption of input with letters first and numbers next.

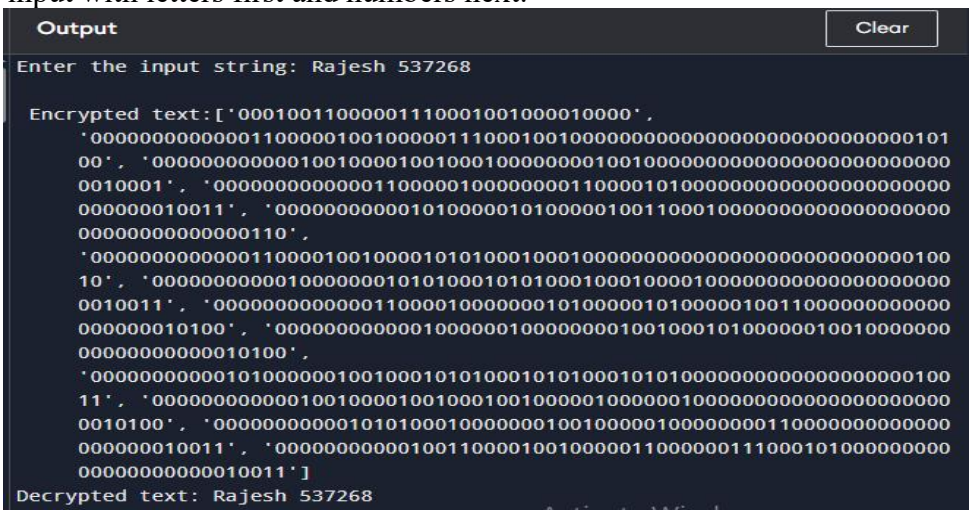

Figure 8 Output of Proposed Cryptographic Algorithm with input String given first and Numbers next

Figure 9 shows the python output of proposed cryptographic algorithm with input contains both numbers and letters. The input string given is “74583 Dinesh” and the encrypted text obtained from this proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through this proposed decryption algorithm is “74583 Dinesh” shown in the output which is similar to the input string. This proposed cryptographic algorithm can also perform encryption and decryption of input with numbers first and letters next.

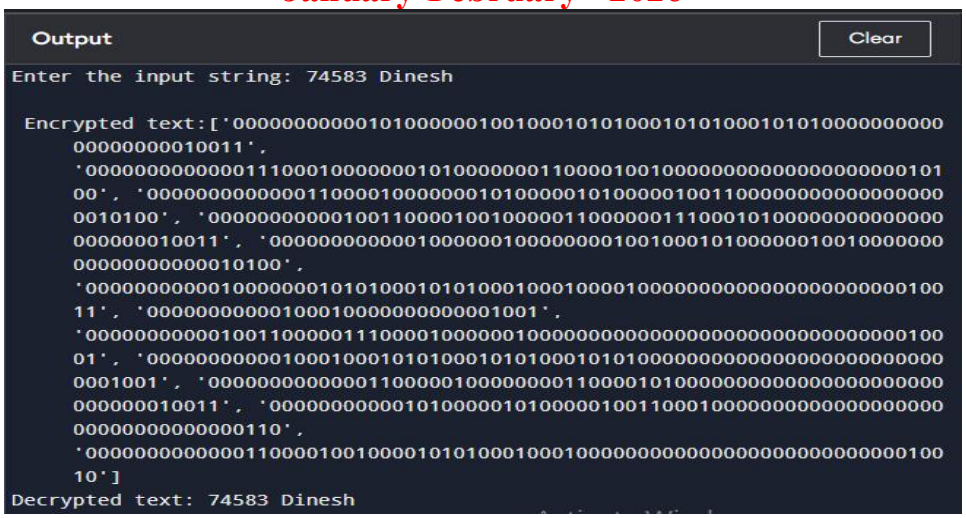

Figure 9 Output of Proposed Cryptographic Algorithm with input Numbers given first and String next

Figure 10 shows the python output of proposed cryptographic algorithm with input contains both letters and special characters. The input string given is “Suresh #&%$!” and the encrypted text obtained from this proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through this proposed decryption algorithm is “Suresh #&%$!” shown in the output which is similar to the input string. This proposed cryptographic algorithm can also perform encryption and decryption of input with both letters and special characters.

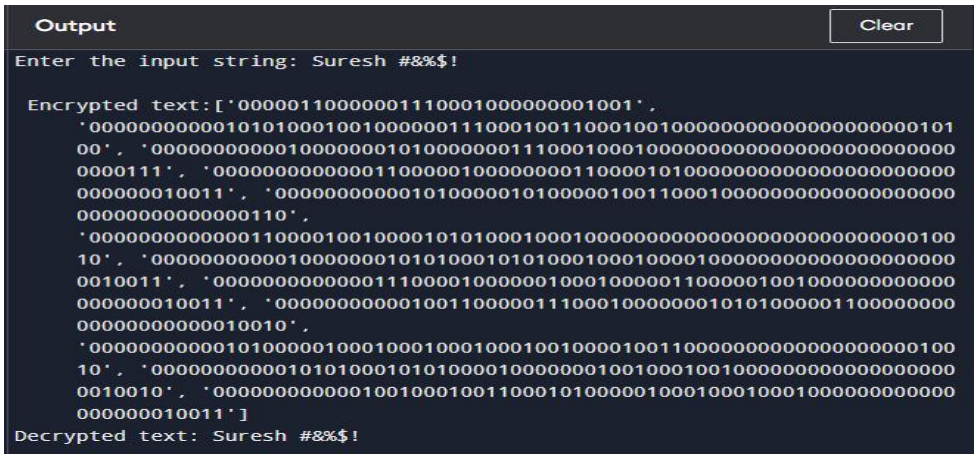

Figure 10 Output of Proposed Cryptographic Algorithm with input String given first and Special Characters next

Figure 11 shows the python output of proposed cryptographic algorithm with input contains combination of letters, numbers, and special characters. The input string given is “Shiva 5274 &$%#” and the encrypted text obtained from this proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through this proposed decryption algorithm is “Shiva 5274 &$%#” shown in the output which is similar to the input string. This proposed cryptographic algorithm can also perform encryption and decryption of input with group of letters, numbers, and special characters.

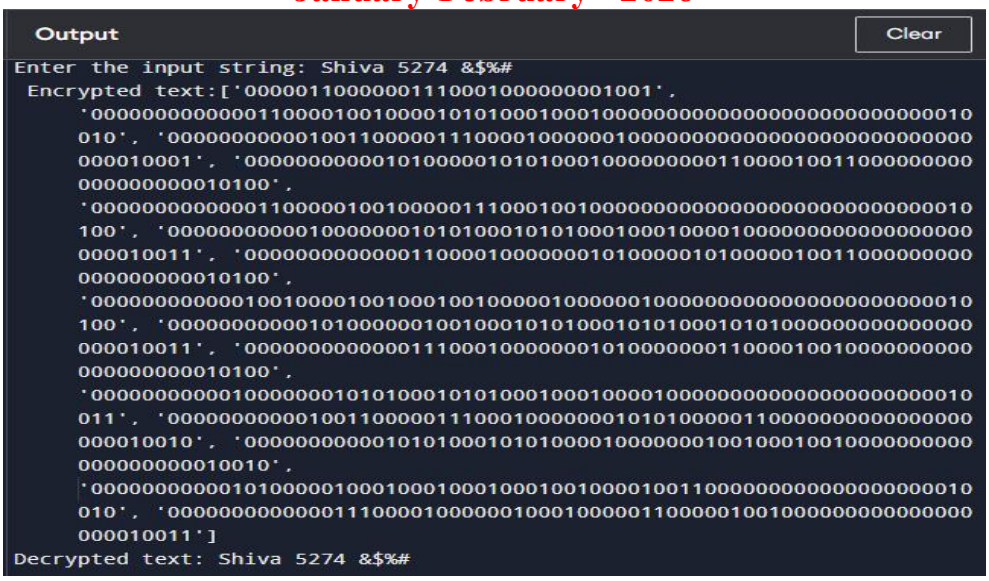

Figure 11 Output of Proposed Cryptographic Algorithm with input given is combination of String, Numbers, and Special Characters

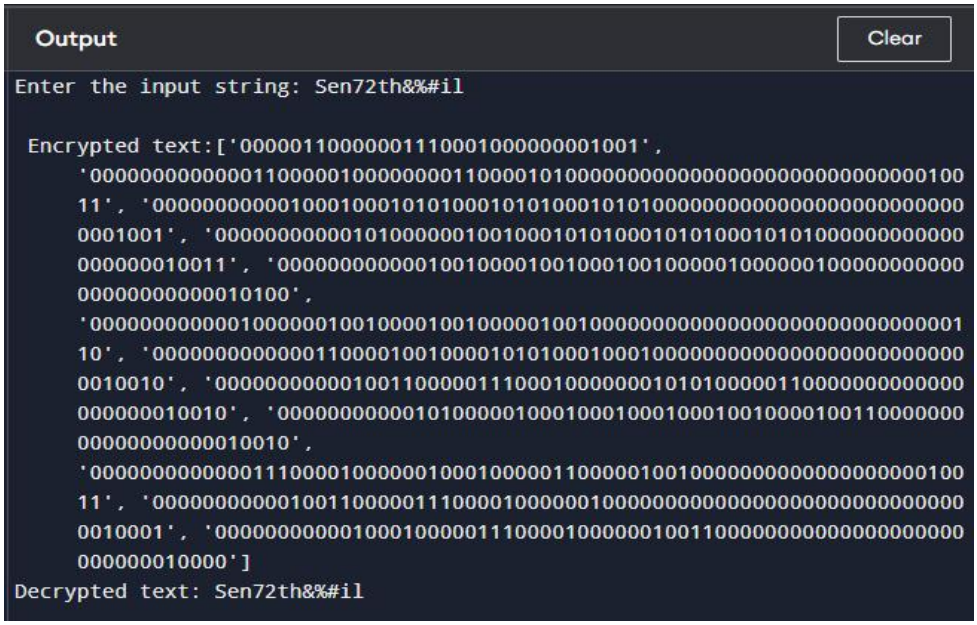

Figure 12 Output of Proposed Cryptographic Algorithm with input given is mixture of String, Numbers, and Special Characters

Figure 12 shows the python output of proposed cryptographic algorithm with input contains mixture of letters, numbers, and special characters. The input string given is “Sen72th&%#il” and the encrypted text obtained from this proposed cryptographic algorithm is a group of zeros and ones. The decrypted text obtained through this proposed decryption algorithm is “Sen72th&%#il” shown in the output which is similar to the input string. This proposed cryptographic algorithm can also perform encryption and decryption of input with mixture of letters, numbers, and special characters.

The novel cryptographic algorithm is proposed which can be utilized for encryption and decryption of string with uppercase, string with lowercase, combination of uppercase and lowercase, combination of string and numbers, combination of string, numbers, and special characters. This proposed cryptographic algorithm offers wide range of security applications include encryption of string, string with numbers and special characters, email messages, whatsapp messages, SMS (Short Message Service), bank account holder name, bank account number, ATM pin number, bank fixed deposit and recurring deposit number, various insurance policy number, various ID cards such as Aadhaar number, PAN number, Passport number, Voter ID number, Smart card number, College

students name, students roll number, faculty name, faculty ID, corporate employee name, employee ID, confidential messages related to bank operations, industrial operations, country borders, central and state government service oriented, online transactions, various transportation related messages include bus, train, and flight. The information and messages related to the various applications mentioned above can be encrypted and transmitted over internet.

The purpose of this proposed cryptographic algorithm is to ensure confidentiality of information transmitted through internet. The benefit of this proposed algorithm is the length of ciphertext increases greatly with variation or increase in number of characters in the input plain text. In addition, there is no limitation in the size of the characters in the input string. This proposed cryptographic algorithm accepts mixture of letters, numbers and special characters and performs encryption and decryption. Attackers cannot detect the original input string since the encrypted text is a combination of several zeros and ones. This proposed cryptographic algorithm offers strong security against unauthorized access, and securing the information across wide range of applications.

Conclusion

Internet is widely used for communicating the process data, private information, bank online transactions, patient's health condition, border's information, credit and debit card transactions. Intruders try to get access and misuse the private information which leads to loss of original data. Attackers can monitor the online transactions takes place across worldwide. They try to get the account details of individuals, and transfer the money in an unauthorized way. Due to this unauthorized transactions, bank customers losses their amount. Security is essential to maintain the sensitive data, messages, and information secret during transmission across internet. This proposed work is the novel encryption and decryption named PrasathSrinivasan Sushmitha algorithm for String Encryption and Decryption. This proposed algorithm involves series of mathematical operations to convert the input string into ciphertext. This ciphertext can be transmitted through internet across worldwide. Decryption is performed reverse of the encryption to convert the ciphertext into original string. The benefit of this proposed encryption algorithm is simple mathematical operations, and it assures confidentiality of data, private information, and messages. This proposed algorithm can be suitable for usage in wide range of applications including text encryption, securing online transactions of amount and account details, securing email messages, securing medical data related to patients, securing industrial process information, and securing the personal information.

References

[1] George S. Rizos, Konstantinos A. Draziotis, "Cryptographic primitives based on compact knapsack problem," Journal of Information Security and Applications, Vol. 83, pp. 103781-103790, 2024.

[2] Li-Woei Chen, Kun-Lin Tsai, Fang-Yie Leu, Wen-Cheng Jiang, Shih-Ting Tseng, "Time Parameter Based Low-Energy Data Encryption Method for Mobile Applications," Computer Modeling in Engineering and Sciences, Vol. 140, No. 3, pp. 2779-2794, 2024.

[3] Abidemi Emmanuel Adeniyi, Rasheed Gbenga Jimoh, Joseph Bamidele Awotunde, "A systematic review on Elliptic Curve Cryptography algorithm for Internet of Things: Categorization, application areas, and security," Computers and Electrical Engineering, Vol. 118, pp. 109330-109351, 2024.

[4] J.S.Prasath, V.Irine Shyja, P.Chandrakanth, B. Kiran Kumar, A. Raja Basha, "An optimal secure defense mechanism for DDoS attack in IoT network using feature optimization and intrusion detection system," Journal of Intelligent and Fuzzy Systems, Vol. 46, No. 3, pp. 6517-6534, 2024.

[5] Nimish Mishra, SK Hafizul Islam, Sherali Zeadally, "A survey on security and cryptographic perspective of Industrial Internet of Things," Internet of Things. Vol. 25, pp. 101037-101065, 2024.

[6] Mishall Al-Zubaidie, Raad A. Muhajjar, "Integrating Trustworthy Mechanisms to Support Data and Information Security in Health Sensors," Procedia Computer Science, Vol. 237, pp. 43-52, 2024.

[7] Olusogo Popoola, Marcos Rodrigues, Jims Marchang, Alex Shenfield, Augustine Ikpehai, Jumoke Popoola, "An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security," Internet of Things, Vol. 27, pp. 101314-101351, 2024.

[8] Vatsal Vasani, Kumar Prateek, Ruhul Amin, Soumyadev Maity, Ashutosh Dhar Dwivedi, "Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions," Journal of Industrial Information Integration, Vol. 39, pp. 100594-100617, 2024.

[9] Ch. Jnana Ramakrishna, D. Bharath Kalyan Reddy, B.K. Priya, P.P Amritha, K.V Lakshmy, "Analysis of Lightweight Cryptographic Algorithms for IoT Gateways," Procedia Computer Science, Vol. 233, pp. 235-242, 2024.

[10] Haochen Dou, Zhenwu Dan, Peng Xu, Wei Wang, Shuning Xu, Tianyang Chen, Hai Jin, "Dynamic Searchable Symmetric Encryption With Strong Security and Robustness," IEEE Transactions on Information Forensics and Security, Vol. 19, pp. 2370 - 2384, 2024.

[11] K. Sasikumar, Sivakumar Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," IEEE Access, Vol. 12, pp. 52325 - 52351, 2024.

[12] Guowen Xu, Shengmin Xu, Jinhua Ma, Jianting Ning, Xinyi Huang, "An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud," IEEE Transactions on Information Forensics and Security, Vol. 18, pp. 5171-5185, 2023.

[13] Lanxiang Chen, Yi Mu, Lingfang Zeng, Fatemeh Rezaeibagha, Robert H. Deng, "Authenticable Data Analytics over Encrypted Data in the Cloud," IEEE Transactions on Information Forensics and Security, Vol. 18, pp. 1800-1813, 2023.

[14] Lei Xu, Xingliang Yuan, Zhengxiang Zhou, Cong Wang, Chungen Xu, "Towards Efficient Cryptographic Data Validation Service in Edge Computing," IEEE Transactions on Services Computing, Vol. 16, No. 1, pp. 656-669, 2023.

[15] Changhee Hahn, Hyundo Yoon, Junbeom Hur, "Multi-Key Similar Data Search on Encrypted Storage With Secure Pay-Per-Query," IEEE Transactions on Information Forensics and Security, Vol. 18, pp. 1169-181, 2023.

[16] Edward Keitaro Heru, Faisal, Hady Pranoto, "File Encryption Application using Menezes-Vanstone Elliptic Curve Cryptography Based on Python," Procedia Computer Science, Vol. 227, pp. 651-658, 2023.

[17] Fairouz Beggas, Ali Lounici, "Generation of random sequences using DNA cryptography for OTP encryption," Biosystems, Vol. 234, pp. 1050-1064, 2023.

[18] Kenan Begovic, Abdulaziz Al-Ali, Qutaibah Malluhi, "Cryptographic ransomware encryption detection: Survey," Computers and Security, Vol. 132, pp. 1033-1049, 2023.

[19]Ankit Vishnoi, Alok Aggarwal, Ajay Prasad, Manish Prateek, Shalini Aggarwal, "Text encryption for lower text size: Design and implementation," Materialstoday: Proceedings, Vol. 79, pp. 278-281, 2023.

[20] Shabana Urooj, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz, S Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," Alexandria Engineering Journal, Vol. 72, pp. 37-50, 2023.

[21] P. Ramadevi, S. Ayyasamy, Yalla Suryaprakash, Chunduru Anilkumar, S. Vijayakumar, R. Sudha, "Security for Wireless Sensor Networks using Cryptography," Measurement: Sensors, Vol. 29, pp. 100874-100880, 2023.

[22] Heba Kadry, Ahmed Farouk, Elnomery A. Zanaty, Omar Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," Alexandria Engineering Journal, Vol. 71, pp. 491-500, 2023.

[23] Swetha Gadde, J. Amutharaj, S. Usha, "A security model to protect the isolation of medical data in the cloud using hybrid cryptography," Journal of Information Security and Applications, Vol. 73, pp. 103412-103425, 2023.

[24] Rathnakar Achary, Chetan J Shelke, Kavin Marx, Aishwarya Rajesh, "Security Implementation on IoT using CoAP and Elliptical Curve Cryptography," Procedia Computer Science, Vol. 230, pp. 493-502, 2023.

[25] D. Shivaramakrishna, M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control," Alexandria Engineering Journal, Vol. 84, pp. 275-284, 2023.

[26] M. Indrasena Reddy, M. Purushotham Reddy, R. Obulakonda Reddy, A. Praveen, "Improved elliptical curve cryptography and chaotic mapping with fruitfly optimization algorithm for secure data transmission," Wireless Networks, Vol. 30, pp. 1151-1164, 2023.

[27] Qiuyun Tong, Yinbin Miao, Jian Weng, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, "Verifiable Fuzzy Multi-Keyword Search Over Encrypted Data With Adaptive Security," IEEE Transactions on Knowledge and Data Engineering, Vol. 35, No. 5, pp. 5386 - 5399, 2023.

[28] Dajiang Chen, Hao Wang, Ning Zhang, Xuyun Nie, Hong-Ning Dai, Kuan Zhang, Kim-Kwang Raymond Choo, "Privacy-Preserving Encrypted Traffic Inspection with Symmetric Cryptographic Techniques in IoT," IEEE Internet of Things Journal, Vol. 9, No. 18, pp. 17265-17279, 2022.

[29] Lei Zhang, Hu Xiong, Qiong Huang, Jiguo Li, Kim-Kwang Raymond Choo, Jiangtao Li, "Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities," IEEE Transactions on Services Computing, Vol. 15, No. 1, pp. 57-587, 2022.

[30]Muhammad Nadeem, Ali Arshad, Saman Riaz, Syeda Wajiha Zahra, Shahab S. Band, Amir Mosavi, "Two Layer Symmetric Cryptography Algorithm for Protecting Data from Attacks," Computers, Materials and Continua, Vol. 74, No. 2, pp. 2625-2640, 2022.

[31] Piyush Garg, Dileep Kumar Singh, "Analysis of cryptographic encryption algorithm design to secure IoT devices: A review," Materialstoday Proceedings, Vol. 51, pp. 810-814, 2022.

[32]Dilip Kumar Sharma, Ningthoujam Chidananda Singh, Daneshwari A Noola, Amala Nirmal Doss, Janaki Sivakumar, "A review on various cryptographic techniques and algorithms," Materialstoday: Proceedings, Vol. 51, pp. 104-109, 2022.

[33] Malik Hamza Murtaza, Hasan Tahir, Shahzaib Tahir, Zahoor Ahmed Alizai, Qaiser Riaz, Mehdi Hussain, "A portable hardware security module and cryptographic key generator," Journal of Information Security and Applications, Vol. 70, pp. 103332-103347, 2022.

[34] Yukun Zhou, Baidong Hu, Yitao Zhang, Weiming Cai, "Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance," IEEE Access, Vol. 9, pp. 122362-122372, 2021.

[35] Aleksandr Ometov, Krystof Zeman, Pavel Masek, Lukas Balazevic, Mikhail Komarov, "A Comprehensive and Reproducible comparison of Cryptographic Primitives Execution on Android Devices," IEEE Access, Vol. 9, pp. 54625-54638, 2021.

[36] Jin Li, Yanyu Huang, Yu Wei, Siyi Lv, Zheli Liu, Changyu Dong; Wenjing Lou, "Searchable Symmetric Encryption with Forward Search Privacy," IEEE Transactions on Dependable and Secure Computing, Vol. 18, No. 1, pp. 460-474, 2021.

[37] Mohammed Abbas Fadhil Al-Husainy, Bassam Al-Shargabi, Shadi Aljawarneh, "Lightweight Cryptography system for IoT devices using DNA," Computers and Electrical Engineering, Vol. 95, pp. 107-117, 2021.

[38] Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal, Sudhir Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," Global Transitions Proceedings, Vol. 2, No. 1, pp. 91-99, 2021.

[39] Cristian Chinas-Palacios, Jesus Aguila-Leon, Carlos Vargas-Salgado, Edith X. M. Garcia, Julian Sotelo-Castanon, Elías Hurtado-Perez, "A smart residential security assisted load management system using hybrid cryptography," Sustainable Computing: Informatics and Systems, Vol. 32, pp. 1-10, 2021.

[40] Avijit Mondal, Radha Tamal Goswami, "Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security," Microprocessors and Microsystems, Vol. 81, pp. 103719-103726, 2021.

[41] Danda B. Rawat, Ronald Doku, Moses Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security," IEEE Transactions on Services Computing, Vol. 14, No. 6, pp. 2055 - 2072, 2021.

[42] J.S.Prasath, U.Ramachandraiah, G.Muthukumaran, "Modified Hardware Security Algorithms for Process Industries using Internet of Things," Journal of Applied Security Research, vol. 16, No. 1, pp. 127-140, 2020.
[43] Hua Deng, Zheng Qin, Qianhong Wu, Zhenyu Guan, Robert H. Deng, Yujue Wang, Yunya Zhou, "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," IEEE Transactions on Information Forensics and Security, Vol. 15, pp. 3168 - 3180, 2020.
[44] Shuguang Zhang, Hequn Xian, Zengpeng Li, Liming Wang, "SecDedup: Secure Encrypted Data Deduplication With Dynamic Ownership Updating," IEEE Access, Vol. 8, pp. 186323-186334, 2020.
[45] Yan Ke, Min-Qing Zhang, Jia Liu, Ting-Ting Su; Xiao-Yuan Yang, "Fully Homomorphic Encryption Encapsulated Difference Expansion for Reversible Data Hiding in Encrypted Domain," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 30, No. 8, pp. 2353 - 2365, 2020.
[46] J.S.Prasath, S. Jayakumar, K. Karthikeyan, "Real-Time Implementation for Secure monitoring of Wastewater Treatment Plants using Internet of Things," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, pp. 2997-3002, 2019.
[47] Mahdi H. Al Hasani, Kais A.Al Naimee, "Impact security enhancement in chaotic quantum cryptography," Optics and Laser Technology, Vol. 119, pp. 1055-1075, 2019.
[48] Ge Wu, Fuchun Guo, Willy Susilo, "Generalized public-key cryptography with tight security," Information Sciences, Vol. 504, pp. 561-577, 2019.
[49] Roderick Hodgson, "Solving the security challenges of IoT with public key cryptography," Network Security, Vol. 2019, No. 1, pp. 17-19, 2019.
[50] Sunil Kumar, Manish Kumar, Rajat Budhiraja, M.K. Das, Sanjeev Singh, "A cryptographic model for better information security," Journal of Information Security and Applications, Vol. 43, pp. 123-138, 2018.
[51] Gaurang Panchal, Debasis Samanta, "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security," Computers and Electrical Engineering, Vol. 69, pp. 461-478, 2018.

AUTHOR PROFILE

Dr. J.S.Prasath received Master of Engineering degree in Process Control and Instrumentation Engineering from Annamalai University, Chidambaram and Doctor of Philosophy degree in Wireless Sensor Networks for Industrial Security from Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as Professor in the Department of Computer Science and Engineering at Sapthagiri NPS University, Bengaluru, India. He is an interdisciplinary and guiding many Research projects at Under graduate and Post graduate level. Earlier he served as Assistant Professor in SRM University, Hindustan University, KCG College of Technology and Narayana Engineering College. His research interests are Embedded Systems, Wireless Sensor Networks, Internet of Things, Process Control and Industrial Automation. He has published twenty five articles in International Journals, presented twenty papers in International Conference, published two patents, written two books and three book chapters. He received the best teacher award and the two innovation awards for his research work.

Ms. Sushmitha G S is currently pursuing her Bachelor of Engineering degree in Computer Science and Engineering from Sapthagiri NPS University, Bengaluru, India. She is an aspiring researcher with a strong interest in Artificial Intelligence, the Internet of Things (IoT), and Web Technologies. She is committed to deepening her technical knowledge and actively engages in workshops and seminars to enhance her skills. Her goal is to contribute innovative solutions to real-world problems through her research in emerging technologies.