JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

Provision of Security Using Substitution Ciphers

N.SureshKumar[1], Ashok Kumar Nanda[2], Purnachand Kollapudi[3] & Bachu Harish[4]

[1]Department of Computer Science Engineering, GITAM Institute of Technology, Visakhapatnam, India.

[2,3,4] CSE Department, B V Raju Institute of Technology, Narsapur, Medak (Dist.), Telangana, India - 502313
Email: **nskgitam2009@gmail.com,** ashokkumarnanda@yahoo.com, purnachand.k@gmail.com,
harishbachu18@gmail.com

Received: 14 Feb 2020 Revised and Accepted: 25 March 2020

ABSTRACT: In recent decade many organizations are facing seviour problems from message hacking and security threats at different levels of organization. The security threats can be overcome with efficient cryptographic techniques. The cryptographic industry has many challenges such as responding the threats on time before being late. The rapid attacks of malicious software highly demands strict implementation of cryptographic techniques. The emerging technologies in cryptographic techniques rises confidence level to overcome security problems in various domains of industries.In the present paper different classical cryptographic techniques are discussed and analysed their respective flaws to analyse the security tools in cryptography industry.

KEYWORDS: : cryptography, security, encryption, decryption

I. INTRODUCTION

In the era of internet millions of computers connected via internet throughout the globe. The number of devices connected via internet growing rapidly and throwing enormous challenges in the internet.There are multiple number of browsers are using internet to synchronize and communicate the data between server and client system. The communication via internet is an essential facility required by millions of people. The necessity of internet facility is growing day-by-day parallelly the security threats also. The essence of internet is increase in daily life of ordinary people in many applications like financial applications, e-commerce, social sites, military, health care and etc. It became very difficult task for internet service provider to provide security for internet users[1][2].

There are many ways presently existing to provide security in many applications such as providing security for login passwords, ecommerce sites, payment gateways, and etc. The most common technique used in all the domains is cryptographic technique. The main concept of cryptography is to provide security for data and personal information. The cryptographic techniques increase the confidentiality in providing security by avoiding unauthorised persons from accessing the private data[3].

The cryptographic texts have many advantages like, the texts can be transmitted through untrusted channels and the hackers cannot see the original text and difficult for them to crack the data under the circumstances that thay have accessed. In the present paper various cryptographic algorithms and their functionalities are discussed with respect to encryption and decryption.The working principle of cryptography includes, when a message want to be transmitted to destination privately and secure form and wants unauthorized persons not allowed to see the content in the message by encryption tools. At the receiver side the encrypted message will be decrypted by a secured key provided by the sender. In this way the data will be transmitted with security and hence the data cannot be hacked in the middle of the transmission. This can be achieved by cyphers. While the data is transmitting to the sender the data initially will be in meaning full format. The cryptography is art of science which converts meaning full data into meaningless data and that data will be transmitted to receiver. The meaningless data will be again transformed into original format using decryption technique as shown in figure 1. Hence, the encryption and decryption provide reliability, confidentiality, and accuracy while transmitting the data through unsecured network or channel[4].

It demands some security issues in the context of effective communication between several applications, such as valid authentication, privacy, integrity, and Non-repudiation. The authentication represents one's identity between sender and receiver communication. It ensures that valid persons are authorised to access the communication channel. The privacy in the communication indicates only a valid authenticate person only receives the message and able to decrypt the message. The integrity of the data communication represents that original data is received by the receiver without any deviation from the original data even after encryption of the original data. The Non-repudiation represents that valid transmitter has really sent the genuine data to receiver [5][6].

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

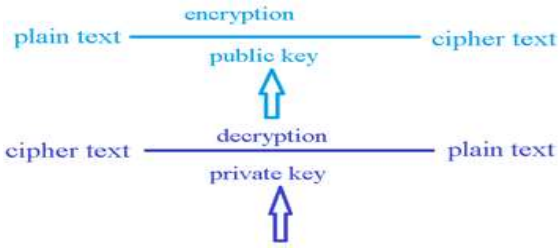


Figure 1Process of transforming the plain text

II. Implementation

In the present work the performance of various algorithms are analysed and shown the results obtained from their execution.

2.1 Substitution Cipher: In substitution cipher the character present in the text from the defined set of character set is substituted with another character derived from the same set of characters with respect to a key [7]. For instance, with a shift of 1, B would be replaced by C, C would become D, and so on. In the following section different types of substitution cipher techniques are discussed.

i. Simple Substitution: The cypher character encrypted in more complex way by shifting or scrambling or reversing the text. This is called deranged alphabet or mixed alphabet. Mixed alphabets are deranged with the help of a keyword and removing repeated letters after which they are arrange in normal order.

ii. Homophonic Substitution: The standard substitution can be cracket by identifying the frequency of the letter. Some letters most commonly used in text framing. Those letters are easily identifiable after checking frequency of occurrence. If the common letter is allowed to replace by different letters, then the common letter will be spread over several characters. Hence the resulting cypher text will be more secure. Homophonic substitution is providing more secure way of providing cipher text by replacing single type of letters with several different types of alphabets, numbers, and symbols. The simplest way is numerical substitution of plain text. Hence the number of homophones given for a single letter is proportional to the frequency of its occurrence [8].

iii. Polyalphabetic Substitution:In this technique multiple cypher alphabets are used and saved in a table. The encryption of a text is done reading next cypher text from the corresponding column of the table. One of the famous polyalphabetic substitutions is Vigenere cipher.

iv. Polygraphic substitution: In this technique the plain text letters are encrypted with large groups of cypher texts. Instead of substituting with single letters individual letters will be replace with groups. The main advantage is that frequency of letter distribution in encryption is good and large number of symbols are used for cypher text.

v. The one-time pad:It is one of the efficient methods used where it is proved unbreakable when compared with its previous techniques. In this technique the plain text is combined with the key text in the manner such as XOR format. The one-time pad is unbreakable as it is used key material only once.

2.2 Atbash cipher: The Atbash cipher is one of the substitution cipher where the the letters are replaced with reversed character with a specified key. For instance letter ‘A’ is replaced with ‘Z’ and letter ‘B’ replaced with ‘Y’. Here the cipher is a substitution key applied with a fixed key. The substitutional key is used for decrypting the message. The functional flow diagram is shown in figure 1.

2.3 Caesar Cipher: The Caesar Cipher is one of the simplest ciphers used in cryptography techniques. In this technique the letters in the plain text is moved to some specific position with respect to the cypher key. For instance with shift of 2 the letter ‘Z’ will be replaced by letter ‘B’. The figure 2 depicts the functional flow diagram of Caesar Cipher [8].

2.4 Vigenere Cipher: The vigenere cipher technique is one of the polyalphabetic substitute method. To implement a cryptographic technique a table format is used for storing letters fro mA to Z. The table contains 26 rows to store all alphabets.The first row of the table fill with the input contains plain text. The successive rows in the table will be the succeeding letters of the previous row letters [11]. The cypher key will decide which cipher text of the corresponding row of plain input text has to consider. If the key word is ‘wild’, then the plain text enciphered according to the key values. The first letter of plain text will be encrypted with the alphabet under ‘w’, the second letter will be enciphered with the letter under ‘I’ of key ‘wild’, the third letter of plain text will ciphered under letter ‘l’, and the fourth letter will be enciphered under letter ‘d’. The flow diagram of encryption nand decryption of vigenere cipher is shown in figure 3.

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

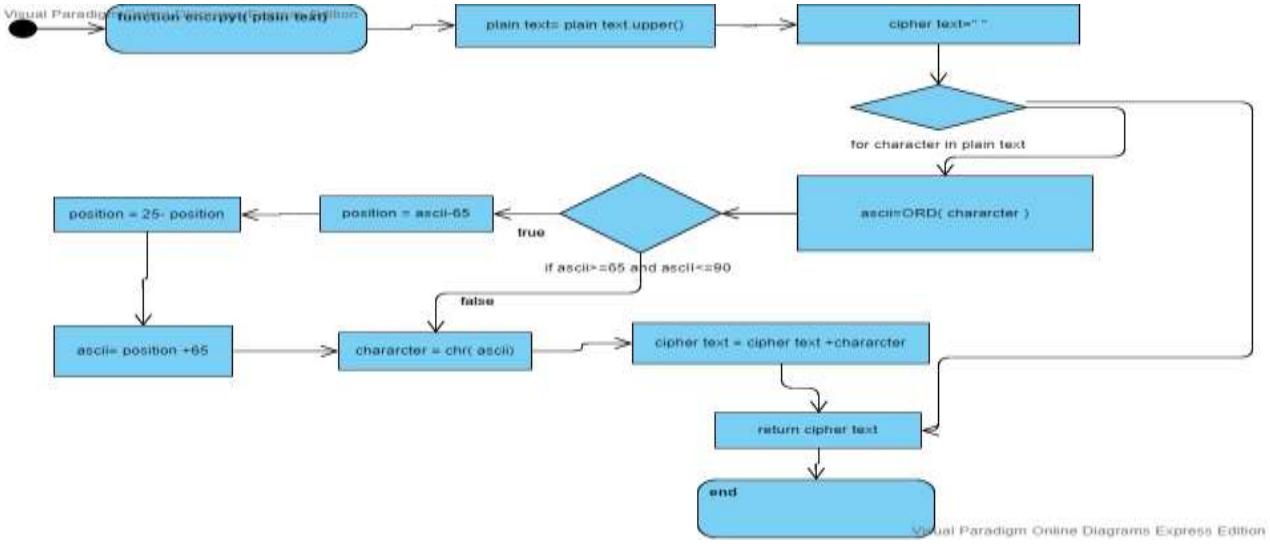


Figure 1: UML diagram of Atbash cipher

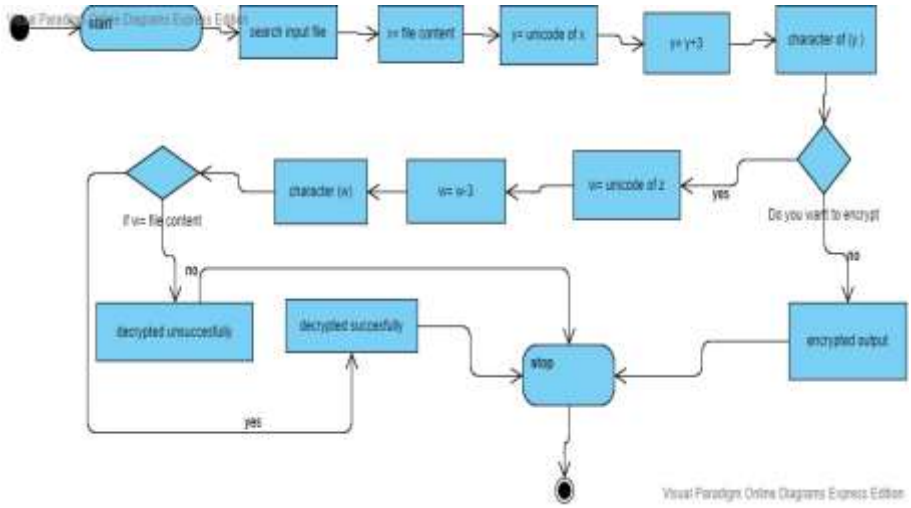


Figure 2: UML diagram of Caesar Cipher

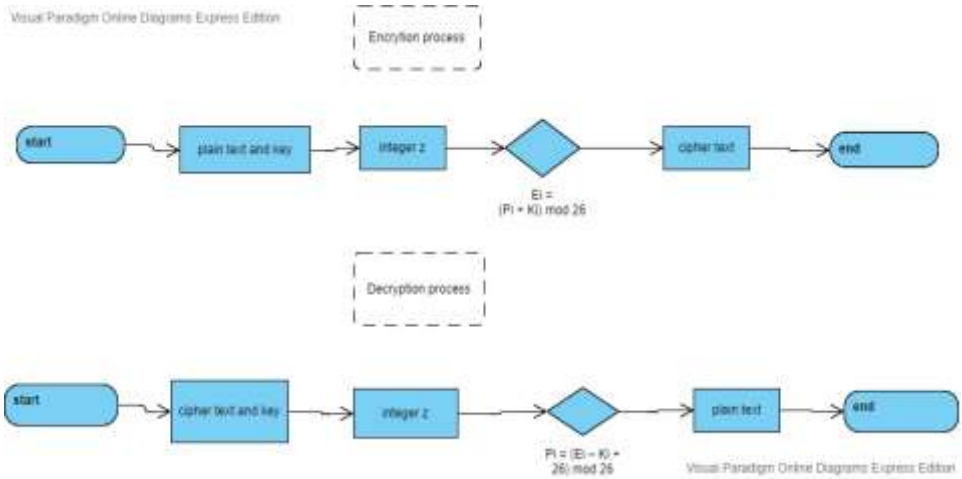


Figure 3: UML diagram of vigenere cipher

2.5 Vernam Cipher: It is a substitution type of cipher technique. Here each character of the plain text is assigned with a number and similarly for the key according to the alphabetic order in the text. Add the both numbers after assigning the number to letters. If the sum after the addition is greater than value 26, then subtract letter number from 26 [12].

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

2.6 One Time Pad: In this technique plain text will be paired with random secret key. This is referred as one time pad. Here each bit or character of plaintext encrypted by combining with each bit or character of secret key. For instance the combination may be XOR combination. Hence this cipher code complex to break, but it require the same size or longer pre-shared key when compared with length of given message.

These classical algorithms are not totally free from the loopholes present in cryptographic techniques. The key size of classical cryptographic techniques is small and hence the security is less and life expectancy will be reduced. The classical cryptographic techniques are easy for implementation, but the process is complex for generating cypher key [12]. The one-time pad is cumbersome process of transaction of pads. Hence it is observed that classical cryptographic techniques are not used regularly. To overcome these problems more sophisticate and efficient techniques are developed in recent era of cryptographic techniques.

III. Results

The output of atbash cipher is shown in figure 4. To encipher a message, find the letter you wish to encipher in the top row, then replace it with the letter in the bottom row. The figure 4a depicts the message "Lets" gets converted to Ovgh. Similarly, all others are encrypted following the same rule.

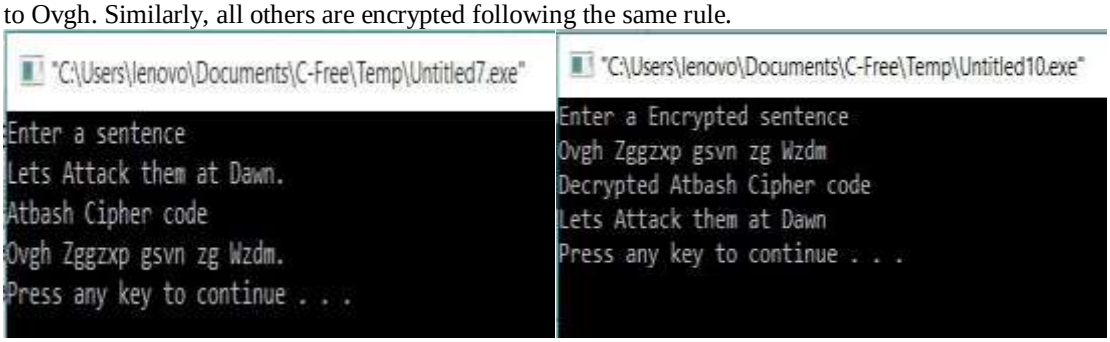


Figure 4: a) Encryption of atbash cipher b) Decryption of atbash cipher

Similarly, the figure 4b is showing decipher and bring back the original text, reverse the process, that is the letter of bottom row gets replaced by the letter in top row. In the output also the word "Zggzxp" gets decrypted to Attack as the letter Z is replaces by A and similarly for others letters also.

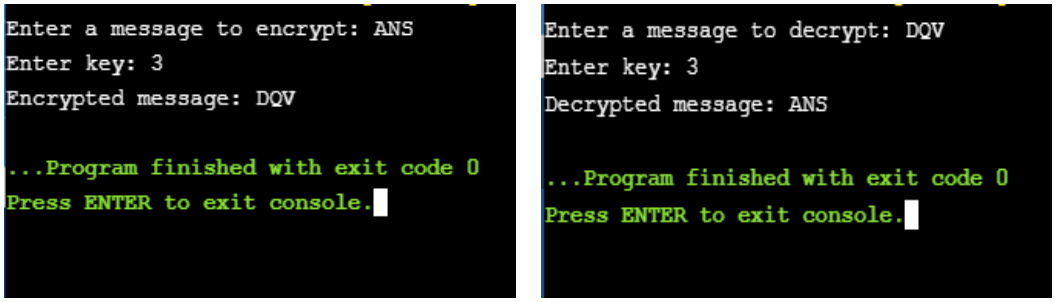


Figure 5: a) encryption of caesar cipher b) decryption of caesar cipher

The figure 5a showing a shift value of 1, A will be replaced by B, B becomes C, and so on. An Integer values between 0 and25 denoting the required shift. Traverse the given text one character at a time. Therefore, A on 3 gives encrypted message as D and so on for remaining letters. The figure 5b showing an offset of given key number to reverse the obtained cipher text to plain text. Traverse the given text one character at a time. Here depending on integer specified we shift in backward direction.So, D when given an input of 3 shifts backward to 3 places and returns A and so on.

Here figure 6 showing a new key by repeating the given key till its length become equal to original message length. Then the new Generated Key transformed into HELLOHELLOHELLOHEL. For encryption take first letter of message and new key i.e. T and H. Take the alphabet in Vigenere Cipher Table where T row and H column coincides i.e. A. Repeat the same process for all remaining alphabets in message text. In decryption process take first alphabet of encrypted message and generated key i.e. A and H. AnalyzeVigenere Cipher Table, look for alphabet A in column H, the corresponding row will be the first alphabet of original message i.e. T. Repeat the same process for all the alphabets in encrypted message.

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

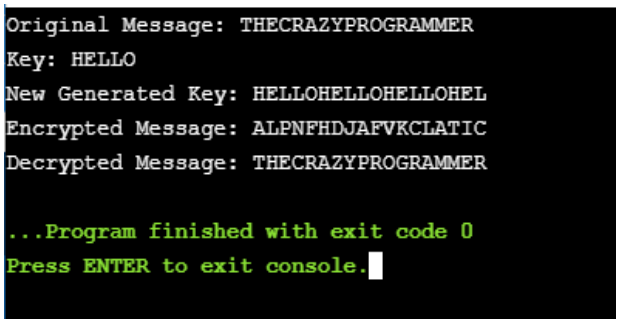
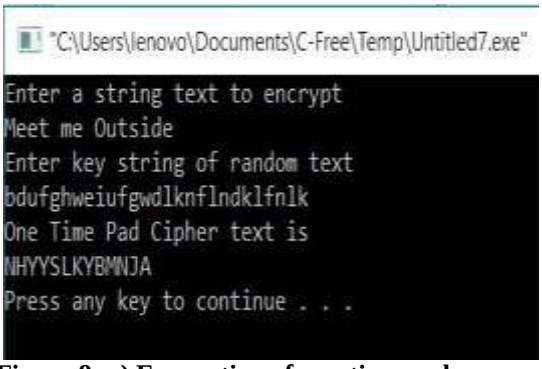


Figure 6: encryption and decryption of vigenere cipher

Figure 7: encryption and decryption of vernam cipher

In the vernam mechanism a number is assigned to each character of the plain text, like (a = 0, b = 1, c = 2, … z = 25) and the key according to alphabetical order. Figure 7 is showing the output screen wher "h" is assigned with number 6 and key letter "g" as 7 and after addition sum will be 13 which is "n". Similarly to get back the original text instead of addition we perform subtraction between the integers.



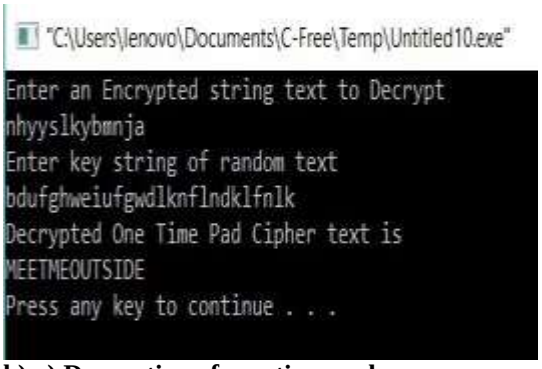


Figure 8: a) Encryption of one-time pad **b) a) Decryption of one-time pad**

The output screen of one-time pad is shown in figure 8. The cross section achieved between two letters is the plain text. It is described in the figure 8. In the above example m, this is 12 and b which is 1 when gets added gives rise to 13 which is n and so on for remaining text. For decrypting a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter. It is nothing but subtracting the key from encrypted text to get back the original one.

IV. Conclusion

The use different types of algorithms help to establish security services in different service mechanisms. Also, cryptography plays a vital and critical role in achieving the primary aims of security goals, such as authentication, integrity, confidentiality, and no-repudiation. The algorithms are developed in order to achieve these goals. It has the important purpose of providing reliable, strong, and robust network and data security. In this paper, a review of some of the techniques has been conducted in the field of cryptography as well as of how the various ciphers used in cryptography for different security purposes work. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and ecommerce data and providing a respectable level of privacy.

.

ISSN- 2394-5125 VOL 7, ISSUE 04, 2020

V. REFERENCES

1. Seddeq EG et al., “New text encryption Method Based on Hidden Encrypted System Key”, ACIT-2018, June 2018, Czech Republic, pp 240-244.
2. Williaqm stalling, “Cryptography and Network security principle and practice”, person, third edition, 2006.
3. Mohammad Barakat et al., “An Introduction to cryptography”, Second Edition, Lecture notes university of kaiserslautern, Sept, 2018.
4. Arjen Ket al., “ Selecting cryptographic key sizes”, In public key cryptography, 2000
5. Ayushi, “A symmetric key cryptographic algorithms”, International Journal of Computer Application, vol 1 No 15, 2010
6. P N V Syamala Rao M et al., “Bitcoin Analysis & Prediction Using Var”, International Journal of Advanced Science and Technology, Vol. 28, No. 19, (2019), pp. 1141 - 1151
7. Shobhavatsa et al., “Novel Cipher Technique Using Substitution Method”, ijins, vol1 issue 4, sept 2012.
8. Chris Savarese and Brian Hart, " The Caesar Cipher ", Trinity College,Last updated: Mon, 26 Apr 2010
9. valdemar c. rochajr, cid b. Dearaújo, "Homophonic Substitution",Departamento de Eletrônica e Sistemas, UFPE, Recife, PE, Brazil.
10. Al-Amin Mohammed Aliyu et al., “Vigenere Cipher: Trends, Review and Possible Modifications”, International Journal of Computer Applications (0975 – 8887) Volume 135 – No.11, February 2016.
11. AndysahPuteraUtamaSiahaan, “Securing Short Message ServiceUsingVernam Cipher in Android Operating System”, International Journal of Mobile Computing and Multimedia Communications, vol 3(4), jul 2016
12. ShachiSharma et al., “Encryption And Decryption Using One Pad Time Algorithm In Mac Layer”, nternational Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 6, June 2013.