International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-7, Issue-7,2020 Regular Edition E-ISSN: 2349-7084

NISSC: A New Information Security System Using Cryptography

Ira Nath*[1], Avijit Baidya[2], Sajal Kumar Biswas[3], Snehartha Dam[4], Kabita Singha[5]
[1,2,3,4 &5]*Computer Science and Engineering, JISCE, Kalyani, Nadia, West Bengal, India, 741235*

Ira.nath@gmail.com[1], avijitbaidya8132@gmail.com[2], sajalkumar306@gmail.com[3], sc.snehartha@gmail.com[4], kabitasinghamrn@gmail.com[5]

**Corresponding Author: avijitbaidya8132@gmail.com*

Available online at: http://www.ijcert.org

Received: 30/06./2020, Revised: 01/07/2020, Accepted: 21/07/2020, Published: 03/08/2020

Abstract: - When we talk one to one that is called human language that is called plain text or normal text. When we talk in normal text or plain text, then all human can understand this text or language easily. That is why we create a cryptography security system to convert this plain text to cipher text. In this security system, we use both number and English alphabet for encryption and decryption the text to hide the plain text. In this security system encryption is mainly depend upon the key generation. The main goal of this security system is to convert simple message or text to non-readable text to secure the messages from hackers; this is called decryption. In this project, at first we find the ASCII value and binary value of the number and alphabet then after all calculation of this value we find the encrypted value and using this value we find decrypted value. In this project, we use RSA and DES and Cryptography for doing encryption and decryption. Moreover, use the ASCII number. In improvement, we complete the whole key generation and encryption and decryption process, which will take linear time.

Keywords: Both Symmetric and Asymmetric key, Prime Number, English Alphabet, Cryptography.

---

1. Introduction

In the current century can be promptly marked as the era of Information. When we sent electronic message, this message is saved as electronic data. This2 electronic massage and the data which can be in any form, be it, text, audio, video etc., this type of message is sent trough the Android Phone, Tablet and any electronic communicator medium. Now, as the saying goes "there are two sides of the same coin "1, similarly advanced technology calls upon many disadvantages along with its advantages. When we send an important message without security protection, then its high probability to leaked the message. To the rescue among many measures, comes up one of the remarkable, significant and vital measures which is cryptography that involves encryption and decryption. In the past days, people write a message. Moreover, those days people send their message or Information limited number of people that is why people devolved this type of security system to secure the Information or hide Information to unwanted people or hackers. This Security system is called the cryptography.

We all heard about the cryptography system. Cryptography comes from the Greek word krypton; it means the hidden. In cryptography mainly depends upon the encryption and decryption. In the 1970 "s new era of cryptography is come that's called advance cryptography system. In the new cryptography system, data or Information is more secure. The first cryptography algorithm is called the

Data Encryption Standard (DES) invented on January 15 1977. It is the First standard algorithm in cryptography. Then after this, in 1980 American National standard Institution use this algorithm for commercial use in the United States. The Cryptography system a very big role in our life and the economy of the world. In the banking and commercial sites cryptography Played a vital role because it helps to secure the message or instruction over the hackers. The major processes which constitute the cryptography are The Encryption, The Decryption, and the key generation. In the Cryptography the Encryption system is two types.

(1) Symmetric Encryption.

(2)Asymmetric Encryption.

In this day in our world cryptography is not only the encryption and decryption. In the cryptography system in these days there are several theoretical formulas. Furthermore, cryptography is mainly on modification are take place. It provides several study material and algorithm and several protocols to use in internet security and secure any instruction or message on the internet.

In the cryptography, there are another algorithm is RSA .In this algorithm based on the RSA and DES algorithm. In this algorithm, there are two prime number and one English alphabet. Moreover, after this at first, multiply this two prime number and find the ASCII value of the English alphabet and adding these two number. Adding find the Binary value of this number and after finding binary value, use this value for encryption and decryption.

Rest of the paper is organized as Section describes the literature survey; the proposed algorithm has been illustrated in section 3. The illustrative example has been depicted in section 3. The conclusion is shown in section 4.

1.1 Objective

The main objective of this paper is to propose an algorithm for security measures. In our computer system, several attacks are occurred by attackers; this type of attack is known as a malicious or mischievous attack. In this type of attack mainly occurred because of creaking the fanatical transaction, Information and instruction. Because of this, we create this key or system the attackers cannot easily creak the instruction that occurs on encryption and decryption process. In this system in encryption process mainly work on ACKSII value and multiplication, and decryption process mainly work on the reverse of the encryption. In this system private key mainly depend upon Encrypted message and decrypted message. The main objective of this system is to secure the instruction or key to the attackers.

1.2 Scope

The main aim of the project is to convert the message plain text to cipher text. By using this plain text cannot readable by attackers or unwanted people and the message only readable by authorized people. In this system provide a good environment for key Generation, Encryption and Decryption. And it sends the encrypted and decrypted message securely. This system helps several security issues in cryptography system.

2. Literature Survey

Today increases wireless communication security is the most important thing during data transmission. In this paper, we represent the literature study of cryptography security encryption and decryption algorithm, wireless communication, and its available application in communication and data communication for the security of data transmission from source to destination. The main reason for using cryptography is to secure our data and also to protect Information by transforming with the help of technology applications. Cryptography plays a vital role in secure data through secret writing. The encryption algorithm is a type of algorithm by which we can encode the data in a non-readable format so that no one can hack or use the data.

The decryption algorithm is a type of algorithm which is converted the encrypted data in a readable format which can be understood by the computer and can also read the text or the data. It decodes the encrypted data so that the authorized person can use the data. The decryption process is like a reverse of the encryption process. As we know that the data are transfer over the internet so due to this encrypted data, we can reduce the data loss and theft.

Cryptography is two types.

Secret key Cryptography: In cryptography secret key cryptography means the same message is used for encrypted and decrypted, For example, DES, Triple DES, AES etc.

Public key cryptography: In cryptography, public-key cryptography are those type of cryptographies who use different

 https://doi.org/10.22362/ijcert/2020/v7/i07/v7i0704

Key for encryption and decryption, For example, RSA.

Some of the concept used in cryptography is followed: -

Plain text- it is the original message or any language we are used to communicating that is used by a human being.

Cipher text- it is the non-readable format of the plain text or code or a secret message.

Encryption-the process of encode the plain text into cipher text message is known as the encryption process.

Decryption- it is like a reverse of encryption process that is transforming the cipher text into a plain text known as decryption process.

Key-perform the encryption and decryption process we need an important aspect is known as key. There are mainly two keys are used in encryption and decryption process are public key and private key.

Cryptography is used to protect our data network and data transmission over the wireless network.

The main purposes of cryptography are follows

1. confidentiality- it means that keeps the message secret. If A send a message to B then it is impossible to know the concept or the Information of an encrypted message without knowing about the secret key.

2. Integrity- it is used for verifying that the message is not modified between transmissions.

3. Authentication- it means that P send a message to S then S received it so S want to Know that it is the message that P sends or not.

4. Non -repudiation - it means that someone can't deny that they sent the message.

2.1 MD5 Algorithm

It is a message-digest algorithm. It is used hash function producing a 128-bit hash value. It is designed for used as a secure cryptographic hash algorithm for authenticating the digital signature. It is very easy to generate a message digest of the original message using this algorithm. In MD5 algorithm mainly based on hash or Fingerprint technique. When we send a long message, the MD5 algorithm is used. The most common technique is used in MD5 is verification in a digital signature.

2.2 RSA Algorithm

Rivest Shamir Adleman is a type of algorithm used by a modern computer to encryption and decryption process. It uses different keys for encryption and decryption process, that is why it is known as an asymmetric algorithm. Once the message is encrypted using the public key it can only be decrypted by another key is the private key. In this algorithm, work on two different keys that are public and private key. By the name of the public key the key is given to all, and the private key is secret by its name.

2.3 DES Algorithm

Data encryption standard is a symmetric key algorithm which means that same key used for encryption and decryption process. It takes 64bits of blocks in plain text and converts them into ciphertext using keys of 48bits. Moreover, the all 64 bits the 56 bits are used for algorithm and the last 8bit are used in checking parity. That's why the 56bit of the key is called an effective key. It is more secure compare to all of the algorithm in cryptography. The main advantage of using DES algorithm is it uses the same hardware and software and the direction of both.

2.4 Cryptography

Data or Information are travels over the internet through one computer to another computer at that time the most important is that the data or Information to be safe and secure. Cryptography plays a major role in security that data are safe during transmission that is an unauthorized person cannot use our data / Information. Cryptography is a technique where firstly the data are converted into a non-readable format is known as encryption process and the non-readable data are converted into readable format means the original message is known as decryption process.

Plain text - It the original message that can be easily understood by anyone.

Cipher text- It the converted message or the transformed message.

Key- There are two types of key used in cryptography they are if the sender and receiver use the same key it is said to be symmetric key or public key. If the sender and receiver use different keys it is said to be an asymmetric key or private key.

 https://doi.org/10.22362/ijcert/2020/v7/i07/v7i0704

3. Proposed Algorithm

ASSKI Algorithm

3.1 Key Generation: -

- We take two prime numbers as input for key generation and Take a character from English Alphabet.
- At First multiply two prime number. Take Character A, Find the ACSKII value of A=65
- After this we perform addition of this two number.
- 24+65=89 Find the Binary Value of this Number
- 89 is the ACSKII Value of Y.

3.2 Encryption Algorithm for Heuristic ASSKI with suitable example.

- 89=1011001 the number is not in 8 – bit number so we add an extra zero at MSB position as per the encryption Algorithm.
- So, it would be0 1 0 1 1 0 0 1 Take the reverse of this 8-bit binary number.
- Take the reverse of this 8-bit binary number
- The reverse number is 1 0 0 1 1 0 1 0
- Let 1 0 0 1 as divisor i.e. key. Divide 1 0 0 1 1 0 1 0(dividend) by 1 0 0 1 (divisor). The remainder is 1 which is 1-digit number so make it 3 digits as 001 and the quotient is 1 0 0 0 1Which is 5-digit numbers.
- Now remainder is added at first three digits and quotient are added at next five digits. And add this 3- and 5-digit number. 0 0 1 1 0 0 0 1 ACSII emulation of this 8bit is 49 is number 1 in decimal. Means 49 ACSII Value is 1.

3.3 Decryption algorithm for Heuristic ASSKI

- We have Got the chipper Text 0 0 1 1 0 0 0 1.
- Multiply this last Five digits i.e. quotient by Four-digit key.
- Add the first 3 digits of the cipher text that is remaining to the resultant of multiplicand to produce the new result.
- If the finding result is produced after the addition in the previous step is not A 8-bit number then we need to make it the 8-digit binary number.
- Then reverse the number to get the original text that is called plain text in cryptography

3.3 Decryption Algorithm for Heuristic ASSKI Example.

- In the encryption algorithm, we generate a number 1.
- In the decimal number system, the ASCII value of character 1 is 49.
- The Binary equivalent is 00110001.

  0 0 1 1 0 0 0 1
- Multiply the last 5 digits (10001) by the key i.e. 1001.

  1 0 0 1 1 0 0 1
- Adding the first three digits of ciphertext, i.e. 001 from the result of the previous step.

  1 0 0 1 1 0 1 0
- Reverse this 8-digit binary number.

  0 1 0 1 1 0 0 1
- The number obtained is the original text, i.e. 01011001 in binary and 89 in decimal which is a letter "Y"

4. Result

At first, we find 89 is the ASCII Value of Y in key generation after this in encryption process we find 49 for key and 49 is one decimal no that's way 49 ACSKII Value is 1.then this 49 we got one chipper text and reverse of this chipper text we find plain text the plain text is 0 1 0 11 0 0 1. The value of this chipper text is 89 that's means the value is same the encryption and decryption is successfully done.

5. Conclusion and Future Scope

The main conclusions of the study may be presented in a short Conclusion Section. In this Section, the author(s) should also briefly discuss the limitations of the research and Future Scope for improvement. While we were doing addition, multiplication, reverse and division after we get chipper text and reverse of this chipper text, we get plain text. In this cryptography system gives more high security for key exchange and prove more security. Furthermore, we can say that this cryptography helps online security and effective for hidden data from hackers.

 https://doi.org/10.22362/ijcert/2020/v7/i07/v7i0704

References

[1] Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). A Greek-English Lexicon.Oxford University Press.

[2] David Naccache, "Cryptography and Security: From Theory to Applications", Springer, 2012.

[3] H.B. Pethe, Dr S. R. Pande, "An overview of Cryptographic Hash Function M-5 and SHA", IOSR-JCE, 2016.

[4] Ius Mentis: Law and technology explained, "The MD5 cryptographic hash function", October 1, 2005.

[5] Alok Kumar Kasgar, Mukesh Kumar Dhariwal, NeerajnTantubay, HinaMalviya, "A Review Paper of Message Digest 5 (MD5)", IJMEMR, Volume1, Issue 4, December 2013, ISSN: 2320- 9984 (Online).

[6] EvgenyMilanov, "The RSA Algorithm", June, 2009.

[7] AviKak, "Public-Key Cryptography and the RSA Algorithm", Lecture Notes on "Computer and Network Security", February 16, 2017.

[8] William Stallings, "Cryptography and Network Security: Principles and Practices", Publisher: Prentice Hall, November 16, 2005, Pages-592.

[9] Nath, Ira. "NHSKCA: A New Heuristic for Symmetric Key Cryptographic Algorithm." *Ira Nath, Deepashree Bhattacharyya AgnisuddhaMandal, NandiniKundu and Oindrila De (2017). NHSKCA: A NEW HEURISTIC FOR SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHM. International Journal of Computer Engineering in Research Trends* 4, no. 12 (2017): 547-553.

Authors:-

Ira Nath is presently working as an Assistant Professor in the Department of CSE in JISCE, India. She received the Master of Technology (M.Tech.) degree in Software Engineering from the MAKUT University India formerly WBUT, India in 2008. She also received the degree of Bachelor of Technology (B.Tech.) in CSE from the same university in 2005. She is presently pursuing her Ph.D in Computer Science & Technology at Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India.

AVIJIT BAIDYA is a student of JISCE pursuing Computer Science &Engineering. He has completed his Diploma from Gomati District Polytechnic, Tripura He was trained as an efficient computer science engineer; He is an elegant leader, a great Speaker and an expert in technicalities. Cryptography has always caught his interest and eventually he came out with bright colors with his new cryptographic algorithm.

SAJAL KUMAR BISWAS completed schooling from Bangladesh and is presently pursuing her B. Tech in CSE from JISCE Kalyani Nadia West Bengal. He is keen for research; his areas of interests include cryptography, network security.

SNEHARTHA DAM. Completed his secondary and higher secondary Kalyani public School. Now he is pursuing BTech in CSE from JISCE Kalyani Nadia West Bengal. His aim is to become a software engineer. Her areas of interest are network security, programming languages.

KABITA SINGHA has completed Diploma from Gomati District Polytechnic, Tripura. She is currently pursuing B.Tech CSE from JISCE Kalyani Nadia West Bengal She is keenly interested in Research work related to cryptographic algorithms. Her others areas of interest are web development and machine learning.

 https://doi.org/10.22362/ijcert/2020/v7/i07/v7i0704