Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 06, Issue, 07, pp.8753-8756, July, 2016

Full Length Research Article

TEXT ENCRYPTION AND DECRYPTION WITH EXTENDED EUCLIDEAN ALGORITHM AND COMBINING THE FEATURES OF LINEAR CONGRUENCE GENERATOR

[1,*]Solanki Pattanayak and [2]Dipankar Dey

[1]Assistant Professor, Haldia Institute of Management, (An Institution of ICARE), Haldia, Purba Medinipur,pin-721657, India
[2]Assistant Professor, Global Institute of Science & Technology,(An Institution of ICARE), (An Institution of ICARE), Haldia, Purba Medinipur, pin-721657

ARTICLE INFO

Article History:

Received 28th April, 2016
Received in revised form
27th May, 2016
Accepted 15th June, 2016
Published online 31st July, 2016

Key Words:

Encryption,
Decryption,
ASCII Value,
Secret Key,
Linear Congruence Generator,
Inverse Key.

ABSTRACT

Security plays a vital role in our communication system through internet. For this reasons, we protect data from unauthorized users using appropriate encryptions algorithm. Using encryption we convert plain text to cipher text using our proposed secret key and similarly using inverse key we can decrypt the original text. In this algorithm, we read a string, then extract each of the single characters from the string and convert these characters to ASCII equivalent value. Apply proposed secret key, along with ASCII value and appropriate encryption algorithm we encrypt the text. Similarly, using the inverse key along with appropriate decryption algorithm we can decrypt the original text.

INTRODUCTION

Encryption and decryption is the part of Cryptography. Cryptography is the term of Science and Arts, which generate the secret message and protecting this message from unauthorized access. Cryptography is the word, comes from Greek Origin, which means of "Secret or Hidden writing". The purpose and goals of cryptography are Confidentiality, Authentication, Data Integrity, Non-Repudiation and Access Control.

Key elements

Plain Text: The original message, known as plain text, which is input by the sender to the receiver.

Example- A sends the message "Hi" to B; this is considered as plain text. (Fig.1)

Corresponding author: Solanki Pattanayak,
Assistant Professor, Haldia Institute of Management, (An Institution of ICARE),Haldia, Purba Medinipur,pin-721657, India.

Cipher Text: The meaningless message, known as Cipher text, which is the output of encryption process. This message is difficult to understand by unauthorized users.

Example - "v4" is the cipher text of plain text "Hi", which is send by A to the receiver B.(Fig.1)

Encryption: Encryption is the process of converting message from plain text into cipher text, using encryption algorithm and secret key.

Decryption: Decryption is the process of converting messages from cipher text into plain text, using decryption algorithm and inverse key.

Secret Key: Using Extended Euclidean Algorithm, we can design our proposed secret key which can be used for encrypt the text message. Actually, more than 2000 years ago, this algorithm is developed by Euclid who was a mathematician.

This algorithm describe that the two integers a and b from it we can find the GCD of two numbers.

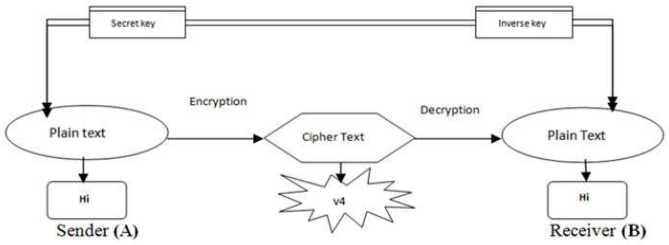


Fig. 1. Components of cryptography system

That is

gcd (a,b) = gcd (b,r) [where r is the remainder of dividing a by b.

If b is a prime number then remainder is always 1]

Inverse Key: Using Extended Euclidean Algorithm, we can generate the secret key, if b is prime number then we can get the inverse key by using Multiplicative Inverse Law. That is

$a \times b = 1 \pmod{n}$ [where a and b are the multiplicative inverse of each other and n is the prime number]

Message Confidentiality: Message confidentiality preserves the privacy of message between senders and receiver. Only the authorized receiver to know the meaning of the message. But except the receivers other recognized it meaningless message.

Message Integrity: Sender first broken the message into several tokens and send these tokens in random order. But receiver accepts these random tokens and arranges these tokens as sender's original message. The message integrity defines that without loss of any tokens, receiver rearranges the tokens as sender send original message. Actually message integrity defines the secure communication between sender and receiver.

Message Authentication: Message authentications define that sender's identity that he or she is the appropriate sender who sends the secure message. The receiver identifies the appropriate senders using message authentication process.

CLASSIFICATION OF CRYPTOGRAPHY

Cryptography divided into two parts:

- Symmetric Key Encryption
- Asymmetric Key Encryption

Symmetric Key Encryption

In symmetric key encryption, the secret key is shared between sender and receiver. The sender uses this key and use encryption algorithm to encrypt the text. Using the similar keys and a corresponding decryption algorithm, receive decrypt the original text.

Example: DES, BLOWFISH, AES, etc.

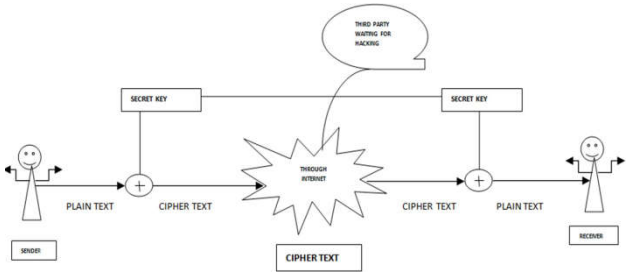


Fig. 2. Symmetric key encryption (Here secret key are shared between sender and receiver

Asymmetric Key Encryption

Asymmetric key encryption, is also known as public key cryptography. In this Encryption, two secret keys are used by sender and receiver, one is public key and another is private key. Sender used the public key to encrypt the text and receiver used the private key to decrypt the text.

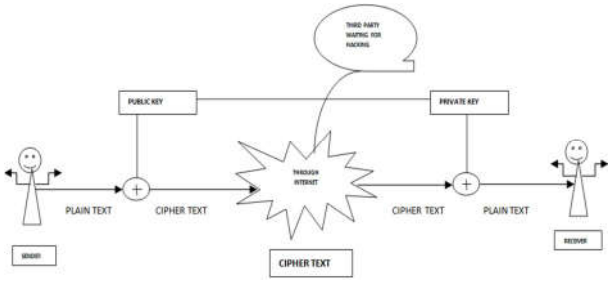


Fig. 3. Asymmetric key encryption

LITERATURE REVIEW

The comparative studies of other research papers are briefly stated below:

"An ASCII value based text data encryption system" [. Zeenat Mahmood, 2012], Udepal Singh, Upasna Garg proposed this algorithm. In this algorithm, they take an input text and then separate each character from input text and convert each character in ASCII equivalent numerical value. Then apply modulus operation and secret key on each ASCII value and convert new numerical value and then convert each numerical value to binary equivalent form and apply right shift operation on this binary value. Again convert this binary value to numerical form and numerical form convert to character form and then get the encrypted text using reverse key, they decrypt the text."Enhancing the security of DES algorithm Using Transposition Cryptography Techniques" [Venkateswaran and Sundaram, 2010], Sombir Singh,Sunil K. Maakar, Dr.Sudesh Kumar proposed this text encryption algorithm. DES concepts are implementing in this algorithm. They give the concept of 56 bit secret key and but when design the key they discard 8, 16, 24, 32,40,48,56 and 64 bits and used 48 bit key. For confuse

text, they used substitution concept. First they apply initial permutation on the input text.
Then divided text in two parts, one is left plain text and 2nd is right plain text. After that 48-bit secret key XOR with Right plain text and then used s-box (substitution) and p-box (permutation) to encrypt the text. Similarly, using reverse process they decrypt the text. "An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms" [Akanksha Mathur, 2012], Akanksha Mathur, proposed this data encryption algorithm. In this algorithm she implements an ASCII value based data encryption and data decryption technique. He used ASCII values for every encrypted data. Using secret key modified encrypted data into cipher text and another side also using this similar secret key to decrypted data into plain text. When he put the input, then each character shows his ASCII value. She used modulus operation on each ASCII content values and save the resultant in mod content array. Then find the min ASCII content values from the array. She took the binary values of each mod key and shifted this binary values using right circular shift 4 times. By following this process, he encrypts the data and similarly, using reverse process she decrypts the data.

"Information Security: Text Encryption and Decryption with poly substitution Method and Combining the features of Cryptography" [Sombir Singh et al., 2013], R. Venkateswaran, Dr. V. Sundaram, proposed this cryptography algorithm. They proposed a new Methodology using genetic algorithm. They used poly substitution method of genetic algorithm. In the plain Polyalphabetic substitution the text is enciphered differently. In this polyalphabetic method they used several two Keys, three Keys and random keys combination. They used three key, like e1, e2 and e3 and took ASCII value of e1 is 1 and e2 is 2 and e3 is 3. Then add the text. After that adding the ASCII value of e1 to the 1st character and ASCII value of e2 to the second character and e3 to the third character. Then they used poly substitution method of cryptography system for data by 3 keys. Same technique is used in decryption method by applying the reverse method.

PROPOSED WORK

- **Linear Congruence Generator**

The linear congruence generator is an algorithm that generates sequence of random number using piecewise linear functions. The functions become y = (ax + b) mod n [where a and b are secret key and n is a prime number] Here, if b=0 then it is called a multiplicative congruential generator (MCG) and if b not equal to 0 then it is called a mixed congruential generator. If anyone choose the values of a, c and n, then it is generated the random number between 0 to n-1.

- **Design Secret key for encryption**

We can design our secret key using Extended Euclidean Algorithm that is

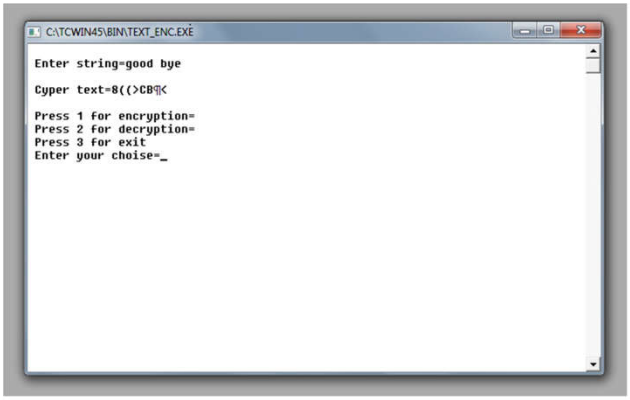
key1= (x * a) mod 131 [where a is an numerical value that equivalent to ASCII value form text and x is a random number that can generated by Linear Congruence Generator] The Extended Euclidean Algorithm determines the greatest common devisors or gcd between two integers. That is ax + by = gcd (a, b). This algorithm is useful if a and b are co-primes of each others. Here x and y is the modular multiplicative inverse between a and b. The Modular Multiplicative Inverse is used for find out the inverse of our proposed secret key. The method defines that a-1 ≡ x (mod m) where a-1 is the inverse of x where m is Integer module. Using this Modular Multiplicative Inverse we can generate inverse of our secret key.

- **Proposed algorithm for encryption**
  - Read the text message as an input
  - Extract each character from this text message and convert each of the character in ASCII equivalent numerical value.
  - Using Extended Euclidean Algorithm, generate our proposed secret key.
  - The proposed secret key is used to converting each of these ASCII values (these ASCII values corresponds to our text message) to new values.
  - These new values are again converting to characters.
  - These sequence of characters are combined to create the string
  - This string is actually the cipher text.
  - The cipher text now generate encrypted text message.

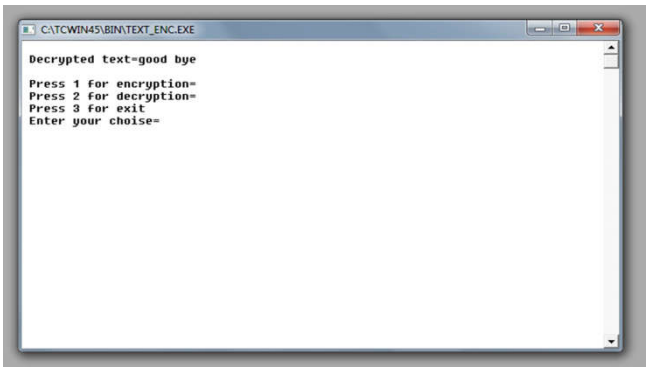
Using Modular Multiplicative Inverse algorithm we can generate inverse key of our proposed secret key. This inverse key and also appropriate decryption algorithm we can decrypt the cipher text back to original text message.

RESULTS

Examples of Text Encryption



Examples of Text Decryption



Conclusion

Our proposed algorithm is encrypting the text which can be used for further research in cryptography. This method is so easy but third party cannot hack our algorithms.

REFERENCES

Akanksha Mathur. 2012. "A Research paper: An ASCII value based data encryption with other symmetric data encryption Algorithms", *Intenational Journal on Computer Science and Engineering* (ISSN: 0975-3397), vol. 4 No. 09 Sep.

Behrouz A. Forouzan. 2008. TATA McGRAWHILL, "Cryptography & Network Security" p.- 20-69

Sombir Singh, Sunil K. Maakar, Dr. Sudesh Kumar. 2013. "Enhancing the Security of DE Algorithm Using Transposition Cryptography techniques", International Journal of Advanced Research in Computer Science and Software Engineering (ISSN: 2277 128X), vol. 3, Issue 6, June.

Udepal Singh, Upasna Garg. 2013. "An ASCII value based text data encryption System", International Journal of Scientific and Research Publications, vol. 3, Issue 11, November.

Venkateswaran, R. and Dr. Sundaram, V. 2010."Information Security: Text Encryption and Decryption with poly Substitution Method and Combining the features of Cryptography", International Journal of Computer Applications (0975-8887), vol. 3 – No. 7, June.

Zeenat Mahmood, J. L Rana, Prof. Ashis Khare.2012. "Symmetric Key Cryptography using Dynamic Key and Linear Congruential Generator (LCG)", International Journal of computer Applications (0975-8887), vol. 50-No.19, July.

****