Securing text through the use of Binary cipher algorithm under Asymmetric encryption strategy

Prof. Kiran M. Shinde
Lecturer
Institute of Industrial and Computer Management & Research,
(I.I.C.M.R.), Nigadi, Pune Pin. : 411044 Maharashtra, India
Affiliated to University of Pune, Recognized by AICTE
+9102027657648,
(Mobile) +919822796540, **(Mobile) +919822332275**
aadeoskar@rediffmail.com kiranfeelgood@sify.com

Abstract

Increasing boom in Information Technology sector increases security threats in network environment globally. Day by day there is increase in cyber crime. Statistical data shows the dangerous effects of cyber crimes with the invention & modernization of Information Technology. E transaction is the prime application used by today's B world. But keeping the transaction secured is still a challenging job. Several encryption & Decryption algorithms are used in various ways for the implementation of secured electronic transaction. But still hackers are able to crack the encryption logic. Existing Encryption & Decryption logic has their own pros & Cons. This paper highlights the existing simple encryption & decryption logic with their advantages & disadvantages. The paper is proposing a new encryption algorithm to get the secured transaction & confidential text. The proposed algorithm generates the secured key logic from source text itself.

Introduction

Encryption, Decryption technology is a way of securing any text by coding it through the use of some key. This process is known as Crypt analysis process. Any user who is unaware of the encrypted key cannot read encrypted data. To encode & decode any data encryption & decryption algorithms are required.

Figure 1 shows that sender sends a message, which is encrypted in to cipher text through encryption algorithm. This cipher text is then decrypted in to plain text. This encoding & decoding uses same key for conversion & is known as Symmetric conversion logic.

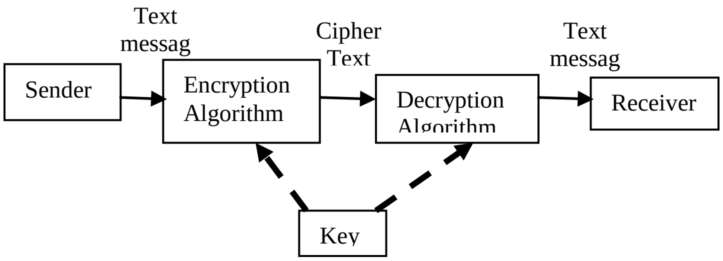
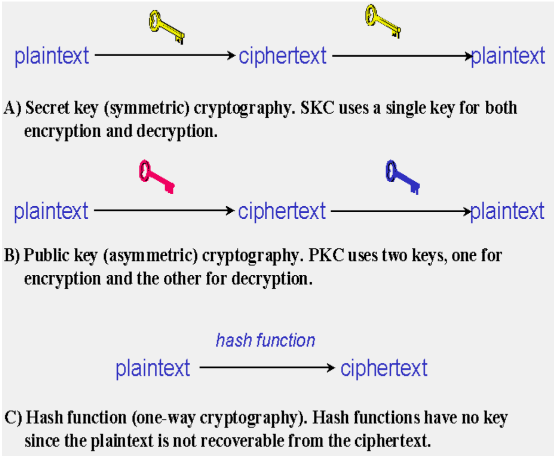


Fig. 1 : Encryption - Decryption concept (Key is shared by Sender & Receiver)

Symmetric encryption uses same key called as session key for encoding & decoding logic. Public Key encryption logic uses two separate keys called as public & Private key for encoding & decoding the data. Fig.1 shows three most commonly used cryptography algorithm categories :



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

FIGURE 2: Three types of cryptography: secret-key, public key, and hash function, source : Gary c. Kessler May 1998 (26 September 2005)

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
Hash Functions: Uses a mathematically calculated hash value to encrypt the data.

Need of Study

Technological evolution all over the globe has changed the working scenario. Message communication through electronically has replaced the paperwork everywhere. But this requires the security of such electronically communicated confidential text. Despite of existing algorithms hackers are able to crack the code. Types of Attacks on Encrypted Messages could be as mentioned below:

Types of attack	**Known to Cryptanalyst**
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known Plaintext	• Encryption algorithm • Cipher text to be decoded • One or more cipher text-plaintext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Cipher text to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Chosen cipher text	• Encryption algorithm • Cipher text to be decoded • Purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	• Encryption algorithm • Cipher text to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key • Purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Source: Cryptography & Network Security by William Stallings, Table 2.1

The paper highlights the existing algorithm under Symmetric Concept & proposes a new algorithm for encrypting the message.

Existing Algorithms in Symmetric Cipher Concept

Encryption is the process of converting plain text to coded text also known as Cipher text. Decryption is the logic of converting the cipher text back to the original plain text. This technique is known as Cryptography. Several algorithms have been introduced for Encryption & Decryption. Each of them have their advantages & disadvantages. Some of them are:

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
- One Time Pad
- Transposition Technique

- Steganography
- Blowfish

Caesar Cipher:

- Makes use of substitution technique that involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- But if this technique is known ,then a brute-force cryptanalysis is easily performed
- Three important characteristics of this problem enabled us to use a brute-force cryptanalysis
  - The encryption & decryption algorithms are known
  - There are only 25 keys to try
  - The language of plain text is known & easily recognizable

Monoalphabetic Cipher:

- Caesar cipher is far from secure , with only 25 possible keys
- Increase in the key space can be achieved by allowing an arbitrary substitutions
- Here different combinations of 26 characters i.e 26! Possible keys are used
- Compared to Caesar cipher brute-force techniques for cryptanalysis can be eliminated
- But if cryptanalyst knows the nature of the plaintext , then the analyst can exploit the regularities of the language
- Relative frequency of letters is used to break the cipher text into plain text

Playfair Cipher:

- Best known multiple letter cipher
- Treats diagrams in the plain text as single units & translates these units into cipher text diagrams
- Based on the use of 5*5 matrix of letters constructed using a keyword
- It is great advance over simple monoalphabetic ciphers, where instead of using 26 letters 26 * 26 = 676 diagrams are used to make identification of individual diagrams more difficult
- Frequency analysis is much more difficult with diagrams as compared to letters
- But still easy to break because it still leaves much of the structure of the plaintext language intact
- A few hundred letters of cipher text are generally sufficient

Hill Cipher:

- Another multiletter cipher is the Hill Cipher, developed by mathematician Lester Hill in 1929
- Takes m successive plaintext letters & substitutes for them m cipher text letters
- Substitution is determined by m linear equations in which each character is assigned a numerical value (a=0,b=1………,z=25)
- As with playfair, the strength of the Hill cipher is that it completely hides single letter frequencies
- With Hill the use of a larger matrix hides more frequency information
- But it can be easily broken with a known plaintext attack

Polyalphabetic Cipher:

- Another way to improve on the simple monoalphabetic cipher techniqueis to use different monoalphabetic substitution as one proceeds through the plaintext message
- Set of related monoalphabetic substitution rule is used
- A key determines which particular rule is chosen for a given transformation
- The algorithm used in this is referred to as Vigenere Cipher
- Set of related monoalphabetic substitution rules consist of 26 Caesar ciphers, with shifts of 0 through 25
- Each cipher is denoted by a key letter
- The strength of this cipher is that there are multiple cipher text letters for each plaintext letter , one for each unique letter of the keyword
- Thus the letter frequency information is obscured

One-Time Pad:

- An army Signal Corp officer, Joseph Mauborgne, proposed One-Time Pad technique.
- A random key with no repetitions produces random output that bears no statistical relationship to the plaintext.

- As the cipher text contains no information whatsoever about the plaintext , there is simply no way to break the code.
- The security of the one-time pad is entirely due to the randomness of the key. Because of this there are no patterns or regularities that a cryptanalyst can use to attack the cipher text.
- But there is a practical problem of making large quantities of random keys.
- For every message to be sent, a key of equal length is needed by both sender receivers. Thus a mammoth key distribution problem exists.

Transposition Techniques:

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher
- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed.

Steganography:

- A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.
- In this technique an arrangement of words or letters within an apparently innocuous text is used that spells out the real message.
- Various other techniques used under steganography are:
    - Character marking
    - Invisible ink
    - Pin punching
    - Typewriter correction ribbon
- Steganography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information, although using some schemes mention above may make it more effective.

Blowfish:

- Blowfish is a symmetric block cipher developed by Bruce Schneier.
- Blowfish was designed to have the following characteristics:
    - **Fast**: Blowfish encrypts data on 32-bit microprocessors at a rate of 18 clock cycles per byte.
    - **Compact**: Blowfish can run in less than 5K of memory
    - **Simple**: Blowfish's simple structure is easy to implement and eases the task of determining the strength of the algorithm.
    - **Variably secure**: The key length is variable and can be as long as 448 bits. This allows a tradeoff between higher speed and higher security.
- Blowfish encrypts 64-bit blocks of plaintext into 64-bit blocks of ciphertext.
- Blowfish is implemented in numerous products and has received a fair amount of scrutiny.
- The security of Blowfish is unchallenged.

Proposed Algorithm "Binarycipher"

The new proposed algorithm is based on symmetric model approach. It uses the text message itself as key for encrypting the data. This algorithm does not restrict only to 26 alphabets but may also consider any special character if any is there. The Binarycipher algorithm uses the concept of dividing the given text in two equal length sub string & then by applying the encryption logic (given below) among these substring we can get the cipher text.

Encryption Algorithm:

1. Read the message (S)
2. Get the length of message (n).
3. Check the value of n, if n is even divide it by 2. Separate out two sub matrix A & B of length 0 to (n/2) – 1 & (n/2) to

n-1 respectively. Interchange every even position letter of A with even position letter of B & retain the odd position letter as it is in A as well as B. Join the sub matrix A & B to get the cipher text.

4. If the length is odd then leave the nth letter as it is in S & consider the text size for encryption as n-1 then apply the algorithm specified in step 3. Join A & B Matrix with S to get the cipher text.

Example:

Plain text: **data transmission in intranet.**
Cipher text: oa antiatsaies.dnti rnnrmnsti

Decryption Algorithm:

1. Read the cipher text
2. Get the length of text (n).
3. Check the value of n, if n is even divide it by 2. Separate out two sub matrix A & B of length 0 to (n/2) – 1 & (n/2) to n-1 respectively. Interchange every even position letter of A with even position letter of B & retain the odd position letter as it is in A as well as B. Join the sub matrix A & B to get the cipher text.
4. If the length is odd then leave the nth letter as it is in S & consider the text size for encryption as n-1 then apply the algorithm specified in step 3. Join A & B Matrix with S to get the cipher text.

Example:

Cipher text : oa antiatsaies.dnti rnnrmnsti
Plain text : data transmission in intranet.

Main features of proposed algorithm

- Uses key from data itself
- Easy to understand but difficult to crack.
- With n (as length of text) number of iterations text can be encrypted & decrypted.
- Logic varies with the length of text.
- Same algorithm is applicable for decryption as well as encryption technology.

Conclusion

Securing the text is the prime need of today's era. The suggested algorithm provides a simple way for encrypting the text. Text may comprise of alphabets or any another special characters. The e-world & the B-world use electronic media for communication. The paper emphasis on the symmetric approach of encryption. It can be extended to implement the public encryption strategy in future.

References

1. Article on Encryption & Decryption Algorithm By Aloba Olumuyiwa B.
2. Article on Firewall by Olundegun Afeez O www.webopedia.com/
3. Cryptography & Network Security Principle & Practices By William Stalling
4. Information on Cyber crime on www.cybercrime.gov
5. Information on phishing & government security guides on www.antiphishing.org, www.schneier.com, www.governmentsecurity.org, www.spywareguide.com