Volume : 2 | Issue : 12 | Dec 2013 • ISSN No 2277 - 8160

Research Paper | Cryptography

Number Cryptography

C R S BHARDWAJ 33, first floor, BDA layout, HAL IInd stage, Kodihalli, 6th main, Bangalore

ABSTRACT

This research paper discusses the 'Number Cryptography' which is the alternate solution of the letters. We can convert the message into number form. It is the local modification of the message before the transmission. As we know that there are number of software available in the market which are used for the encryption and decryption. Some agencies have automatic decryption sets. These sets are used for the radio surveillance to decipher the message. Therefore safe and secure message can only be sent if before sending the message by the commercial Standard encryption techniques it is encrypted by using the number cryptography which is totally customized. In the number cryptography the very important message are numbered beforehand. During the transmission only numbers are transmitted with the operation of the key. The symmetric key can be used by the terminals. The sending of the message is safe on line than the wireless set.

KEYWORDS : Number cryptography, wireless link, encryption, commercial software

Introduction

The secrecy of the communications plays an important role in the business and army transactions. The progress of a person or an organization depends on the safety and security of online data communications. In modern times, for businesses and in the military wars there is a crucial and critical role of cyber security. The confidential information is passed on the Internet for the commercial purposes. The confidential information system is the key of success during the wars and trades. Various Symmetric-keys and asymmetric-keys type security protocols have been developed to get rid of the problems. Until you have something secret in your hand, it can be leaked anywhere in the middle during the transmission. The number Cryptography has been explained which is based on the above fact. The commercial encryption / decryption software can be used during the transmission after the number cryptography.

Symmetric-key encryption techniques Symmetric-key algorithms[1] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. Examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, and IDEA.

Asymmetric key encryption techniques

There are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented [5].

Pretty good privacy (pgp)

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. Current versions of PGP encryption include both options through an automated key management server [6].

Materials, apparatus and procedures

The procedures of encryptions which are explained above are not so reliable because they can also be decrypted by using the same software. The entire spy uses all types of commercial software to extract the information. Any encryption method is not secure because it has also decoding software. Once it is traced, your information can be decoded by your enemy. Till the information is not in your hand it can be leaked out certainly. If you are the first and last man to decode the information then sourly you will get through. Before transmission of the message it should be encrypted locally by using the local techniques. Some methods of number cryptography are given below.

Method 1:- The number can be encrypted by using the algebraic equations. Let x is the number any y is the key then we can use the following algebraic equations to transmit the message. After number cryptography the message can be transmitted by using any crypto software.

$(x + y)^2 = x^2 + y^2 + 2xy$. Let the number which is to be transmitted is x = 6, the key is y = 87, therefore, the number cryptography = $(6 + 87)^2$ = 8649. The formula $(x + y)^n$ can also be used where the value of x, y and n can be chosen as your wish.

(II) $x^2 + y^2$ and 2xy can also be used to encrypt any message.
(III) $x^n + y^n$ and n xy can also be used to encrypt any message.
(IV) $x^n - y^n$ and (n xy) can also be used to encrypt any message.
(V) $x^2 + y^2 + xy$ or $x^2 + y^2 - xy$ formula can also be used.

Method 2:- The number can be encrypted by using the algebraic indices. Let x is the number any y is the key and a is the base which can be assumed. Then we can use the following algebraic equations to transmit the message. After number cryptography the message can be transmitted by using any crypto software.

a^{m+n}, (ii) a^{m-n}, (iii) a^{mn}

Let a = 2, m = 7, n = 5 , then $a^{m+n} = 4096$, $a^{m-n} = 4$, $a^{mn} = 2^{35}$

Method 3:- We can change the text into numbers and then use the discriminant to modify the message before transmission. After reception the process can be reversed to get the plain text. The encryption formula is given below. $b^2 - 4ac$, where a is the message, b is the key and c is any constant. Let b = 11, a = 3 and c= 5, then $b^2 - 4ac = 11^2 - 4.3.5 = 61$

Method 4:- Plain text can be changed into numbers and the key can be thought separately according to the suitability of the situation and then the arithmetic progression and the geometric progression can be used to modify the message before transmission.

i) $l = a + (n-1)\,d$ (ii) $S = n/2\,(2a + (n-1)\,d)$, (iii) $l = a\,r^{n-1}$. The value of a, r, n and d can be assumed as per the suitability.

Method 5:- Plain text can be changed into numbers and the key can be thought separately according to the suitability of the situation and then the matrix can be formed to modify the message before transmission. The inverse of the inverse is the original matrices. Transpose of the matrices can also be sent as the transpose of the transpose matrix is the original matrix. Transpose of a matrix means the reflection of the elements along the diagonal. The transpose of the transpose of matrix is the original matrix. A square matrix will remain square matrix after the operation of transpose. The transpose of the sum of two matrices is

equal to the sum of transpose of one matrix and transpose of another matrix. The inverse of A is only when the product of A and is I. I mean identity matrix which has same number of rows and columns. To find the inverse of the matrix A, its magnitude and adjoint are to be found out. The inverse or reciprocal of A is equal to the ratio of the adjoint and the magnitude of the matrix.

If A = is a non singular square matrix, then thus if A =

$$= \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \text{ then}$$

$$\text{Adj A} = \begin{bmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{bmatrix}$$

$$\text{and } A^{-1} = \frac{1}{|A|} \times \begin{bmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{bmatrix}$$

Implementation:-To implement the number cryptography, sake hand technique is required. The practice is required before the implementation of the plan. A confidential book of very secret message can be prepared well in advance. In number cryptography there is not the requirement of the software. The technique can be prepared well in advance to train the manpower. These technologies can also wok in the adverse condition when the commercial links are in the jammer scan or direction finder scan.

Discussion:

- The number ends cryptography is known to the ends that is why it is better than the other commercial methods. The preference of symmetrical encryption over asymmetric encryption is because of its 100 times faster speed.
- Here only one message is transmitted on the entire network and the problem of key distribution has been resolved as the key is distributed in advance. Those keys are basically the codes that are prepared locally. By looking at the serial numbers in the booklet, password can be modified/ changed on daily basis.
- Symmetric keys are vulnerable to intruders. Intruders try to break the key by applying a systematic sequence of keys. As we are using number ends cryptography, there is no way to pick up the actual signals during the transmission by the intruders.
- In this method the password booklet are issued before hand for a month. The exchange of password booklet is done face to face to avoid any threat of intruders. New booklet can be issued for new months.
- The number end cryptography works well with telephone lines, radio sets and mobile services. Number end cryptography with mobile services could be great help during war where quick decisions need to be taken.
- The significance of number end cryptography comes into picture during wars as well as business transactions as they both need high end security and each message has its own importance.

Limitations

1. Number end cryptography is a complex process as the message is in cipher form and to decipher a proper person is required.
2. The members on each terminal should be aware of using number end cryptography. Otherwise it is difficult to decrypt the messages.

Conclusion

The number cryptography is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. A complete secrecy of the message can be ensured if only two parties are involved in the communication. The commercial cryptography is not successful as everybody has got its software. Some radio sets can automatically search the stations and then convert it into plain text. The number cryptography enables you to send the secure data between two computers on private wireless link. It ensures user authentication, bandwidth sharing, and security from eavesdropping and immunity to interference, and difficulty in detection.

REFERENCES

1. Delfs, Hans & Knebl, Helmut (2007)."Symmetric-key encryption". | 2. Belfield, R. (2007). The Six Unsolved Ciphers: | 3. Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press. | 4. Electronic Frontier Foundation. (1998). | 5. Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). |