ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 9, November 2012

POLY HYBRID CRYPTOGRAPHY

CRS BHARDWAJ

Hno. 1195, GRC Road, Modibada, Jabalpur (Mp)

Mobil No 9303149367,

Abstract *-- This research paper discusses the Poly Hybrid Cryptography which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. It is the combination of many cryptographic techniques which ensure the security at the terminal ends and security during transmission over wireless as well as on the internets. Poly cryptography can also be used on mobile communication. Random numbers are used to spread the message during transmission. The original message cannot be detected by using any technique. This technique can be used during the wars.*

Keywords: wireless communication, security, Random numbers, poly cryptography .internet.

Introduction

Encryption fundamentally consists of scrambling a message so that its contents are not readily accessible while decryption is the reversing of that process. These processes depend on particular algorithms, known as ciphers. Curiosity is one of the most common human traits, matched by the wish to conceal private information. Spies and the military all resort to information hiding to pass messages securely, sometimes deliberately including misleading information. Encryption fundamentally consists of scrambling a message so that its contents are not readily accessible while decryption is the reversing of that process. These processes depend on particular algorithms, known as ciphers. Suitably scrambled text is known as cipher text while the original is, not surprisingly, plain text. Readability is neither a necessary nor sufficient condition for something to be plain text. The original might well not make any obvious sense when read, as would be the case, for example, if something already encrypted were being further encrypted. It's also quite possible to construct a mechanism whose output is readable text but which actually bears no relationship to the unencrypted original. A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant, the functionality of a key lies in its being a string of bits determining the mapping of the plain text to the cipher text. Protecting access to information for reasons of security is still a major reason for using cryptography. However, it's also increasingly used for identification of individuals, for authentication and for non-repudiation. This is particularly important with the growth of the Internet, global trading and other activities. The identity of e-mail and Web users is trivially easy to conceal or to forge, and secure authentication can give those

interacting remotely confidence that they're dealing with the right person and that a message hasn't been forged or changed. [1]

Symmetric-Key Encryption Techniques

Symmetric Encryption (also known as symmetric-key encryption, single-key encryption, one-key encryption and private key encryption) is a type of encryption where the same secret key is used to encrypt and decrypt information or there is a simple transform between the two keys.

A secret key can be a number, a word, or just a string of random letters. Secret key is applied to the information to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. Symmetric algorithms require that both the sender and the receiver know the secret key, so they can encrypt and decrypt all information. In any symmetric-key encryption technique, both encryption and decryption process are carried out using a single key. These algorithms are efficient, are secure, execute at high speeds, and consume less computer resources of memory and processor time. However, symmetric key cryptographic techniques suffer from the disadvantages of Key distribution problem, Key management problem and inability to digitally sign a message. Despite these drawbacks, numerous secure symmetric key encryption algorithms such as following have been developed. AES/Rijndael,Blowfish,CAST5,DES,IDEA,RC2,RC4,RC6,Serpent,TripleDES,Twofish,TDES, AES [2]

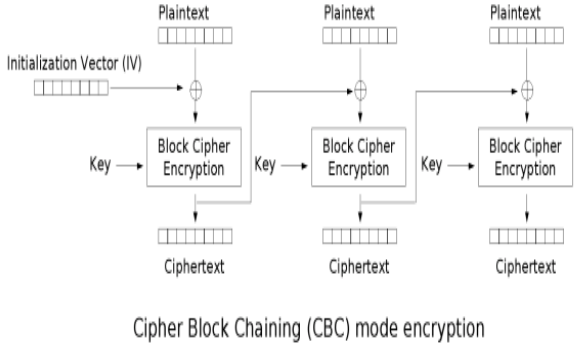


Figure1: Symmetric key encryption method

Asymmetric Key Encryption Techniques

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which 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.[3]

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. The problems associated with symmetric-key cryptographic techniques were solved when asymmetric encryption mechanism was implemented. Here, instead of a single key, every person has a pair of keys. One key, called the public key is known to everyone and the other one,

the private key is known only to the owner. There is a mathematical relationship between both these keys. Thus, if any message 'm' is encrypted using any of the key, it can be decrypted by the other portion. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented. [3]

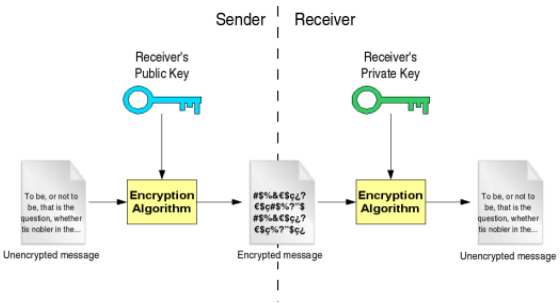


Figure2: Asymmetric key encryption method

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication f or 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. It was created by Phil Zimmermann in 1991.PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and, finally, public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server. [4]

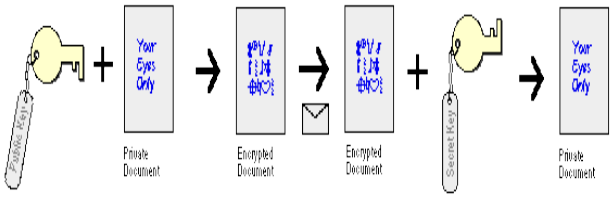


Figure3: PGP encryption method

MATERIALS, APPARATUS AND PROCEDURES

Poly Hybrid Cryptography Using Random Numbers

We can prepare a list of important message in advance. Both the parties (sender & receiver) will share the same list. Lists are kept confidential. The sequence of the list can be changed when required For Example

Random Numbers	**Message**
3740239	Send Ration
7865231	Ammunition
4921805	persons
2649764	Fighter
6652109	Tanks
2124560	Vehicle

And so on

Figure4: Secret table

Explanation of the diagram:

1. Enter the plain text.
2. Find the equivalent random number of the plain text.

3. Encrypt the equivalent random number by using symmetric key encryption.
4. More than one key can be used for encryption.
5. Encrypted message can be spread by using the random numbers.
6. Encrypted message can be transmitted over the wireless or wired channels.
7. At receiving side the process is reversed.

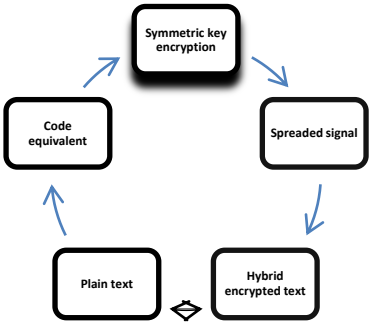


Figure5:- Poly Hybrid encryption /decryption

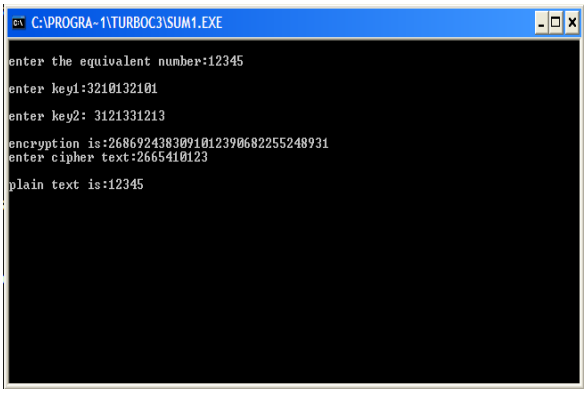


Figure 6: Face diagram of encryption /decryption using random numbers

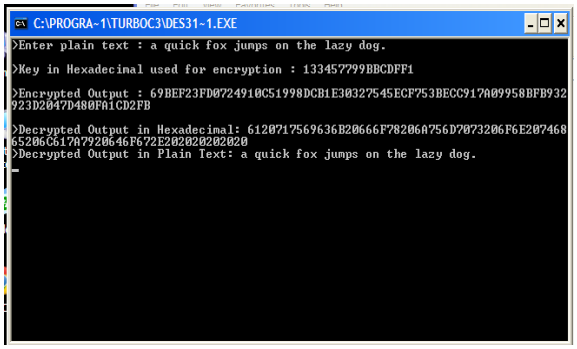


Figure 7:.Data encryption standard by using random numbers

Poly Hybrid encryption is implemented by using hexadecimal numbers. Program is coded in hexadecimal numbers. Implementation means install the software to the destination and make it to work there. Implementation is an ongoing process and can be achieved by one of the following methods:

1. The implementation of dissertation is carried out in language “c” because of the following advantages.
2. C is a building block for many other currently known languages.
3. C is a compiled language versus an interpreted language.
4. A lot of libraries are written in C.
5. The main advantages of C language are that there is not much vocabulary to learn, and that the programmer can arrange for the program is very fast.
6. C has features that allow the programmer to organize programs in a clear, easy, logical way.
7. C is a portable language.

ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 9, November 2012

Implementation of Poly Hybrid Cryptography

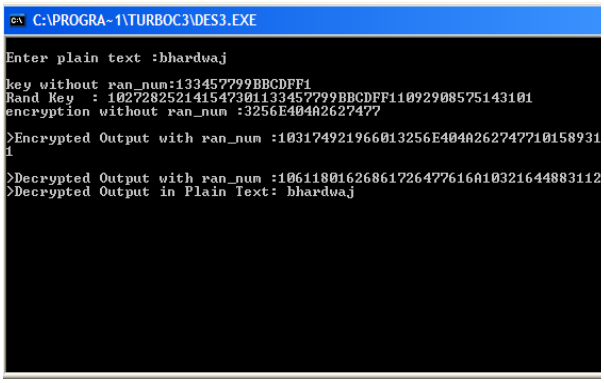
```
#include<stdio.h>

#include<conio.h>

#include<malloc.h>

#include<math.h>

# define COMPUTATION
```

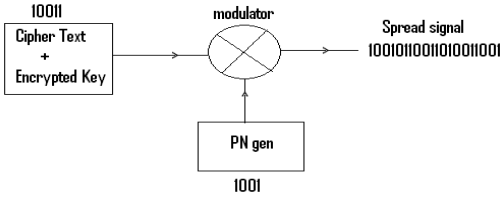


Comparision of both encryptions (DES and DES using random numbers) has been shown in the face diagram. Clearly the modification of DES program by random number is not understandable.

Transmission of Message

Cryptography has two main parts. First part deals with the cryptography at terminal ends. Second part deals with the secrecy during the transmission. To maintain secrecy at the terminal ends, Hybrid Cryptography (symmetric key and PN Generator random number) is used to encrypt the plain text and then PN Generator is used to spread the message.

To encrypt the plaintext symmetric key and PN Generator random number are used.



As shown in the diagram. The other input to the modulator is the PN gen. PN Sequence Generator block generates a sequence of pseudorandom binary numbers. Let the input to the modulator is 10011. Let the PN gen chip rate is 1001.The output of the modulator for the input bits 10011 will be 10010110011010011001 as shown in the diagram

Result and Discussion

1. Asymmetric Encryption is 100-1000 times slower than symmetric algorithms (RSA v. DES). Only code is transmitted. Actual message lies at the terminal ends. Code can be transmitted faster than asymmetric Key.
2. The problem of distributing keys is solved because the codes are prepared locally. One person can have unlimited numbers of codes for different unlimited users. (A booklet of passwords can be prepared in advance and should be kept under lock and key. password may be changed daily by referring the serial numbers of the booklet).
3. Symmetric keys are subject to a brute force attack where all keys in the key space are tried systematically to break the encryption. As we are using Customized advance cryptography, there is no chance to pick up the actual signals during the transmission by the intruders.

4. Distribution of keys becomes a problem, especially if keys change frequently. Keys must be transmitted with extreme security because they allow access to all the information encrypted with them. For applications that extend throughout the world, this can be a very complex task.
   Face-to-face key exchange is done. One booklet may contain passwords for one month. After one month another booklet of password is issued.
5. An alternate solution of hybrid cryptography has been found to increase the speed and to decrease the memory size requirement. Poly Hybrid encryption is the better solution which ensures secrecy at terminal ends and during the transmission of the text.

6. Poly Hybrid encryption is very important during the wars where each message has its own value. It is also important in business transactions.

Poly Hybrid encryption ensures user authentication, bandwidth sharing, and security from eavesdropping and immunity to interference, and difficulty in detection, data encryption and key management.

Limitations

1. Using Poly Hybrid encryption can be a complex process and its concept is often difficult for some people to grasp.
2. Both parties must be able to use Poly Hybrid encryption. It is impossible to use Poly Hybrid encryption unless people at both ends are capable of using this.

Conclusion

This research paper discusses the Poly Hybrid Cryptography which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. It is the combination of many cryptographic techniques which ensure the security at the terminal ends and security during transmission over wireless as well as on the internet. Poly cryptography can also be used on mobile communication. Random numbers are used to spread the message during transmission. The original message cannot be detected by using any technique. This technique can be used during the wars

References

1) Bamford, J. (1983). The Puzzle Palace: Inside the National Security Agency, America's most secret intelligence organization. New York: Penguin Books.
2) Barr, T.H. (2002). Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall.
3) Bauer, F.L. (2002). Decrypted Secrets: Methods and Maxims of Cryptology, 2nd Ed. New York: Springer Verlag.
4) Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.
5) Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press.
6) Electronic Frontier Foundation. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics