INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

PN Generator Cryptography

CRS Bhardwaj
Modibada, Jabalpur, MP, India

Abstract: *This dissertation discusses PN Generator cryptography, which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. A random number is generated by PN Generator which is used as a key to encrypt the message.PN Generator can also be used to spread the encrypted message as per requirements to increase the difficulty for any intruder. It is a technique in which source code is modified to encipher the plain text. Source code includes ASCII Code, binary code, octal code, hexadecimal numbers and decimal numbers. One code can be converted into another code.PN Generator produce the infinite random numbers which can be used as the key to reencrypts the ciphertext. It enables you to send the secure data between two computers on private wireless link.*

Keywords: *Wireless communication, security, pseudorandom generator, cryptography.*

Introduction

This being the age of Electronics & Information Technology, majority of the information of large enterprises is maintained on machines in the form of data. This information is very sensitive & several mission critical applications depend upon this information. Any intruder who may get access to this information can not only leak the information but also alter/tamper this information which can lead to malfunctioning of the defense/mission-critical systems. This certainly can create havoc to the future of such organizations & nations. Thus information hiding is a must – so that information does not get (mis)interpreted and never leaked out and also protected at all costs from any kind of tampering. So, my aim is to provide a cryptographic system with uses of different type of cryptographic algorithms. The PN Sequence Generator block generates a sequence of pseudorandom binary numbers. A pseudo noise sequence can be used in a pseudorandom scrambler and descrambler. It can also be used in a direct-sequence spread-spectrum system. A random number is generated by PN Generator which is used as a key to encrypt the message.PN Generator can also be used to spread the encrypted message as per requirements to increase the difficulty for any intruder. It is a technique in which source code is modified to encipher the plain text. Source code includes ASCII Code, binary code, octal code, hexadecimal numbers and decimal numbers. One code can be converted into another code.PN Generator produce the infinite random numbers which can be used as the key to reencrypts the ciphertext. It enables you to send the secure data between two computers on private wireless link.

Literature Review

Cryptography is the science of mathematics to "encrypt" and "decrypt" data. Cryptography enables us to store sensitive information or transmit it across insecure networks like Internet so that no one else other the intended recipient can read it. Cryptanalysis is the art of breaking Ciphers that is retrieving the original message without knowing the proper key. Cryptography deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications. Today, various cryptographic algorithms have been developed. These are broadly classified as symmetric key (DES, TDES, Blowfish, CAST, IDEA, RC4, RC6, AES) and asymmetric key (RSA, ECC) algorithms.

Private Key Cryptography

In private-key cryptography, the sender and recipient agree beforehand on a secret private key. The plaintext is somehow combined with the key to create the ciphertext. The method of combination is such that, it is hoped, an adversary could not determine the meaning of the message without decrypting the message, for which he needs the key.

The following diagram illustrates the encryption process:

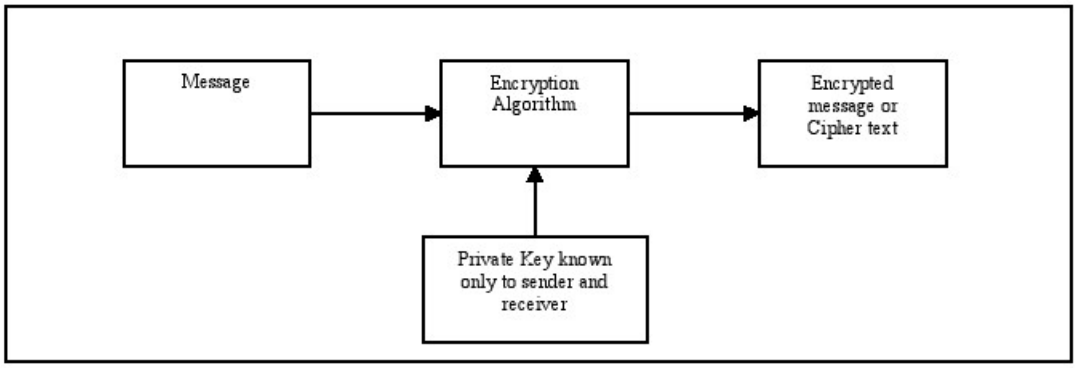

Figure : 1

The following diagram illustrates the decryption process:

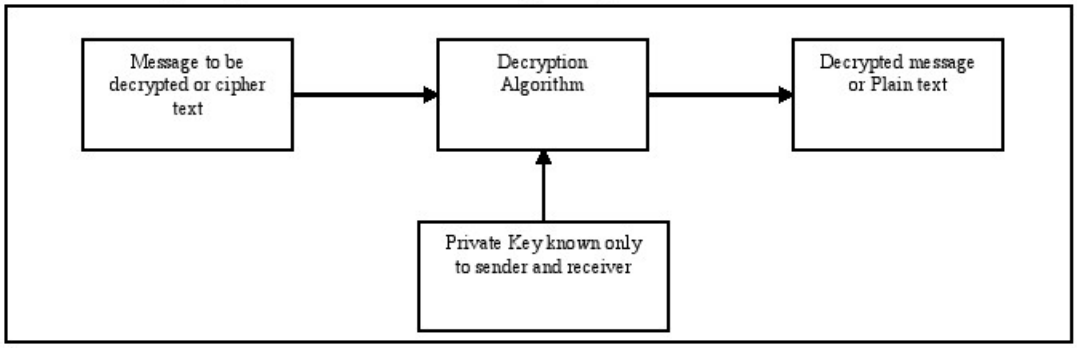

Figure: 2

To break a message encrypted with private-key cryptography, an adversary must either exploit a weakness in the encryption algorithm itself, or else try an exhaustive search of all possible keys (brute force method). If the key is large enough (e.g., 128 bits), such a search would take a very long time (few years), even with very powerful computers. Private-key methods are efficient and difficult to break. However, one major drawback is that the key must be exchanged between the sender and recipient beforehand, raising the issue of how to protect the secrecy of the key. When the President of the United States exchanges launch codes with a nuclear weapons site under his command, the key is

accompanied by a team of armed couriers. Banks likewise use high security in transferring their keys between branches. These types of key exchanges are not practical, however, for e-commerce between, say, amazon.com and a casual web surfer.

Public Key Cryptography

Public Key cryptography uses two keys Private key (known only by the recipient) and a Public key (known to everybody). The public key is used to encrypt the message and then it is sent to the recipient who can decrypt the message using the private key. The message encrypted with the public key cannot be decrypted with any other key except for its corresponding private key. The following Diagram illustrates the encryption process in the public key cryptography

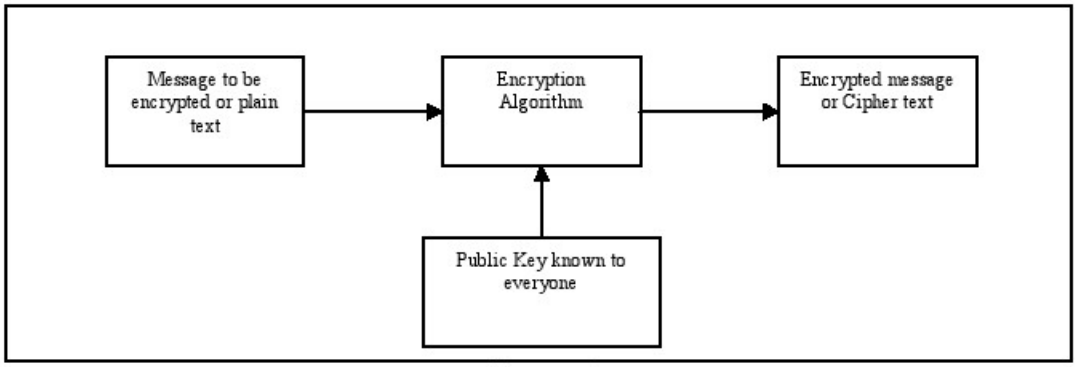

Figure 3

The following diagram illustrates the decryption process in the public key cryptography:

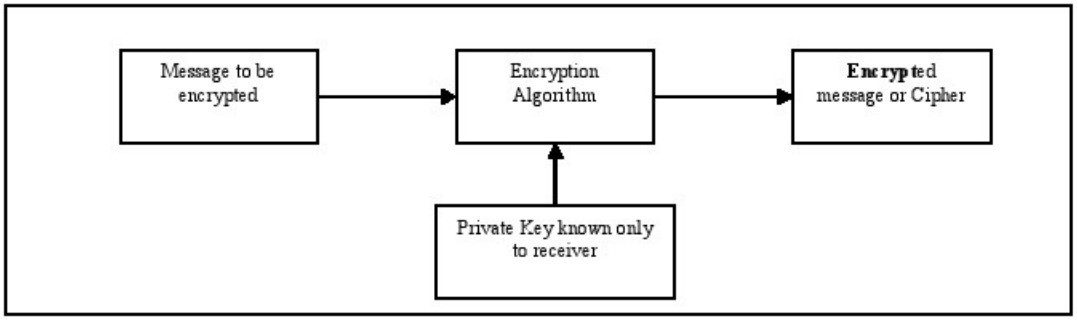

Figure 4

The public-key algorithm uses a one-way function to translate plaintext to ciphertext. Then, without the private key, it is very difficult for anyone (including the sender) to reverse the process (i.e., translate the ciphertext back to plaintext). A one-way function is a function that is easy to apply, but extremely difficult to invert. The most common one-

way function used in public-key cryptography involves factoring very large numbers. The idea is that it is relatively easy to multiply numbers, even large ones, with a computer; however, it is very difficult to factor large numbers.

Materials, Method & Procedure

To encrypt the plaintext symmetric key and PN Generator random number are used to encrypt the plain text and then password is used to encrypt the symmetric and session keys. Once the data is encrypted, the session key and the key produced by PN generator is then stored in different files. These files are encrypted to the recipient's password. One time keypad is recommended for password.

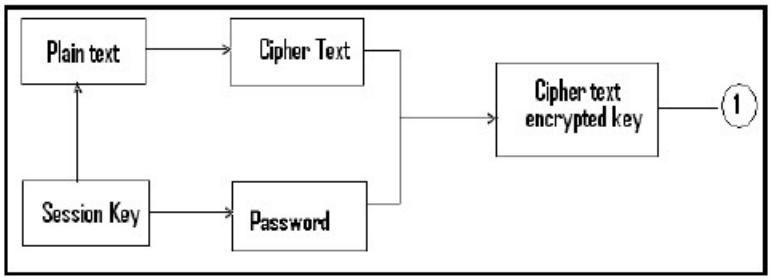

Figure 5

This password encrypted session key is fed along with the cipher text to the input of modulator. 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 4.2.

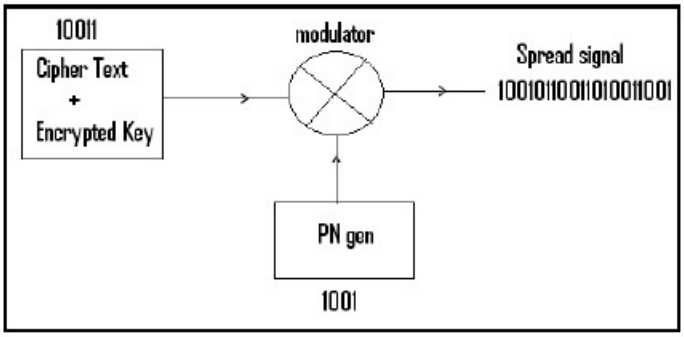

Figure 6

Thus the sender sends a) Cipher text of the message, b) Cipher text of the session key. The receiver upon receiving a) Cipher text of the message, b) Cipher text of the session key, and first decrypts the Cipher text of the session key to obtain the session key. This is then used to decrypt the cipher text of the message to obtain the plain text. This hybrid algorithm is a combination of symmetric and password encryption techniques.

PN Generator produces the infinite random numbers which can be used as the key to encrypt the plain text. Customized PN Generator Hybrid cryptography using PN Generator ensures user authentication, the ability to selectively address, bandwidth sharing, and security from eavesdropping and immunity to interference, and difficulty in detection.

Implementation

```
#include <stdio.h>
#define SHR_LENGTH 4
#define COMPUTATION 1
```

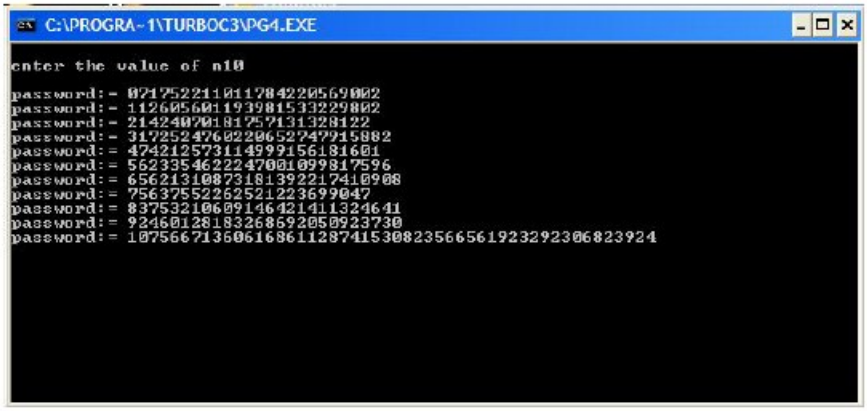

Figure 7: Face diagram of password generator

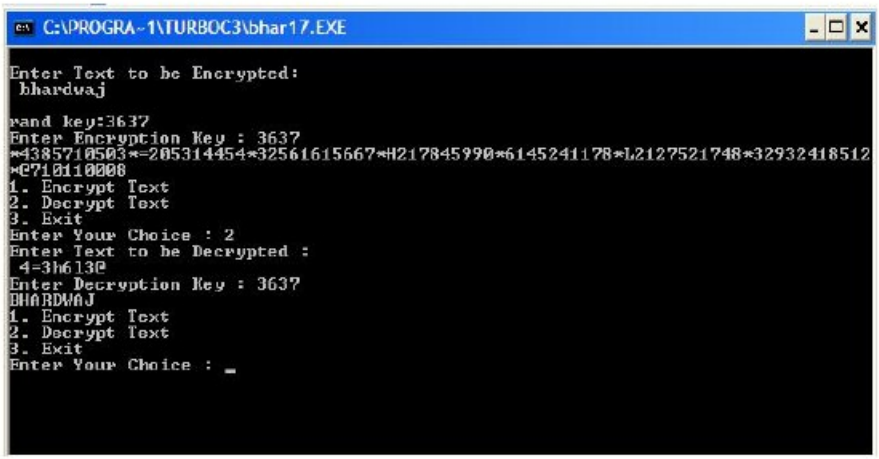

Figure 8: Encryption of text using random number

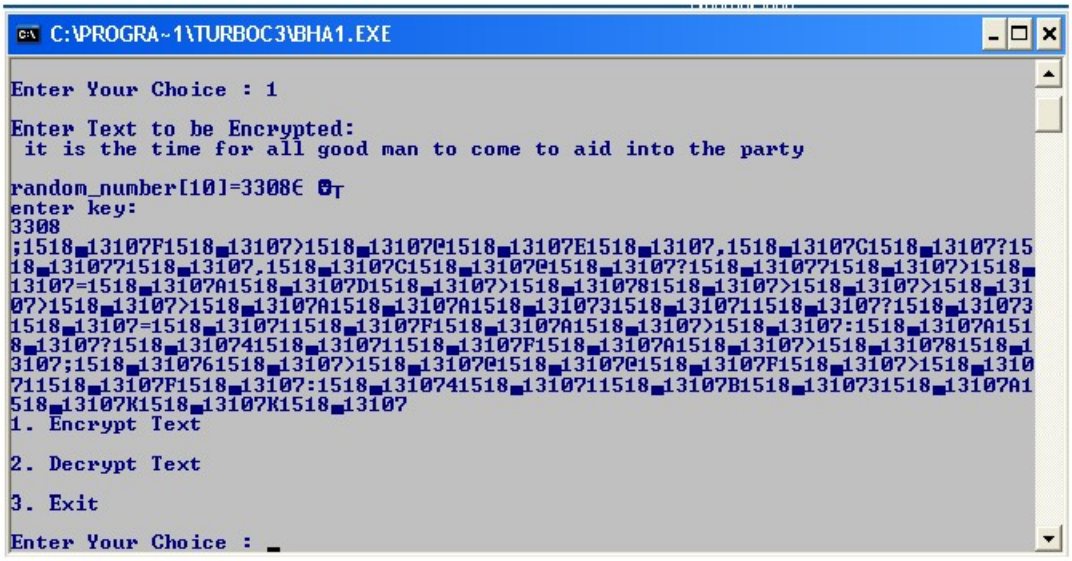

Figure 9: Encryption of text using random number

Implementation means install the software to the destination and make it to work there. The implementation of dissertation is carried out in language "c" because of the following advantages.

1. C is a building block for many other currently known languages.
2. C is a compiled language versus an interpreted language.
3. A lot of libraries are written in C.
4. 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.
5. C has features that allow the programmer to organize programs in a clear, easy, logical way.
6. C is a portable language.

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 PN gen 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 PN gen 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. Customized PN gen Cryptography is the better solution which ensures secrecy at terminal ends and during the transmission of the text.
6. It is very important during the wars where each message has its own value. It is also important in business transactions.
7. Customized PN gen cryptography 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 PN Gen Cryptography can be a complex process and its concept is often difficult for some people to grasp.
2. Both parties must be able to use PN Gen Cryptography. It is impossible to use PN Gen Cryptography unless people at both ends of the connection are capable of using this.

Conclusion

This dissertation discusses PN Generator cryptography, which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. A random number is generated by PN Generator which is used as a key to

encrypt the message.PN Generator can also be used to spread the encrypted message as per requirements to increase the difficulty for any intruder. It is a technique in which source code is modified to encipher the plain text. Source code includes ASCII Code, binary code, octal code, hexadecimal numbers and decimal numbers. One code can be converted into another code.PN Generator produce the infinite random numbers which can be used as the key to reencrypts the ciphertext. It enables you to send the secure data between two computers on private wireless link.

Acknowledgement

I take great pleasure in recording a sincere gratitude and immense heartfelt thanks to the people who helped me in completing this dissertation by giving me their valuable time and guidance. I would like to acknowledge all of them. I would like to thank **Prof.** Rajesh Kumar Pandey for his guidance and help. His constant inspiration and timely suggestions helped me in collection all the information I needed for my dissertation without much difficulty. I also want express my feelings towards all the staff members of Computer Science and Engineering Department and towards all those who have continuously motivated during preparations of the dissertation. Finally, I am highly obliged to all my family members for their support and blessings.

Reference

1. Overview of Cryptography by Alfred J. Menezes
2. M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis. Cryptography—G. Julius Caesar
3. M. Abdalla, M. Bellare, and P. Rogaway.
4. S. S. Al-Riyami and K. G. Paterson.
5. Schneier, Bruce (1995-10-09). Applied Cryptography. New York:
6. Schneier B. Applied Cryptography. John Wiley & Sons Inc., New York, New York, USA, 2nd edition, 1996.
7. Stallings W. Cryptography and Network Security. Prentice Hall, Upper Saddle