A Novel Method for Symmetric Encryption using Split Plaintext Key Pair *(Pi,Ki)* Algorithm

Renjith PR
Department of Computer Science
Rajagiri College of Social Sciences
Cochin, Kerala, India

Arun Sojan
MCA Student
Rajagiri College of Social Sciences
Cochin, Kerala, India

Praseeda K Gopinadhan
MTech (Information System Security) Student
IGNOU India

ABSTRACT
Cryptography, defined as the science and study of secret writing, concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only intended people can see the real message. In this paper, we propose the design and implementation of a new symmetric key algorithm. The algorithm encrypts the plaintext file by using the password of the file as the key. The plaintext and key are split in equal numbers and shift cipher is applied to each block of the plaintext. This new algorithm can be considered as a hybrid approach to its precursors.

General Terms
Information security, cryptography

Keywords
Symmetric cryptosystem, information security, split-plaintext-key pair

1. INTRODUCTION
The ideology of cryptography was introduced earlier, where confidential messages were sent as cipher text [1]. Cryptography is still growing and research is still alive for new cryptography algorithms. There are several cryptographic algorithms that can be as simple as shift cipher or as complex as DES etc. In almost all the cryptographic algorithms, either the plain text is encrypted using key or it is divided into small chunks and applies the same key. In this paper, we propose a novel symmetric cryptographic algorithm that splits the plaintext as well as the key in equal numbers and applies the split key on the corresponding split plaintext. Here the number of splits is determined by a random number generator algorithm. The input to the crypto algorithm is a file (the plaintext) and its password (the key).

1.1. Cryptographic goals of the algorithm
The major objectives of cryptography are

- Confidentiality which deals with the secrecy of the message
- Integrity which deals with the correctness of the content message
- Authentication which deals with the identity of the sender
- Non-repudiation deals with non-denial of sending of the message

This algorithm preserves the basic three properties of cryptography namely confidentiality, integrity and authentication.

1) Confidentiality
The plaintext is encrypted by a symmetric key (i.e. the password of the file). The key is kept secret and no one is able to decrypt the cipher text by using another key. This serves confidentiality.

2) Integrity
The encrypted file can be decrypted only by the same key to enforce integrity.

3) Authentication
Symmetric key makes the sender and receiver share a common key. The authenticated parties who know the key will only be able to decrypt and see the contents of the message [2].

2. SPLIT PLAINTEXT KEY PAIR (Pi,Ki) ALGORITHM
The algorithm uses the password to encrypt the file with a unique number that creates the unique encrypted text file. The same password is use to decrypt the file thus enabling maximum security of the file. Let us now see the algorithm in detail.

The plaintext for the algorithm is a file that contains some text information and the key is the password of the file. The algorithm computes a random number from the password to generate the key. The number of letters and ASCII value of key determines the number of splits of key and plaintext. The key and plaintext are split equally. Let the plaintext P be split into p1,p2, p3…pn & let the key K be split intok1,k2,k3…kn. The

pairs (p1,k1), (p2,k2), (p3,k3)…(pn,kn) undergoes encryption. For a pair (pi,ki) called as split plaintext key pair, pi is encrypted by the key ki.

The algorithm uses shift cipher is used to create the cipher text. The shift cipher is applied on each split plaintext key pair to get the corresponding cipher text. These cipher texts are combined to get the final cipher text. Figure 1 shows the flowchart on the encryption side.

2.1. Algorithm

The encryption is done through the following steps

Step 1 : Start.

Step 2 : Accept file name and password.

Step 3 : Generate unique random number from the password, which serves as the key.

Step 4 : Split the plaintext and the key into n splits.

Step 5 : Encrypt the first split of the plaintext with the first split of the key, second split of plaintext with second split of key and so on.

Step 6 : Combine the splits to get the cipher text

Step 7 : Stop

2.2 Flowchart – encryption

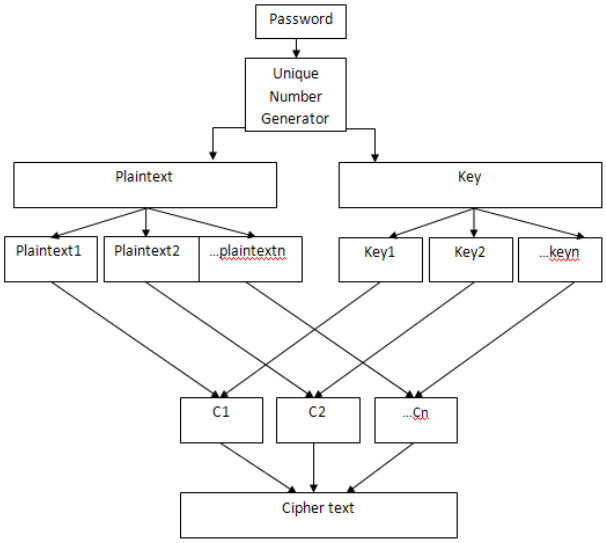
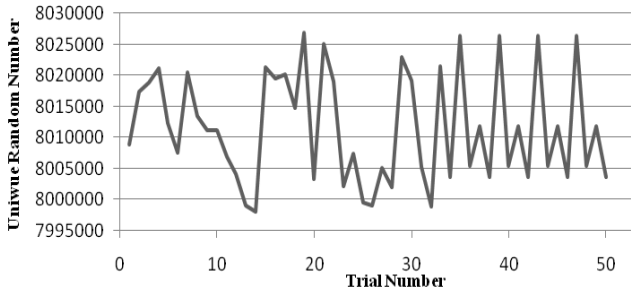


Figure 1: Split-plaintext-key pair algorithm –Encryption

2.3. Unique number generation

The unique random number is generated from the password i.e. the key. Each letter of the password is converted to ASCII. Depending on the number of characters of the key as well as the ASCII value of each character a unique number 'n' is generated. This unique number 'n' represents the number of splits on the plaintext and key. Figure 3 illustrates the randomness of the unique random number generator for 50 trials. For each trial a password is entered and a random number is generated.

Figure 3: Number of trials v/s randomness generator



2.5. Decryption

By applying the unique number generation, the password of the file (symmetric key) is divided to get the number of splits. The key and cipher text are split accordingly. The split key is applied on the corresponding split cipher text (i.e ith key split is applied on ith cipher text) for decryption. Combine the plaintext splits to complete the decryption process as shown in Figure 2.

2.2 Flowchart – decryption

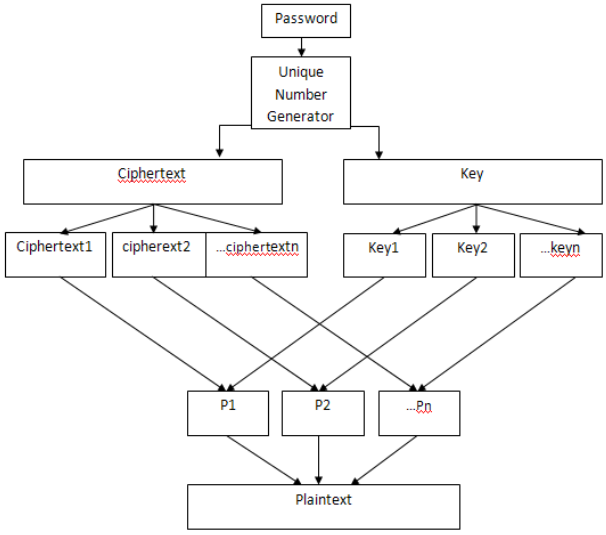


Figure 2: Split-plaintext-key pair algorithm –Decryption

3. ACKNOWLEDGEMENTS

The author would like to thank his students Arun Sojan, Bibin Vargese, Priya Jose, Milan Varghese and Meenu Thankachan for their valuable contribution

4. CONCLUSION

In this paper, a new symmetric encryption algorithm is presented. The algorithm uses the concept of splitting the plaintext and key equally and applies shift cipher for encryption. It needs a secured channel to exchange the key between the sender and receiver. It follows a new hybrid approach of splitting the plain text and the key.

5. REFERENCES

[1] William Stallings, "Cryptography and Network Security" 4th Edition. Pearson Education Inc, Upper Saddle River, New Jersey, 2006.

[2] Christopher Paar, Jan Pelzl, Bart Preneel,"Understanding Cryptography- A Textbook for Students and Practitioners", Springer, Berlin Heidelberg 2010.

[3] Aruljothi, S. Venkatesulu, M.R. Nicole, "Symmetric Key Cryptosystem Based on Randomized Block Cipher", Future Information Technology (FutureTech), 2010 5th International Conference