Journal of Theoretical and Applied Information Technology
15th April 2012. Vol. 38 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# A NOVEL CRYPTOGRAPHIC ARCHITECTURE

**[1]R THANUJA, [2]S DILIP KUMAR**

[1]Assistant Professor, School of Computing, SASTRA University, Thanjavur, Tamilnadu, India

[2]Assistant Professor, Department of CSE, PRIST University, Trichy, Tamilnadu, India

E-mail: [1]thanuja.r@cse.sastra.edu, [2]sdprist@gmail.com

**ABSTRACT**

The goal of cryptography is to make it possible for two people to exchange a message in such a way that other people cannot understand the message. There is no end to the number of ways this can be done, but here we will be concerned with methods of altering the text in such a way that the recipient can undo the alteration and discover the original text. Today the modern cryptography is based on efficient algorithms for encryption that is used to provide better security. Asymmetric and Symmetric are nowadays designed with some complex function or key generations concept to provide security service in better manner. But, still now there are some attacks are reported even on modern cryptographic algorithms. In this paper we are going to propose a Novel Cryptographic architecture that uses IDEA &BLOWFISH algorithm for encryption purposes and using of SHA-I for generating hash value for cipher text in order to provide a strong cryptographic architecture.
Keywords: *Cryptographic Architecture, Hybrid Approach, Block Cipher, Hashing Algorithm*

## 1. INTRODUCTION

A strong cryptography algorithm design is based on type of algorithm and its hardness on computation so that intruders are able to identify the message that is to be send to destination nodes. Cryptography basically works on the principles of mathematics that generate different algorithms known as cryptographic Algorithms. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.

A cryptographic algorithm works in combination with a key or some random numbers to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys designed by the user. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. In this paper we are going design a new novel architecture by choosing IDEA algorithm & Blowfish for encryption as well as SHA-1 as cryptography hash functions.

## 2. RELATED WORKS

A new design of security protocol design by Ravindra Kumar Chahar [4] discuss the issues related to latest possible attacks to cryptosystem and the methods to build to a secure cryptographic architecture. This method uses normal cryptographic algorithms that seems to be easily attacked from intruder side.

The implementation of IDEA algorithm and its time taken to encrypt and decrypt are thoroughly identified by Bonnenberg, A. Curiger [5] seems to be IDEA algorithm works in a efficient manner.

## 3. ENCRYPTION & DECRYPTION PHASE

In our architecture, Figure 1.shows the encryption phase is done by the plaintext of n bit length is divided in to n/2 of two blocks of A and B respectively. The first n/2 bits (A) is encrypted using IDEA algorithm and the remaining n/2 bits (B) is encrypted using BLOWFISH algorithm. The resulting cipher text is named as $C_1$ and $C_2$ .

The size of cipher text $C_1$ and $C_2$ are calculated as P and Q which is useful to split up the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

bits in decryption process. The hashing algorithm SHA-I is applied to cipher text $C_1$ and the hash value of the corresponding cipher text is named as $D_1$. Similarly, the hashing algorithm SHA-I is applied to cipher text $C_2$ and the hash value of the corresponding cipher text is named as $D_2$. At the final stage of the encryption process , cipher text of two n/2 bits are integrated to generate n bits of cipher text ,the corresponding hash values and the size of the cipher text is appended with cipher text of n bits.

Figure 2. Shows the decryption phase of the cipher text of n bits is split into two n/2 bits of cipher text using the size of cipher text which is already calculated in encryption phase. The hashing algorithm SHA-I is applied to $C_1$ and $C_2$ to generate hash values of $D'_1$ and. $D'_2$ .

The hash values generated at encryption phase are compared with hash values generated at the decryption phase in order to identify whether we are receiving the same cipher text are not. If hash values are fond to be same, then it shows that we are able to receive the cipher text of same length as that of it is generated in the encryption phase. If the hash values are of different size that we received at the decryption phase compared to encryption phase, then those packets are discarded.

Once if the hash values are same at the both phases, now the cipher text of n bits is divided in to two n/2 bits using size of the cipher text P and Q .The cipher text $C_1$ is decrypted using IDEA algorithm to get n/2 bits of plaintext (A) and remaining $C_2$ is decrypted using BLOWFISH algorithm to get n/2 bits of plaintext (B). Finally, both plain texts of n/2 bits are integrated to generate n bits of plaintext.

## 4. STRENGTH OF PROPOSED APPROACH

The strength of any cryptographic algorithm is based on the computational methods and key used in the process. In normal cryptographic approach the intruders may be able to identify the cipher text patterns that are transmitted to the destination side. By analyzing the sequence of bit patterns it is possible for the intruder to identify what type of encryption algorithm is used or they will identify the key used for encryption/decryption process.

In our proposed approach we are creating two half's of plaintext of n/2 of length for encryption process. First n/2 bits are encrypted with IDEA algorithm and the resulting cipher text is hashed with SHA-1 to generate hash value for the particular n/2 plain text. Similarly remaining n/2 bits is encrypted with BLOWFISH algorithm and the resulting cipher text is hashed with SHA-1 to generate hash value for the particular n/2 plain text.

Suppose the intruder is analyzing sequence of bit patterns fro sender to receiver at any time, then he will not able to identify correct sequence of bits that is transmitted. Because, first n/2 bits is encrypted with IDEA algorithm and next n/2 bit is encrypted with BLOWFISH algorithm. So, the intruder is not able to identify what type of specific algorithm is applied to generate cipher text. Thus, the intruder is not possible to decrypt the cipher text.

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups that will be useful in diffusion and confusion methods. Idea algorithm seems to be implemented easily in hardware as well as software.

Blowfish is also a secure block cipher scheme that will be implemented easily as in 32-bit micro processor. It uses simple addition, XOR and sub key generation operations.SHA-1 produces 160 bit message digest which will be the input to digital signature algorithm. SHA-1 is secure because it is impossible to recover a message corresponding to given message digest.

## 5. CONCLUSION

In this paper, we proposed a new cryptographic algorithm that uses both IDEA and blowfish for encryption as well as SHA-1 to generate hash values. Thus the intruder is not possible to identify the type of algorithm which is used to generate cipher text. This architecture helps us to provide a secure cryptographic algorithm for next generation of security. The limitation of this approach is difficult to implement the architecture in handheld devices. The design of the architecture is to built a new cryptographic algorithm that helps us to securely communicate between systems. As a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

future work, we are going to compare this architecture with various cryptographic algorithms and try to implement the work.

**REFERENCES**

[1]. William Stallings.(2003).Cryptography and Network Security Principles and Practices 3rd Edition: Pearson Education Asia

[2]. Schneier B(1996).Applied Cryptography 2nd Edition: Wiley.

[3]. Rivest.(1992). The MD5 message-digest algorithm: RFC 1321.

[4]. Ravindra Kumar Chahar(2007). Design of a new Security Protocol. IEEE: International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134

[5]. Bonnenberg, A. Curiger, N. Felber, and W. Fichtner.(1994). IEEE Journal of Solid-State Circuits: A 177Mb/sec VLSI implementation of the international data encryption algorithm, vol. 29, pp. 303-307

[6].

.

Journal of Theoretical and Applied Information Technology
15th April 2012. Vol. 38 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

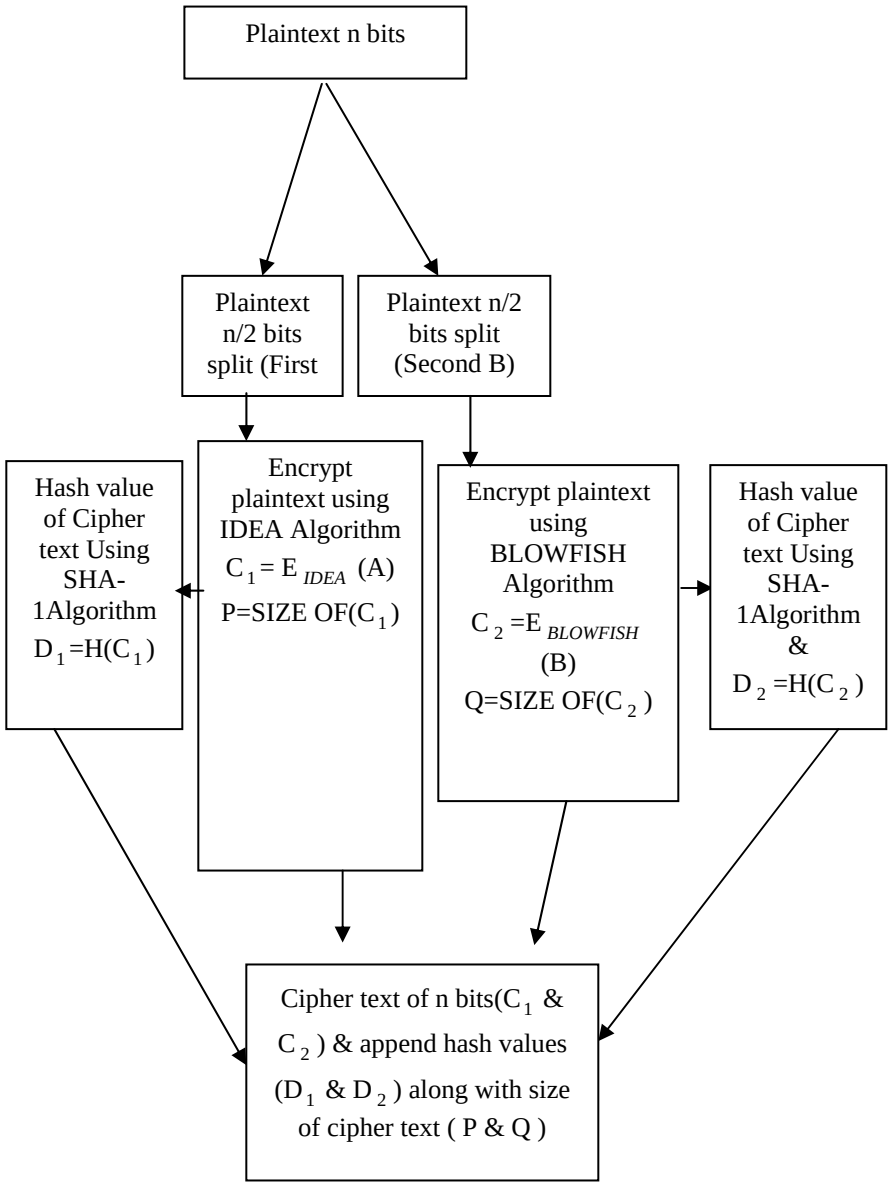


*FIGURE.1. ENCRYPTION PHASE OF NOVEL CRYPTOGRAPHIC ARCHITECTURE*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

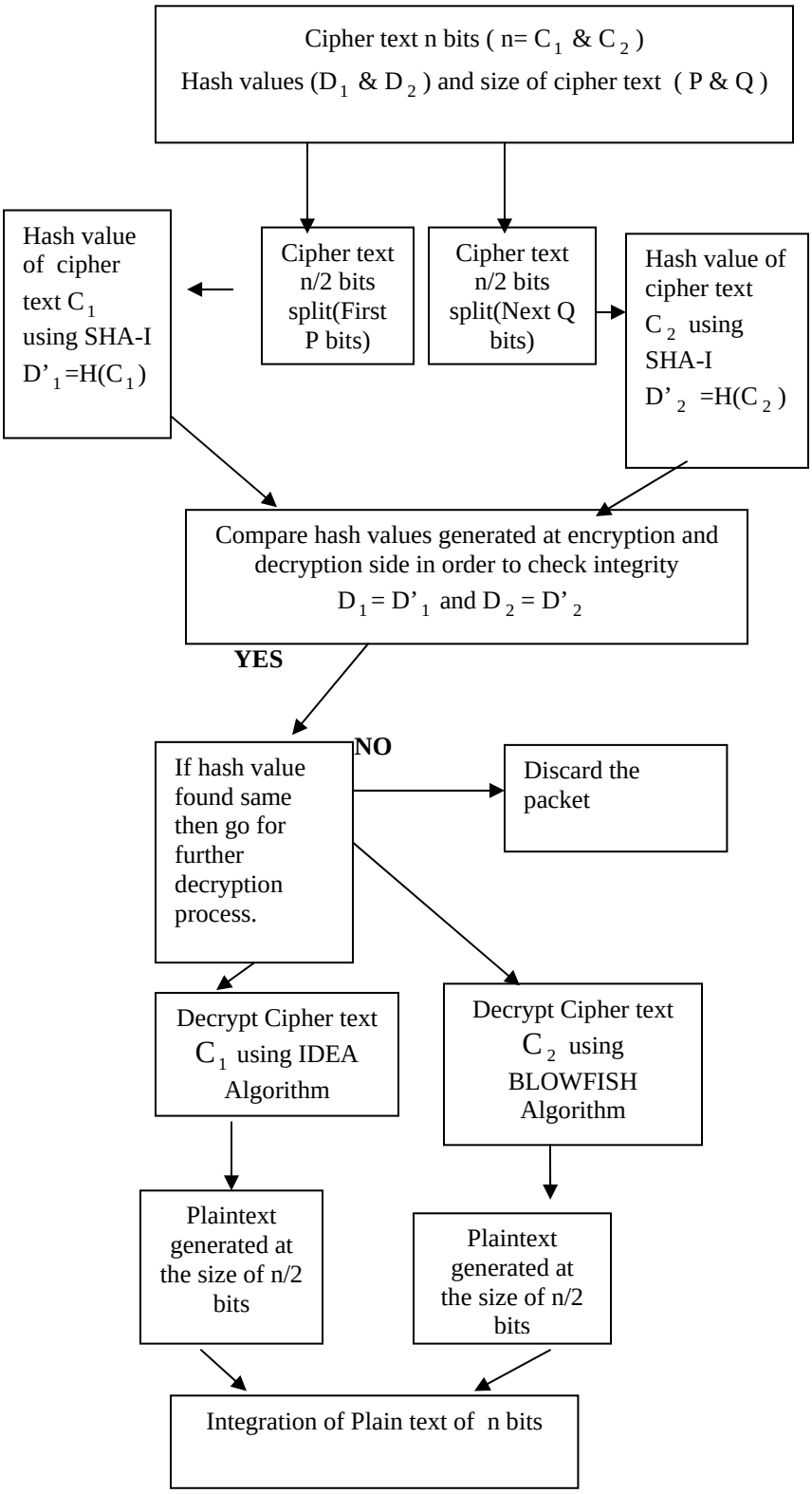


*FIGURE.2. DECRYPTION PHASE OF NOVEL CRYPTOGRAPHIC ARCHITECTURE*