International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 189-196
© International Research Publications House
http://www. irphouse. com /ijict. htm

Block and Stream Cipher Based Cryptographic Algorithms: A Survey

Nikita Arora[1] and Yogita Gigras[2]

[1]CSE-M. TECH, ITM University, M-502,
Guruharkishan Nagar PaschimVihar, Delhi, INDIA.
[2]ITM University, Department of CSE/IT, ITM University ,Gurgaon, INDIA.

Abstract

The encryption algorithms are designed to provide integrity and confidentiality of the messages. Modern cryptosystems are classified into three categories such as Block ciphers, Stream cipher and Hybrid ciphers of Hummingbird. This paper details about various types of block ciphers and stream ciphers. In this paper we also present the hybrid model of hummingbird and its comparison among other cryptographic algorithms.

Keywords: Block cipher, Stream cipher,Hummingbird.

1. Introduction

The elevation in wireless communication has led to the applications employing modern ciphers. These applications are helpful in public transportation, pay tv systems, electricity, military and health monitoring etc. ; These applications necessitate secure storage and transmission of data over insecure and unprotected communication channels.

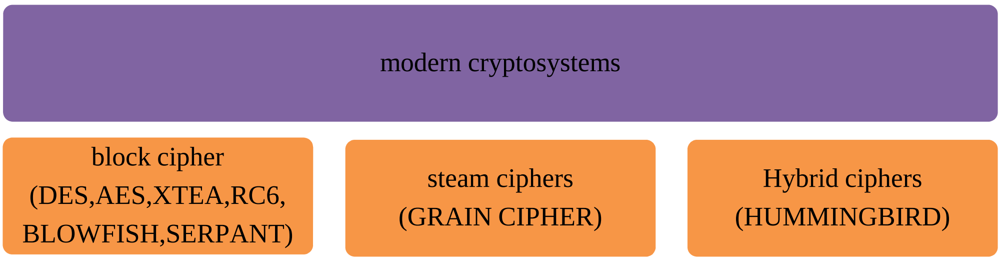

Fig. 1: Types of modern cryptosystems.

Present modern cryptosystems are divided into three categories namely:- block ciphers, stream ciphers and hybrid ciphers as shown in Fig. 1.

2. Block Cipher

Block ciphers are basically algorithms that encrypt a group of plaintext symbols of size m and create the ciphertext of same size. The similar key is used to encipher the whole block size. The main algorithms in this category are described below.

2. 1 DES(Data Encyption Standard)

DES is the symmetric encryption algorithm which uses the fiestel cipher with 16 rounds of processing. It uses 56 bit encryption key and operates on 64 bit of data to generate the ciphertext of 64 bit**[1].** DES performs an initial permutation on entire 64 bit of data, then it is divided into two halves of 32 bit each. Thereafter following operations are executed on the right half of data, namely- expansion step, key mixing layer, substitution layer with 8 s-boxes and permutation with p-box so as to introduce confusion and diffusion in the cipher. The resultant from p-box is in turn XORED with the 32 bit left subblock that we initiated out with, resultant becomes the right half for the next round of processing.

2. 2 AES(Advanced Encryption Standard)

AES is a non-fiestel symmetric cipher that enciphers the data block of 128 bits known as state**[2].** AES uses 10, 12 or 14 rounds with each version using a different key size, that is 128, 192 or 256 bits. State is arranged in the matrix(4*4). All rounds are identical in AES except the last round. Following operations are involved in round processing of AES as shown in the Fig. 2, where substitution using s-boxes introduces confusion and shifting of rows and mixing of columns introduces diffusion in the cipher.

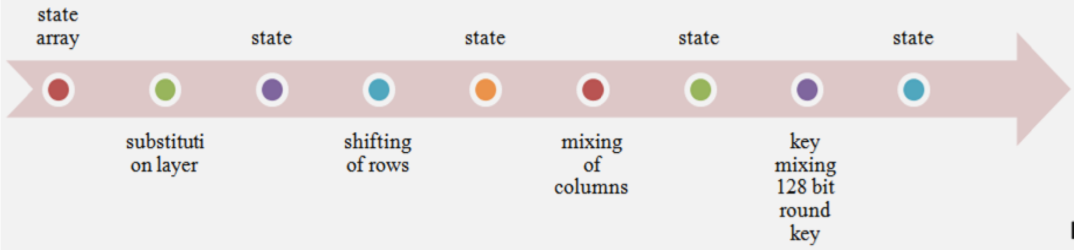

Fig. 2. Round processing in AES.

2. 3 Blowfish

Blowfish is a 64 bit symmetric encryption cipher. It consists of variable key length which ranges from 32 to 448 bits**[3]**. It was basically designed as an alternative to DES algorithm for fast encryption in 32 bit microprocessors. It is a fiestel cipher consisting of 16 rounds and is more suitable for handling large amount of data. The large number of subkeys are used during each round processing. Blowfish comprises of P-ARRAY having 18 subkeys, each of 32 bits and 4 Sboxes of (8*32) having 256 entries. Blowfish is an efficient algorithm but vulnerable to differential and chosen plaintext attacks. During encryption using Blowfish, the I/P data block is split into two halves of 32 bit each,L0 and R0. Now for i=1 to 16, following steps are executed:

L0=L0 XOR P_I;and R0=F(L0) XOR R0.
Swap L0 and R0. After the completion of 16 rounds,
R0=R0 XOR P_{17}; and L0=L0 XORP_{18}.

Finally L0 and R0 are combined to yield ciphertext.

2. 4 XTEA(Extended Tiny Encryption Algorithm)

XTEA is a 64 bit block cipher designed to overcome the weaknesses of TEA(Tiny Encyption Algorithm). TEA was subjected to weak key schedule, hence in XTEA keys are dynamically organized at the runtime, and demands no memory space. XTEA uses 128 bit as the key-size to encipher data block of 64 bit. The process of encryption and decryption is accomplished using Fiestel Network routine that uses 64 rounds. The dynamic key schedule property of XTEA makes it resistant to differential cryptanalytic attacks. XTEA was basically designed for high speed applications that require low power implementations **[4]**and thereby it more capable for resource constrained devices.

2. 5 RC6(Rivest Cipher 6)

RC6 is the improved enhancement of RC5. It is a block cipher of 128 bits and supports variable key –sizes of 128,192 or 256 bits. RC5 lacked the 32 bit integer multiplication operation which is present in RC6. The diffusion in RC6 is greater than RC5 and is capable to execute with few rounds with extreme security level and throughput**[5]**. RC6 comprises of four 32 bits register namely A,B,C,D which contains the original plaintext and the encoded ciphertext at the end of the encryption process. The least significant byte of A contains the foremost byte of the plaintext or ciphertext whereas the rearmost byte of the plaintext or ciphertext is positioned into the most significant byte of D. RC6 comprises of following rudimentary operations such as add, subtract ,multiply ,XOR and rotate. RC6 is susceptible to differential and linear cryptanalysis but offers pretty good performance and substantial flexibility.

2.6 Serpant

SERPANT is a block cipher of 128 bits having variable keysize ie. 128,192 or 256 bits. This cipher is a substitution permutation network with 32 rounds operating on 4-32 bit words. Serpant was designed in a way such that all the operations can be executed with extreme parallelism. It is a 32 round procedure including initial and final permutation. This algorithm has three basic functions:

1. Initial permutation of bits

It is constantly accomplished by the lookup table in which the position of the bits are changed. The resultant of the permutation yields b_0.

2. Round function or linear transformation

Thereafter the round function is applied on B_i 32 times. In every round,B_i is XORED with one of 32 subkeys and the result is passed through the sboxes. One of the 8 Sboxes of size(4*4) are used 32 times in parallel. But in the last round, textblock is mixed with 33 subkey generated from the key schedule instead of the Linear Transformation.

3. Final-permutation

It is performed via lookup table to yield ciphertext.

3. Stream Cipher

Stream cipher are the symmetric key cipher where the plain text digits are combined with pseudorandom keystream. Each plaintext digit is encrypted one at a time with the corresponding digit of keystream.

3.1 Grain cipher

Martin Hell, Thomas Johansson and Willi Meier designed grain cipher in such a way that implementation of hardware is easy and chip area needed is also reduced. LFSR and NFSR are the two building blocks of the Grain Cipher each of 80 bits. The LFSR is used to provide balanceness so that the cipher becomes cryptographically secure. In contrast,NFSR adds nonlinearity to the grain cipher**[6].** The NFSR input is masked with the LFSR output so as to produce the balanced state of NFSR. The initial vector and keysize are 80 bits in size. f(x) and g(x) are the feedback polynomial functions of degree 80 for the LFSR and NFSR. The filter function is nonlinear and is represented by h(x). This filter function uses as input particular bits from both the feedback registers LFSR and NFSR. Thereafter 7 bits from NFSR are added to h(x) which further becomes extraneous feedback to both the registers. This value is also used as the keystream sequence.

4. Hybrid Cipher

Hybrid cipher is the magnific fusion of both Block Cipher and Stream Cipher. Hummingbird is an ultralight weight cryptographic hybrid cipher that inherits the characteristics of both Block Cipher and Stream Cipher**[6].** This hybrid structure makes it suitable for extreme resource constrained devices such as smart devices and wireless nodes**[7].** The Fig. 3 illustrates some differences and similarities among two types of Hummingbird cipher, namely Hummingbird 1 and Hummingbird2. These are ultra lightweight cryptographic algorithms.

4. 1Hummingbird1and Hummingbird2

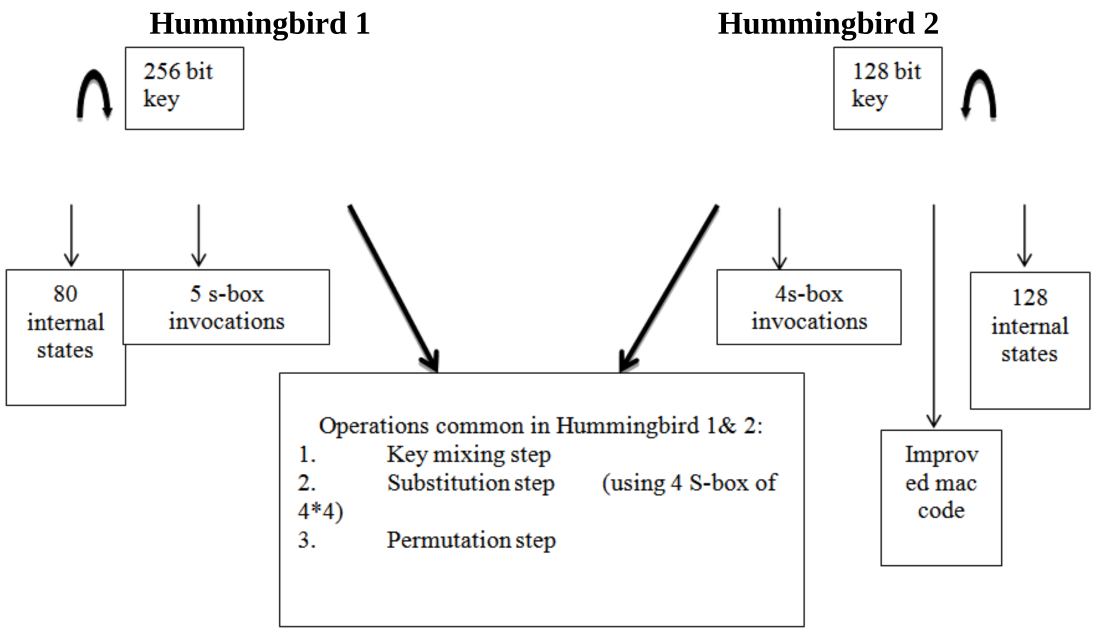

Fig. 3: Difference and common point of Hummingbird 1 and Hummingbird 2.

5. Conclusion

Compared to other cryptographic algorithms such as DES, AES, XTEA, SERPANT, GRAIN, RC6, etc, Hummingbird is the most capable cryptosystem for implementation in resource constrained environment like RFID technology ,wireless sensors and other smart devices. The consumption of power is less and encryption speed is faster in Hummingbird. Hummingbird has the further benefit over other modernized encryption primitives that it yields efficient Message Authentication code and is also known as authentication algorithm. Hummingbird is designed to be used in high security required low cost pervasive devices as it is resistant to most of the cryptanalytic attacks common to block ciphers and stream ciphers.

Table 1: Comparison of various cryptographic algorithms.

	DES	**AES**	**XTEA**	**RC6**	**BLOWFISH**	**SERPANT**	**GRAIN**	**HUMMING BIRD**
Design structure	Balancedfiestel network	Non-fiestel substitution and permutat	Use fiestel structure	Use	Use	Non-fiestel substitution	Not use	Non-fiestelsubstitution permutation network

		ion network				permutation network		
Key size	56	128/192/256	128	128,192, 256	32-448	128,192, 256	80	128/256
Block size	64	128	64	128	64	128	1	64
Rounds	16	10/12/14	64	20	16	32	-	4
Mathematical operations	XOR/ shifts	XOR/ shift	XOR/ shift/ Addition	Modular addition, XOR, multiplications shift	XOR, 2^{32}modular addition	XOR, shift	XOR	XOR, modulo 2^{16} additional shift operations
s-box/ D-box used	8 sbox (6*4); 3 Dbox (4*6)	s-box of size (8*8) is used	Not used	Not used	4 s-box of size (8*32) Is used	8 s-box (4*4)	Not used	4 s-box (4*4)
Key space	2^{56}	$2^{128}, 2^{192}$ 2^{256}	2^{128}	$2^{128}, 2^{192},$	2^{32}-2^{448}	$2^{128}, 2^{192},$	2^{80}	$2^{128}, 2^{256}$
MAC code (message authentication code)	Can use to generate MAC code	Not used	Not used	Not used	Not used	Not used	Not used	Most efficient mac code
attacks	Vulnerable to brute force attacks, linear crypt analysis and known plaintext	Vulnerable to side channel attacks	Vulnerable to related key, differential and chosen plaintext attacks	Vulnerable to Statistical and known plaintext attacks.	Vulnerable to differential attacks and sometimes to other attacks if reflective weak keys are used.	Susceptible to known plaintext and man in the middle attacks.	No better key recover attacks except brute force attacks	It is most secure and resistant to most of the linear and differential attacks but susceptible to related key attacks.

References

[1] Behrouz A Forouzan,DebdeepMukhopadhyay,In Book Title(Cryptography and Network Security),Tata McGraw Hill Education private limited.

[2] Jacob John, Article in a regular journal, International Journal on Computer Science & Engineering, “Cryptography for resource constrained devices :A Survey”,2012

[3] Jasdeep Singh Bhalla, PreetiNagrath ,Article in a regular journal, International Journal of Scientific & Research publications,”Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm”, Volume 3, Issue 4, April 2013.

[4] Jens-Peter Kaps,Article in conference, INDOCRYPT '08 Proceedings of the 9th International Conference on Cryptology in India: Progress in Cryptology,“Chai-tea, Cryptographic Hardware Implementations of XTEA”,2008.

[5] Ronald L. Rivest,MJB Robshaw, “The RC6 Block Cipher”.

[6] Nikita Arora,YogitaGigras,Article in a regular journal,International Journal of Research & Development in Technology and Management, “Light Weight Cryptographic Algorithms:a survey”,2013.

[7] Revini S. Shende, Mrs. Anagha Y. Deshpande, Article in a regular journal, International Journal of Engineering Research and Applications, “VLSI Design Of Secure Cryptographic Algorithm”2013.