# Study on symmetric key encryption: An Overview

Dharitri Talukdar

**ISSN Print:** 2394-7500
**ISSN Online:** 2394-5869
**Impact Factor:** 5.2
IJAR 2015; 1(10): 543-546
www.allresearchjournal.com
Received: 14-07-2015
Accepted: 17-08-2015

**Dharitri Talukdar**
Ph. D Research Scholar,
Assam down town University,
India, Guwahati.

**Abstract**

Cryptography is the art to keep data secure from hackers by means of a secret that is only known to the communicating parties. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. This paper aims to provide an overview on symmetric key encryption.

**Keywords:** Cryptography, block cipher, stream cipher, Symmetric-key cryptography, encryption, decryption

## Introduction

Cryptography means sending confidential information over an insecure network in a secured manner by hiding information. The modern cryptosystem is about the design and analysis of various methods that are related to various aspects in data security, integrity and authentication. Cryptography can be classified in two ways- symmetric and asymmetric key cryptography.

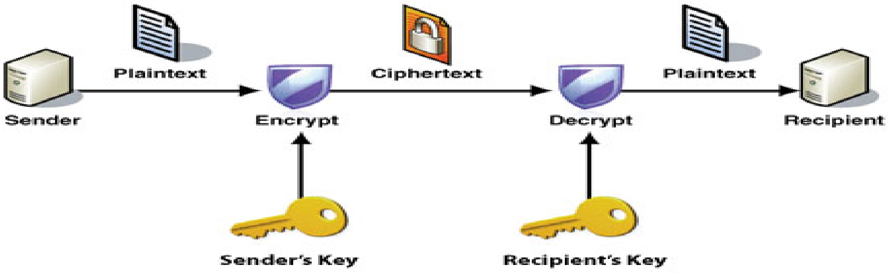

**Fig 1:** Symmetric-key cryptography

## Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern embodiment of Alberti's polyalphabetic cipher: block ciphers take as input a block of plaintext and a key, and output a block of cipher text of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the modes of operation and must be carefully considered when using a block cipher in a cryptosystem [1].

## Asymmetric-key cryptography

In asymmetric key cryptography, there are two keys: private key and public key. Both are required to encrypt and decrypt a message. Message sender encrypts the message or data using public key that may be known to all publicly. On the other side message receiver uses other secret key to decrypt the message.

**Correspondence**
**Dharitri Talukdar**
Ph. D Research Scholar, Assam down town University, India, Guwahati.

### Implementations of Symmetric Key Encryption

There are several modern algorithms that implement a symmetric key encryption method. One method of symmetric key encryption is a block cipher and stream cipher. Block cipher operates on fixed-length groups of bits. When encrypting, a block cipher takes a set amount of bits (i.e. 128 bit block) of plaintext and outputs a corresponding same size (i.e. 128-bit) block of cipher text. The exact transformation of a block cipher is controlled by the encryption/decryption key. Popular block ciphers include: Blowfish, Twofish, DES, and AES.

In stream cipher, a stream of random, or pseudo random, numbers are combined with the original message. Specific stream ciphers include: One-Time Pad, Linear Feedback Shift Register (LFSR), Linear Congruential, and RC4. RC4 is the most widely-used stream cipher and is used in Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP) [12].

### Overview of encryption block and stream ciphers for data security

Here we will discuss two block cipher (Blowfish and AES) and stream cipher (One-Time Pad and RC4) encryption techniques used for encryption purpose.

### Blowfish

Blowfish is an encryption algorithm and is also a block cipher. There are two parts to this algorithm-

- A part that handles the expansion of the key.
- A part that handles the encryption of the data.

The expansion of the key: break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.

The encryption of the data: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration). Security of data with blowfish Cipher is excellent [2].

### AES (Advanced Encryption Standard)

The AES encryption algorithm is a block cipher that uses an encryption key and a several rounds of encryption [3]. It has variable key length of 128, 192, or 256 bits; default 256.It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size [14]. A round for the AES algorithm consists of four operations: the Sub Bytes operation, the Shift Rows operation, the Mix Columns operation, and Add Round Key operation [2]. AES is better for live video streaming transmission compared to RC4 and XOR. AES can be implemented more comfortably in high and low level language [3].

### Rivest Cipher 4 (RC4)

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Used for secured communications as in the encryption of traffic to and from secure web sites using the SSL protocol [3].

### One-Time Pad

The "one-time pad" encryption algorithm was invented in the early 1900's, and has since been proven as unbreakable. *Army* Signal Corp. Officer, Joseph Mauborgne, proposed an improvement to Vernam Cipher that was the Ultimate in security [5]. He suggested that we use a random key that is as long as the message means the key need not to be repeated. In additional key must be use once for encryption and decryption of a single message and then that key is discarded. So this technique is called as One Time Pad and there is relationship between key and plaintext and it is unbreakable. In this as advance of vignere cipher scheme we Can use 27 character in which 27th character is SPACE, so in this key will be as long as message. So table of Vignere cipher must be expanded to 27*27. One time pad is used only for low Bandwidth Channels requiring very high security. In this technique, comes problem of generation of keys in so much quantity which is so tough to handle that increases the cost of this technique [4].

### Methodology

a. Collecting various algorithms
b. Exploring different designs and their security level.

### Literature Survey

Thambiraja *et al.* [6] showed that AES consumes highest processing power among DES, 3DES, BLOWFISH. AES is better than RC4 for smaller packets also it is better for live video streaming transmission compared to RC4 and XOR. Time taken by RSA is much higher than that of AES and DES. Memory usage of RSA is high compared to AES, DES. Output byte in RSA is less as compared to AES and DES.RC4 is fast and energy efficient than AES for larger packets. Time for encryption and decryption almost remains constant for RC4 if key size is increased and less time is required to encrypt as compared to AES, DES, and 3DES.

Susan *et al.* [7] concluded that Computer network security is a new and fast moving technology in the field of computer science. As such, the teaching of security is still a moving target. Security courses originally focused on mathematical and algorithmic aspects such as encryption and hashing techniques. However, as crackers hacked away at networks and systems, courses arose that emphasized the latest attacks. These attacks soon became out-of-date with security software responses. As security technology continues to mature, there is an emerging set of security techniques and skills. Network security skills emphasize business practices, legal foundations, attack recognition, security architecture, and network optimization.

Krishnamurthy P. *et al.* [8] analysed that Encryption algorithms are known to be computationally intensive. They consume a significant amount of computing resources such as CPU time, memory, and battery power. A wireless device, usually with very limited resources, especially battery power, is subject to the problem of energy consumption due to encryption algorithms. Designing energy efficient security protocols first requires an understanding of and data related to the energy consumption of common encryption schemes. In this paper, we provide the results of experiments with AES and RC4, two symmetric key algorithms that are commonly suggested or used in WLANs. Our results show that RC4 is more suitable for large packets and AES for small packets.

Elbirt A.J. *et al*. [9] studied that efficient implementation of block ciphers is critical towards achieving both high security and high-speed processing. Numerous block ciphers have been proposed and implemented, using a wide and varied range of functional operations. As a result, it has become increasingly more difficult to develop a hardware architecture that allows the efficient and fast realization of a wide variety of block ciphers. In an effort to achieve such hardware architecture, a study of a wide range of block ciphers was undertaken to develop an understanding of the functional requirements of each algorithm.

Meyer C.H. *et al*. [10] proposed that Cryptography is the only known practical method for protecting information transmitted through potentially hostile environments, where it is either impossible or impractical to protect the information by conventional physical means. Also, damage resulting from message alteration, message insertion, and message deletion can be avoided. Administrative and physical security procedures often can provide adequate protection for offline data transport and storage. However, where file security methods are either nonexistent or weak, encryption may provide the most effective and economical protection. The authors gives an overview of cryptographic methods using symmetric and asymmetric algorithms and demonstrates why future cryptographic applications should use a hybrid approach, i.e., combination of symmetric and asymmetric (public key) methods.

Thakur *et al*. [11] showed that AES can be implemented more comfortably in high and low level language as compared to DES. Blowfish has better performance when packet size is changing as compared to AES, DES, 3DES, RC2, and RC6.

J. Daemen [13] concluded that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes a study in is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input less of varying contents and sizes. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data. Therefore, AES is a feasible solution to secure real time video transmissions. It was shown in that energy consumption of different common symmetric key encryptions on hand-held devices. It is found that after only 600 encryptions of a 5 MB le using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly. Using H.264 to compress and encrypt, videos can solve the speed and security problems in mobile application.

M. Anand Kumar *et al*. [14] presented the performance evaluation of two commonly known symmetric cryptographic algorithms. These algorithms are tested with different performance metrics. The simulation results shows that Blowfish has better performance than AES in almost all the test cases. There is no significant difference in the result for base64 encoding and hexadecimal encoding techniques. It is found that blowfish is good for text based encryption whereas AES has better performance for image encryption. It is also identified that there is change in performance when there is a change in key size of AES algorithm. Overall it is identified that AES can be used in circumstances where there is need for high security. In the case of performance aspects, Blowfish can be used.

## Conclusion

Every technique is unique in its own way. Each could be used as per the requirements of the applications. This paper presents an overview of various block and stream ciphers encryption techniques, which are used in cryptography for network security purpose. It can be concluded that One-time pad technique requires very high security and so become costly. RC4 is fast and energy efficient than AES. Time for encryption and decryption almost remains constant for RC4 if key size is increased. AES is a feasible solution to secure real time video transmissions and can be implemented more comfortably in high and low level language. Blowfish is good for text based encryption.

## References

1. Ahmed Al-Vahed, Haddad Sahhavi. An overview of modern cryptography, World Applied Programming 55-61 ISSN: 2222-2510©2011 WAP journal. 2011; 1:1.
2. Gunjan Gupta, Rama Chawla. Review on Encryption Ciphers of Cryptography in Network Security, International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X. 2012; 2:7.
3. Harshraj N Shinde, Aniruddha S Raut, Shubham R Vidhale, Rohit V Sawant, Vijay A. Kotkar. A Review of Various Encryption Techniques, International Journal of Engineering and Computer Science ISSN: 2319-7242. 2014; 3(9):8092-8096.
4. Ritu, Yuvinder Dandiwal. Techniques used for Encryption Purpose, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X. 2015; 5:5.
5. William Stallings. Cryptography and Network Security, 3rd edition, Pearson Education, 2003.
6. Thambiraja E, Ramesh G, Dr. R Umarani. A Survey on Various Most Common Encryption Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X. 2012; 2:7.
7. Othman O, Khalifa MD Rafiqul Islam, Khan S, Mohammed S, Shebani. Communication Cryptography, RF and Microwave Conference, Subang, Selangor, Malaysia, 2004, 5-6.
8. Krishnamurthy P, Prasithsangaree P. Analysis of energy consumption of RC4 and AES algorithms in wireless LANs, IEEE Global Telecommunications Conference 2003; 3:1445-1449.
9. Elbirt AJ, Paar C. Instruction-level distributed processing for symmetric-key cryptography, International Parallel and Distributed Processing Symposium, 2003.
10. Meyer CH, Cryptography-a state of the art review, Conferrence on VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks 1989, 4/150-4/154,
11. Jawahar Thakur, Nagesh Kumar. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, ISSN2250-2459. 2011, 12.
12. Nicholas G, McDonald. Past, present, and future

methods of cryptography and data encryption, 13.

13. Daemen J, Rijmen V, Rijndael: The advanced encryption standard, Dr. Dobb's Journal. 2001; 137-139.
14. Anand Kumar M, Dr. S Karthikeyan. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms, IJ. Computer Network and Information Security 2012; 2:22-28.