RESEARCH ARTICLE OPEN ACCESS

# Overview on Symmetric Key Encryption Algorithms

Mithil P. Gharat
Research Scholar,
Vidyalankar Institute of Technology, Mumbai.

Prof. Dilip Motawani
Assistant Professor,
Vidyalankar Institute of Technology, Mumbai.

**Abstract—**
In today's digital communication era sharing of information is increasing significantly. The information being transmitted is vulnerable to various passive and active attacks. Therefore, the information security is one of the most challenging aspects of communication. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form by using Encryption and Decryption Techniques. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. There are basically two techniques of cryptography Symmetric and Asymmetric. This paper presents a detailed study of the symmetric encryption techniques.

**Keywords**— Cryptography, Encryption, Decryption, AES, DES, TRIPLEDES, Blowfish.

## I. Introduction

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

### *A. Confidentiality / Privacy*

Keeping information secret from all, but those who are authorized to see it. Confidentially is the protection of transmitted data from passive attacks. With respect to the content of data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to Observe to source and destination, frequency, length or any other characteristics of the traffic on a communication facility.

### *B. Data Integrity*

Ensuring the information has not been altered by unauthorized or unknown means. One must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution

### *C. Authentication*

- It should be possible for the receiver of a message to ascertain its origin.
- An intruder should not be able to masquerade as someone else.

### *D. Non Repudiation*

Non-repudiation prevents either sender or receiver from denying a message. Thus, when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received that message.

## II. Overview of Algorithms

Most common Symmetric encryption algorithms are discussed as follows.

The symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt the data. Symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively. There are various symmetric key algorithms such as DES, TRIPLEDES, AES, and BLOWFISH.

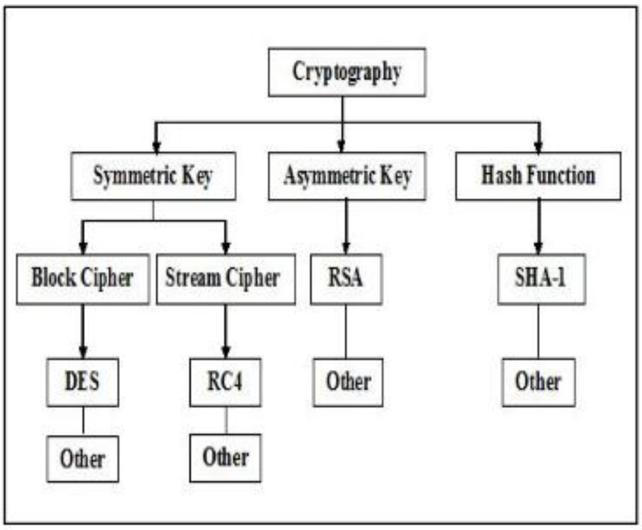

*Fig 1 Classification of Cryptography*

### A. Data Encryption Standard (DES)

DES was the first encryption standards to be published by NIST (National Institute of Standards and Technology).It was designed by IBM based on their Lucifer Cipher. Initially,56 bits of the key are selected from the initial 64 by permuted choice. The remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves, each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits and then 48 sub key bits are selected by permuted choice,24 bits from the left half and 24 from the right. The key schedule for decryption is similar, the sub keys are in reverse order compared to encryption.

### B. Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher published by National Institute of Standards and Technology (NIST) in December 2001.AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size which can be 128,192, or 256 bits, depends on the number of rounds. If both block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are 192 bits, AES will perform 11 processing rounds. If the block and key are 256 bits, then it performs 13 processing rounds. Each processing rounds involves four steps:

- ***Substitute bytes***: Uses an S-box to perform a byte by byte substitution of the block.
- ***Shift rows***: A simple permutation.
- ***Mix column:*** A substitution method where data in each column from the shift row is multiplied by the algorithm’s matrix.
- ***Add round key:*** The key for the processing round is XORed with the data.

### C. Triple DES

In cryptography, TRIPLE DES is the common name for Triple Data Encryption Algorithm block cipher, which applies the Data Encryption Standard cipher algorithm three times to each data block. The original DES cipher’s key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks. It takes three 64-bit keys, for an overall key length of 192 bits. In Triple DES the data is encrypted with the first key, decrypted with the second key, and finally encrypted with the third key. Triple DES runs three times slower than DES, but it much more secure. The procedure for decrypting is the same as the procedure for encryption, except it is executed in reverse.

### D. Blowfish

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and key can be any length up to 448 bits. It is significantly faster than most encryption algorithms when implemented on 32- bit microprocessors with large data caches. The algorithm consists of two parts: a key expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several sub keys arrays totalling 4168 bytes.

## III. Various Symmetric Key Encryption Techniques

This paper describes about some of the symmetric encryption techniques which are already available. In general cryptographic encryption techniques are classified as classical cryptographic techniques and modern cryptographic techniques based on the periods that are developed/used. Classical cryptographic techniques are developed in the earliest days, but still some of the algorithms are used for providing confidentiality to the information. Modern cryptographic techniques are developed in recent years for providing better services like confidentiality, authentication, etc., to the information. In order to increase the degree of security, the modern cryptographic techniques algorithms are incredibly complex than classical cryptographic algorithms.

**Table 1. Modern symmetric encryption algorithms**

| **Sr No** | **Encryption technique name** | **Year** | **Developed By** | **Granularity (Stream/Block Cipher)** | **Key Size** | **Vulnerability to attack** | **Uniqueness about the technique** |
|---|---|---|---|---|---|---|---|
| 1. | Camellia | 2000 | Mitsubushi , NTT | Block cipher (128 bits) | 128, 192, or 256 bits | algebraic attack | 16 rounds 8*8 S-boxes. Nested Feistel Network |
| 2. | Serpent | 1998 | Ross Anderson, Lars Knudsen, Eli Biham | Block cipher (128 bits) | 128, 192, or 256 bits | Linear cryptanalysis and Rectangle algebraic attack | 32 rounds, Open source algorithm |
| 3. | Rijndael | 1998 | Vincent Rijmen, Joan Daemen | Block cipher (128 bits) | 128, 192, or 256 bits | Related Key Attack, Algebraic attack | 10,12,14 rounds (depending on key size) maximal size ofthe input file is 2,097,152 bytes |
| 4. | Skipjack | 1998 | National Security Agency (NSA) | Block cipher (128 bits) | 80 bits | Slide attack | 32 rounds unbalanced Feistel Network Structure |
| 5. | AES | 1998 | Joan Daemen, Vincent Rijmen | Block cipher (128 bits) | 128, 192, 256 bits | Known plaintext, Side channel attack | Substitution permutation network, 10 or 12 or 14 rounds |
| 6. | RC 6 | 1998 | Ron Rivest | Block cipher (128 bits) | 128, 192, 256 bits | Known plaintext, chosen cipher text | Feistel network, 20 rounds |
| 7. | SEED | 1998 | Korea Information Security Agency | Block cipher (128 bits) | 128 bits | Chosen plaintext, Known plaintext | 16 rounds 8*8 s-boxes Nested Feistel Network |
| 8. | Twofish | 1998 | Bruce Schneier | Block cipher (128 bits) | 128 256 bits | Truncated differential cryptanalysis | 16 rounds Feistel Structure.<br>Free to use |
| 9. | RC-2 | 1996 | Ron Rivest | Block cipher (64 bits) | 8-128 bits (64 bits) | Related key attack, Chosen plaintext | 18 rounds Source heavy Feistel Network Structure |
| 10. | Blowfish | 1993 | Bruce Schneier | Block cipher (128 bits) | 32-448 bits | Second order differential attack, Weak key | 16 rounds Feistel Structure.<br>Free to use, key independent S-box |
| 11. | IDEA | 1991 | Xuejia Lai, James Massey | Block cipher (64 bits) | 128 bits | Weak keys, | 8.5 rounds Feistel Network Structure |
| 12. | Triple DES | 1978 | IBM | Block cipher (64 bits) | 112 or 168 bits | Theoretically possible, Known plaintext, chosen plaintext | 48 rounds Feistel Network Structure, Three different keys used |
| 13. | DES | 1977 | IBM | Block cipher (64 bits) | 56 bits | Differential & Linear Cryptanalysis, Brute force attack | 16 rounds Feistel Structure,<br>Left circular shift, Substitution 32-bit swap |

## IV. Conclusion

Cryptography plays vital role in explosive growth of digital data storage and communication. It is used to achieve the mains of security goals like confidentiality, integrity, authentication, non-repudiation. In order to achieve these goals, various cryptographic algorithms are developed. In which some of the algorithms are succeed and others failed due to lack of security. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated. The main purpose of this paper is to disseminate the basic knowledge about the cryptographic algorithms and comparison of available symmetric key encryption techniques based on some parameters like vulnerability to attack, Uniqueness about the technique, etc.

## References

[1] Manoj Kumar Pandey, et.all., "*Survey Paper: Cryptography The art of Hiding Information*", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 2, Issue 12, December 2013.

[2] Irfan Landge et al., "*Encryption and Decryption of Data Using Twofish Algorithm*", World Journal of Science and Technology, ISSN: 2231-2587, Vol. 2, No. 3, pp. 157-161, 2012.

[3] Anjali Arora et al., "*A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers*", International Journal of Computer Science and Information Technology & Security, ISSN: 2249-9555, Vol. 2, No. 2, April 2012.

[4] A. Grediaga et al., "*Analysis and Implementation Hardware-Software of Rijindael Encryption*", IEEE Latin America Transactions, Vol. 8, No. 1, pp. 82-87, March 2010.

[5] Ayushi, "*A Symmetric Key Cryptographic Algorithm*", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010

[6] Christof Paar, JanPelzl, and Bartpreneel, "*Understanding Cryptography: A Text book for student and Practitioners*", Springer, 2010.

[7] Tarun Narayan Shankar and G.Sahoo, "*Cryptography by Karatsuba Multiplier with ASCII Codes*", International journal on computer applications, pp.53-60, 2010.

[8] William Stallings "*Cryptography and Network Security: Principles and Practices*", PHI Learning Private Limited, Forth Edition, 2009, pp 64 - 86.

[9] Yee Wei Law, Jeroen Doumen, and Pieter Hartel, "*Survey and Benchmark of Block Ciphers for Wireless Sensor Networks*", ACM Transactions on Sensor Networks, Vol. 2, No. 1, February 2006.

[10] Chris Christensen, "*The Hill Cipher*", MAT/CSC 483, 2006.

[11] Bruce Schneier et al., "*A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish*", Twofish Technical Report #6, February14, 2000.

[12] Bruce Schneier et al., "*New results on The Twofish Encryption Algorithm*", February1, 1999.

[13] Daemen J., Rijmen V., "*The Rijindael Block Cipher*", AES Proposal, Belgica 1999. ISSN: 2278 – 7798

[14] C.Adams, "*Constructing Symmetric Ciphers Using the CAST Design Procedure*", in selected Areas in cryptography, E. Kranakis and P. Van Oorschot (ed.), Kluwer Academic Publishers, pp. 71-104, 1997.

[15] Ross J. Anderson, "*Why Cryptosystems Fail*", Communications of the ACM, New York, USA, pp. 32-40, 1994.