*Professional paper / Stručni rad*
*Manuscript received: 2016-12-15*
*Revised: 2016-12-21*
*Accepted: 2016-12-22*
*Pages: 127 - 134*

# *Comparative Analysis of Cryptographic Algorithms*

*Zoran Hercigonja*

*Druga gimnazija*
*Varaždin, Croatia*

*zoran.hercigonja@gmail.com*

**Abstract:** Cyber security ensures a secure information exchange and enables communication through the Internet. The data needs to be protected from unauthorized access and transmitted to the intended receiver with confidentiality and integrity. Cryptography enhances security by encrypting and decrypting raw data in a secured network. Many cryptographic algorithms are available, and they fall under either symmetric or asymmetric techniques. To choose an algorithm for secure data communication, the candidate algorithm should provide higher accuracy, security and efficiency. This paper presents the implementation limitations of existing cryptographic algorithms such as DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, and RC6 of symmetric techniques and RSA of asymmetric techniques. This paper also analyzes parameters like key exchange, flexibility and security issues of the algorithms which determines the efficiency of the cryptosystem.

**Keywords:** cryptography, symmetric, asymmetric, architecture, security, limitations, DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC6, RSA

# INTRODUCTION

Cryptography is a technique which is intended to transform the data and can be used to provide various security related concepts such as confidentiality, data integrity, authentication, authorization and non-repudiation [9]. It depends on two basic components: an algorithm (cryptographic technique) and a key. The algorithm is a numerical procedure and the key is a factor used for data transformation. These algorithms provide cryptographic protection to the data by using encryption and the reverse by decryption. These algorithms can be Symmetric key Algorithms or Asymmetric key algorithms. Symmetric algorithms (Secret Key Algorithms) use a single key for both encryption and decryption. Some commonly used symmetric algorithm include DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, and RC6. Asymmetric algorithms (Public Key Algorithms) uses a public key and a private key pair which are related to each other. These algorithms include DH (Diffie-Hellman keys), SSL, RSA, and SSH. In both the cases the keys are generated by random number generators. The cryptographic keys must be established between the sender and the receiver either manually or using trusted third party key management.

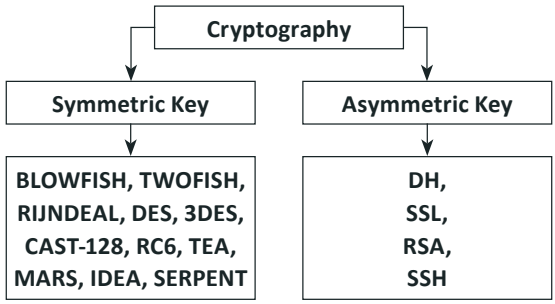


**Figure 1:** Classification of cryptographic algorithms [6]

The basic classification of cryptographic algorithms is shown in Figure 1. Many authors have compared these algorithms on the basis of time complexity and space complexity [6]. This paper compares these algorithms on the basis of parameters like key length and management, security and limitations pertaining to each algorithm.

# CRYPTOGRAPHIC ALGORITHMS

The security of a cryptosystem depends on the architecture of the algorithm. This section analysis the cryptosystems in the basics of key generation, key length, block size and number of rounds used for encryption and decryption process [7]. The rate at which a particular algorithm encrypts the data is an essential parameter in analyzing the performance of encryption algorithm [8].

An algorithm is considered to better if it provides strong security level. This section analyzes also the security levels of various cryptographic algorithms and discuss the limitations of selected cryptographic algorithms.

## *DATA ENCRYPTION ALGORITHM (DES)*

DES is the earliest symmetric key block cipher encryption algorithm developed by IBM and adopted by U.S federal government as a standard encryption technique. DES uses 64 bits plaintext blocks and a key length of 56 bits. DES uses the 8 bits as parity bit for error detection. DES is based on Feistel function (f) which divides the blocks into two halves, applies 16 rounds of processing to encrypt the data [7]. Function f involves 4 stages as expansion, key mixing, substitution and permutation. Security in DES is of major concern because of the 56 bit key length. Brute force attack becomes possible with a massively parallel machine of more than 2000 nodes with each node, capable of a key search rate of 50 million keys/sec. Cryptanalysis is possible by exploiting the characteristics of DES. The weak S-boxes provides a possible mean for a cryptanalytic attack. DES is highly susceptible to linear cryptanalysis attacks. It is exposed to brute force attack because of the weak keys.

## *TRIPLE DATA ENCRYPTION ALGORITHM (3DES)*

3DES is derived from DES and it uses 3 different keys of 56 bits (168 bits total) [7]. It has 3 keying options:

- Option 1: All three keys are independent. This option is the strongest with 168 independent key bits.
- Option 2: All three keys are identical which is the weakest option and equivalent to DES.
- Option 3: First and third keys are identical. It performs 48 rounds of processing to encrypt the data by applying DES three times.

3DES reduces the security issue of DES by combined key size of 168 bits (3 times of 56) which is beyond the reach of brute-force techniques. No serious flaws have been uncovered in 3DES, though it has always been regarded suspicious because of DES. Many Internet protocols uses this cryptosystem. 3DES is vulnerable certain variation of meet-in-the-middle attacks. It is also exposed to differential and related-key attacks.

## *CAST-128*

CAST-128 is a block cipher algorithm based on Feistel function and has 12 to 16 processing rounds [4]. It uses an 64 bit block and a key length of 40-128 bit. If the key size is greater than 80 bits, 16 rounds of processing are performed. CAST increases the security strength by using variable key size of 128 and 256 bits. This increases the resistance against both linear and differential attacks [2]. CAST-128 can be broken by 2^17 chosen plaintexts. The 64 bit key version is susceptible to differential related-key attack.

## *BLOWFISH*

Blowfish is a block encryption algorithm based on Feistel function which uses a 64 bit block and key size ranges from 32-448 bits. Blowfish performs 16 processing rounds [1], [7]. Key expansion and Data Encryption are the two main functions performed by this algorithm.

Substitution boxes are independent of the keys. Blowfish required more processing time because of varying key length. The time consuming sub-key generation process increases the complexity for a brute-force attack. It provides long term data security without any known backdoor vulnerability. Reliability of Blowfish is damaged due to the use of large number of weak keys. The first 4 rounds of process are exposed to 2nd order of differential attacks.

## *INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)*

IDEA is a symmetric key block algorithm based on substitution and permutation structure which performs 8.5 rounds of process where each round performs XOR, addition and multiplication. It is derived from Proposed Encryption Algorithm and uses 64 bit block, 128 bit key for encryption [7]. IDEA is very strong against differential cryptanalysis under a specific hypothesis. The strength of IDEA against many attacks is increased by using multiple group operations. The 128 key size makes IDEA much stronger. IDEA is not yet cracked by linear or algebraic attacks, but it is exposed to a possible collision attack. The first 3 rounds among the 8 rounds of process are exposed to key-schedule attacks and key-related differential timing attacks.

## *ADVANCED ENCRYPTION STANDARD (AES)*

AES is also a block cipher algorithm based on Feistel network, which uses 128 bits block size and varying key length of 128, 192 and 256 bits. Depend on the key length the number of rounds performed for encryption varies between 10, 12, or 14 rounds. Each AES round performs Key expansion, Sub-byte generation, Column-mix and Add-round key. AES provides a high security level since uses variable length key bits. It uses operations similar to the RSA modulo arithmetic operations but it can be mathematically inverted. Security of the encryption depends on how long it takes to crack and how high cost will it take an attacker to find a key? Different types of attack to crack AES like Square attack, Key attack, and Differential attack were tried, but none of them cracked AES algorithm [4]. The combined boomerang and rectangle attack with related key differentials uses the weakness of few non-linear transformations in key-schedule algorithms and can break some reduced round versions of AES [4]. It can break 192-bit, 9 rounds AES by using 256 different related keys.

## *RC6*

RC6 is based on Feistel Structure, derived from RC5 which uses 128 bit block size and varying key size of 128, 192 or 256 bits with 20 processing rounds.RC5 and RC6 differs by the number of registers used (2 and 4 respectively) [2]. It is an evolutionary improvement of RC5 and is highly resistant to differential and cryptanalytic attack. It is a secure, compact simple block cipher whose code and data can readily fit in cache memory [2]. This increases the performance and provides flexibility. The security in RC6 is provided by the rotation amounts during processing. The brute-force attack appears to be infeasible if the key size large and the estimated round of 20 is recommended. RC6 is vulnerable to differential and brute force attack if the key size is small. Time consumption for process in RC6 is high.

### *RSA*

RSA is a public key cryptographic algorithm, known as asymmetric cryptography. The asymmetry of the key is based on factoring the product of two large prime numbers. Messages encrypted with the public key can be decrypted in a reasonable amount of time using the private key. Modulus and exponent operations are performed to generate public and private key. The security of RSA cryptosystem is based on factoring large numbers and taking the eth root modulus of a composite n, finding a value m such that C=m^e(mod n) where (n,e) is a public key and C is the cipher text. If the attacker computes the secret exponent d from a public key (n,e), C can be decrypted using the standard procedure. But naturally it is time consuming to find the integer factorization in a polynomial time, which still proves RSA to be a strong algorithm [3]. Using Small and relatively close primes:

- IF the primes are small enough then the factorization of n will be an easy task.
- IF p and q are relatively close then, finding out the common factors reveals the public key.

It consumes longest encryption time and memory usage which ultimately slows down the speed of the algorithm [5].

## COMPARISON OF CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS PARAMETERS

Among the many existing cryptographic algorithms, DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC6 and RSA are selected and compared on the basis of structure, security, flexibility to expand in future and limitations [6], [7]. Table 1 illustrates the comparative study on selected algorithms.

**Table 1:** Qualitative measures

| Algorithm | Structure | Flexibility and Modification | Known Attacks |
|---|---|---|---|
| DES | Feistel | NO | Brute Force Attack |
| 3DES | Feistel | YES, Extended from 56 to 168 bits | Brute Force Attack, Chosen Plaintext, Known Plaintext |
| CAST-128 | Feistel | YES, 128 and 256 bits | Chosen Plaintext Attack |
| BLOWFISH | Feistel | YES, 64-448 key length in multiplies of 32 | Dictionary Attack |
| IDEA | Substitution-Permutation | NO | Differential Timing Attack, Key-Schedule Attack |
| AES | Substitution-Permutation | YES, 256 key length in multiples of 64 | Side Channel Attack |
| RC6 | Feistel | YES, 128-2048 key length in multiples of 32 | Brute Force Attack, Analytical Attack |
| RSA | Factorization | YES, Multi Prime RSA, Multi power RSA | Factoring the Public Key |

Security in cryptography is based on how secure the algorithm is against various attacks. The performance of these cryptographic algorithms are based on structure, key length, block size, number of rounds used, and cryptographic time. Ultimately, these are the factors which affects the security of a particular algorithm. The block size plays a vital role in encryption and decryption, which is the basic unit of data (see Figure 2).


**Figure 2:** Quantitative measures – Block Size (Bits)

Larger block size provides higher security when other factors were considered to be equal in some algorithms. AES uses block size of 128 bits which is twice bigger than all other symmetric algorithms in discussion. Another critical evaluation is on number of rounds used for encryption/decryption process (see Figure 3).

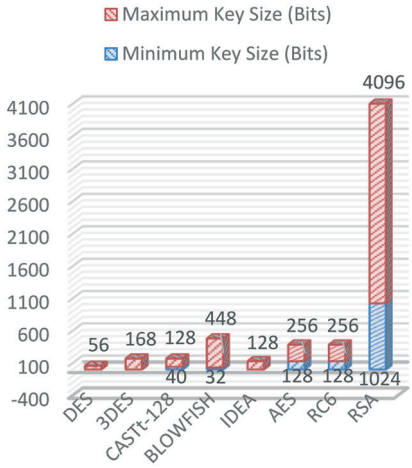


**Figure 3:** Quantitative measures – Key Size (Bits)

Increase in processing rounds, strengthens the security as single Feistel round provides inadequate security. DES and BLOWFISH has 16 rounds of process. 3DES has 3 times of DES (48 rounds). AES has varying number of rounds depending of key size. RC6 is the best candidate which has 20 rounds of process as for as this criterion is concerned. The major issue with symmetric key algorithms is a brute force attack, where all possible keys are tried until the exact key is found to decrypt the message. Longer key lengths reduce the feasibility of attacks, since the number of key combinations increase (see Figure 4).

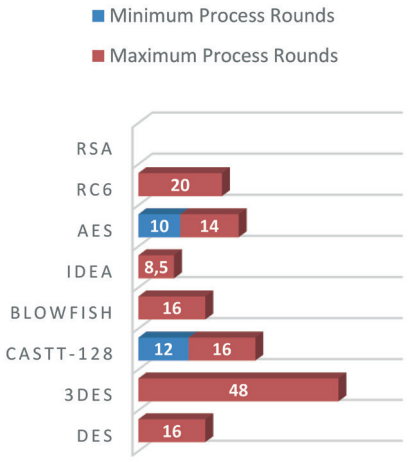


**Figure 4:** Quantitative measures – Key Size (Bits)

DES has a weak key of 56 bits. CAST-128, IDEA use 128 bits key which is considered to be average key strength. 3DES has 168 bits key with good resistance against attack. RC6 and AES has variable key lengths of 128, 192, and 256 which provide a larger number of key combinations. BLOWFISH uses 448 bit keys which are considered to be longest and strongest as far as brute force attacks are concerned.

In asymmetric RSA, a key exchange is not needed and this increases the security of the algorithm. RSA uses factorization for the cryptographic process which significantly reduces the speed of the algorithm. Symmetric algorithms like AES, BLOWFISH, and RC6 are much faster than RSA. Security of the cryptosystem is defined by a secured encryption scheme to guard against brute force attacks and differential plaintext-cyphertext attack. Though CAST-128, IDEA, DES, 3DES are faster, they are less secure due to weak keys.

The analysis shows in case of symmetric algorithms RC6, Blowfish and AES that they are considered to be secure and efficient based on high security and less limitations. The expansion and flexibility of RC6, Blowfish and AES are high compared to other symmetric algorithm. The comparison of symmetric and asymmetric keys show that RSA is more secure than any symmetric cryptographic algorithm.

# CONCLUSION

This paper provides an analytical study on various symmetric encryption algorithms such as DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC6 and asymmetric RSA Algorithm. The analysis is based on the architecture of the algorithms, the security aspects and the limitations they have. The comparison clearly states that though asymmetric algorithms are superior in security, they take more time for processing and requires more memory. Practically, asymmetric algorithms like RSA are used for the key exchange and symmetric algorithms are used for encryption/decryption. Further, general implementation limitations of cryptographic algorithm emphasis the selection between hardware and software cryptosystem, choosing among symmetric and asymmetric key algorithm and the essential factors to be followed to have a secure key management. Efficient cryptosystems can be provided by applying more than one algorithm as a hybrid cryptosystem which provides high security and secure data transfer.

## *REFERENCES*

[1] Agrawal, M. and Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. *International Journal on Computer Science and Engineering*, vol. 4, no. 5, p. 877.

[2] Apoorva, Y. K. (2013). Comparative study of different symmetric key cryptography algorithms. *International Journal of Application or Innovation in Engineering and Management*, vol. 2, no. 7, pp. 204-6.

[3] Arora, S. (2015). Enhancing Cryptographic Security using Novel Approach based on Enhanced-RSA and Elamal: Analysis and Comparison. *International Journal of Computer Applications*, vol. 112, no. 13.

[4] Daemen, J. and Rijmen, V. (1999). AES Proposal: Rijndael. AES Algorithm Submission, September 3, http://www.nist.gov/CryptoToolKit

[5] Joseph, D. P., Krishna, M. and Arun, K. (2015). Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Research in Computer Science*, vol. 6, no. 3.

[6] Mandal, A. K., Parakash, C. and Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 2012*.

[7] Nadeem, A. and Younus Javed, M. (2005). A performance comparison of data encryption algorithms. *Information and communication technologies, 2005. ICICT 2005. First international conference on. IEEE*.

[8] Salama, D. et al. (2008). Performance Evaluation of Symmetric Encryption Algorithms.

[9] William, S. (1999). Cryptography and network security: principles and practice, pp. 23-50, Prentice-Hall, Inc.