

# Survey of Performance Comparison of DES, 3DES and AES Algorithms

Chiranth B O

Dept. of Computer Science & Engg  
B.T.L. Institute of Technology  
Bangalore, India

Shashikala B

Dept. of Computer Science & Engg  
B.T.L. Institute of Technology  
Bangalore, India

## ABSTRACT

Today cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without worries of deceit and deception. Every day hundreds of thousands of people interact electronically, whether it is through e-mail, e-commerce (business conducted over the Internet), ATM machines, or cellular phones. The perpetual increase of information transmitted electronically has led to an increased reliance on cryptography. In this paper of survey about DES, 3DES and AES, DES uses 56-bit key length nowhere DES algorithm can be cracked but the only way is by brute force technique, where it takes around 400 days to decrypt at a rate of 2-billion keys per sec. 3DES uses 112-bits by brute force it takes 800 days to decrypt the message at the same rate. But when it come to AES it uses 256-bit key length even the brute force fails because it takes  $5 \times 10^{21}$  days to decrypt at the same rate. So AES is the best-known encryption standard.

## Index Terms

Data Encryption Standard; Triple Data Encryption Standard; Advance Encryption Standard.

## 1. INTRODUCTION

DES, 3DES & AES is used for protecting information from undesirable folks by translating it into a non-recognizable form to its attackers while both stored and transmitted [1]. Data cryptography mainly is the climbing of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unlicensed assailants. In modern days cryptography is no longer limited to secure sensitive R&D, military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources, and electronic financial transactions. Which recuperate the original data. Since cryptography first known usage in ancient Egypt it has passed through different stages and was affected by any major event that affected the way people handled information. In the World War II for instance cryptography played an important role and was a key element that gave the allied forces the upper hand, and enables them to win the war sooner, when they were able to dissolve the Enigma cipher machine, which the Germans used to encrypt their military secret communications.

The hurried development in various hypermedia technologies, also the Internet allows for wide dissemination of digital media data. It becomes much easier to edit, modify and replicate digital information. Besides that, digital documents are also easy to copy and distribute, therefore it will be faced by many terrorizations. It is a big security and privacy issue, it become necessary to find appropriate protection because of the significance, accuracy and sensitivity of the information, Which may include some sensitive information which should not be

accessed by or can only be partially exposed to the general users. Therefore, safety and confidentiality has become an important issue. Another problem with digital document and video is that untraceable modifications can be made with very simple and widely available equipment, which put the digital material for evidential purposes under question. Cryptography considers one of the techniques, which used to protect the important information. In this paper a three algorithm of multimedia encryption schemes have been proposed in the literature and description. The New Comparative Study between DES, 3DES and AES within Nine Factors achieving an efficiency, flexibility and security, which is a challenge of researchers. Original data that to be transmitted or stored is called plaintext, also the one that can be readable and understandable either by a person or by a computer. Whereas the disguised data so-called ciphertext, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem [3]. Cryptosystem uses an encryption algorithm, which determines how simple or complex the encryption process will be, the necessary software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data [3], [4]. In the 19th century, Kirchhoff has proposed a famous theory about the security principle of any encryption system. This theory has become the most important principle in designing a cryptosystem for researchers and engineers. Kirchhoff observed that the encryption algorithms are supposed to be known to the opponents [5].

Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. For even though in the very beginning the opponent doesn't know the algorithm, the encryption system will not be able to protect the ciphertext once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space [6]. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. In encryption, the key is piece of information (value of comprise a large sequence of random bits), which specifies the particular transformation of plaintext to ciphertext, or vice versa during decryption. The larger key space the more possible keys can be constructed (e.g. today we commonly use key sizes of 128,192,or 256 bit , so the key size of 256 would provide a 2256 key space) [5],[6]. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together [6]. Depend on the algorithm, and length of the key, the strength of encryption can be considered. Assume that if the key can be broken in three hours using Pentium 4 processor the cipher consider is not strong at all, but if the key can broken with thousand of multiprocessing systems within a million years, then the cipher is pretty darn strong. There are two encryption/decryption key types: In some of encryption technologies when two end points need to communicate with one another via encryption, they must use the same algorithm, and in the most of the time the same key, and in other encryption technologies, they must use different but related keys for

encryption and decryption purposes. Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys).

## 2. CRYPTOGRAPHY WITH BLOCK CIPHER

In Cryptography, a block cipher is a symmetric key cipher, which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and outputs a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input — the secret key [7]. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of cipher text together with the secret key, and yields the original 128-bit block of plaintext. To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used. Block ciphers can be contrasted with stream ciphers; a stream cipher operates on individual digits one at a time and the transformation varies during the encryption. The distinction between the two types is not always clear-cut: a block cipher, when used in certain modes of operation, acts effectively as a stream cipher as shown in Fig 1.

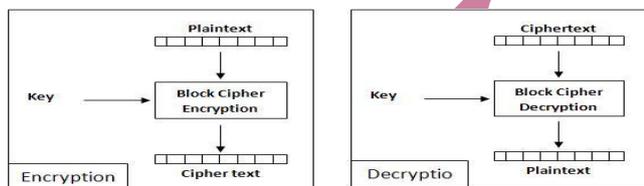


Fig 1: Stream Cipher

An early and highly influential block cipher design is the Data Encryption Standard (DES). The (DES) is a cipher (a method for encrypting information) Selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm was initially controversial, with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor.

DES consequently came under intense academic scrutiny, and motivated the modern understanding of block ciphers and their cryptanalysis. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours. There are also some analytical results, which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the Advanced Encryption Standard has superseded the cipher.

## 3. DATA ENCRYPTION STANDARD (DES)

DES is a Feistel-type Substitution-Permutation Network (SPN) cipher, specified in FIPS PUB 46. The result of a 1970s effort is to produce a U.S. encryption standard. DES uses a 56-bit key, which can be broken using brute-force methods, and is now considered obsolete. A 16 cycle Feistel system is used, with an overall 56-bit key permuted into 16 48-bit sub keys, one for each cycle. To decrypt, the identical algorithm is used, but the order of subkeys is reversed. The L and R blocks are 32 bits each, yielding an overall block size of 64 bits. The hash function "F", specified by the standard using the so-called "S-boxes", takes a 32-bit data block and one of the 48-bit subkeys as input and

produces 32 bits of output. Sometimes DES is said to use a 64-bit key, but 8 of the 64 bits are used only for parity checking, so the effective key size is 56 bits [9].

Since the time DES was adopted (1977), it has been widely speculated that some kind of backdoor was designed into the cryptic S-boxes, allowing those "in the know" to effectively crack DES.

Time has proven such speculation idle. Regardless of any backdoors in the hash function, the rapid advances in the speed of electronic circuitry over the last 20 years, combined with the natural parallelism of Feistel ciphers and DES's relatively small key size, have rendered the algorithm obsolete. In 1998, the Electronic Frontier Foundation built a DES Cracker (full specifications available online) for less than \$250,000 that can decode DES messages in less than a week [7],[8],[9].

## 4. TRIPLE DES

Triple DES was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques such as those used by the EFF DES Cracker. Triple DES has always been regarded with some suspicion, since the original algorithm was never designed to be used in this way, but no serious flaws have been uncovered in its design, and it is today available cryptosystem used in a number of Internet protocols [8], [9].

## 5. ADVANCED ENCRYPTION STANDARD (AES)

In the late 1990s, the U.S. National Institute of Standards and Technology (NIST) conducted a competition to develop a replacement for DES. The winner, announced in 2001, is the Rijndael (pronounced "rhine-doll") algorithm, destined to become the new Advanced Encryption Standard. Rijndael mixes up the SPN model by including Galios field operations in each round. Somewhat similar to RSA modulo arithmetic operations, the Galios field operations produce apparent gibberish, but can be mathematically inverted. AES Security is not an absolute; it's a relation between time and cost. Any question about the security of encryption should be posed in terms of how long time, and how high cost will it take an attacker to find a key?

Currently, there are speculations that military intelligence services possibly have the technical and economic means to attack keys equivalent to about 90 bits, although no civilian researcher has actually seen or reported of such a capability. Actual and demonstrated systems today, within the bounds of a commercial budget of about 1 million dollars can handle key lengths of about 70 bits.

An aggressive estimate on the rate of technological progress is to assume that technologies will double the speed of computing devices every year at an unchanged cost. If correct, 128-bit keys would be in theory be in range of a military budget within 30-40 years. An illustration of the current status for AES is given by the following example, where we assume an attacker with the capability to build or purchase a system that tries keys at the rate of one billion keys per second.

This is at least 1000 times faster than the fastest personal computer in 2004. Under this assumption, the attacker will need



- Network Security, 2009, Vol.1, No.1, ISSN: 1985-1553, P.P 71-76.
- [3] A.W.Naji, A.A.Zaidan, B.B.Zaidan, Shihab A, Othman O. Khalifa, " Novel Approach of Hidden Data in the Using Computation (IJCSNS) , Vol.9, No.5 , ISSN : 1738-7906, pp. 294-300.
- [4] Anas Majed Hamid, Miss Laiha Mat Kiah, Hayan .T. Madhloom, B.B Zaidan, A.A Zaidan," Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis".
- [5] A.A.Zaidan, Fazidah. Othman, B.B.Zaidan, R.Z.Raji, Ahmed.K.Hasan, and A.W.Naji," Securing Cover-File without Limitation of Hidden Data Size Using Computation between Cryptography and Steganography ", World Congress on Engineering 2009 (WCE), The 2009 International Conference of Computer Science and Engineering, Proceedings of the International.
- [6] A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman and B.B. Zaidan, " Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ",International Conference on IACSIT Spring Conference (IACSIT-SC09) , Advanced Management Science (AMS).
- [7] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji, and S.M.Mohammed," Implementation Stage for High Securing Cover- File of Hidden Data Using Computation Between Cryptography and Steganography", Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Vol.19, Session 6, p.p 482-489.
- [8] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for CoverFileof Hidden Data in the Unused Area Two within EXE File Using Distortion Techniques and Advance Encryption Standard.", Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 498-502.
- [9] M. Abomhara, Omar Zakaria, OthmanO. Khalifa , A.A.Zaidan, B.B.Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore..
- [10] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " Novel Framework for Hidden Data", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.
- [11] Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File", International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria
- [12] Alaa Taqa, A.A Zaidan, B.B Zaidan , "New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm", International Journal of Computer and Electrical Engineering (IJCEE),Vol.1 ,No.5, ISSN: 1793-8163, p.p.566-571 , December (2009). Singapore.
- [13] A.A.Zaidan,B.B.Zaidan,Hamid.A.Jalab,"ANewSystemforHiding Data within (Unused Area Two + Image Page) of Portable Executable File using Statistical Technique and Advance Encryption Standard ", International Journal of Computer Theory and Engineering (IJCTE), 2010, VOL 2, NO 2, ISSN:1793-8201, Singapore.