International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.241-246
http://dx.doi.org/10.14257/ijsia.2015.9.7.21

# A Comparison of the 3DES and AES Encryption Standards

Noura Aleisa

*n.aleisa@seu.edu.sa*

***Abstract***

*A comparison of two encryption standards, 3DES and AES is presented. It may seem that DES is insecure and no longer of any use, but that is not the case since the DES and 3DES algorithms are still beyond the capability of most attacks in the present day. However, the power of computers is increasing and stronger algorithms are required to face hacker attacks. AES has been designed in software and hardware and it works quickly and efficiently, even on small devices such as smart phones. With a large block size and a longer keys, AES will provide more security in the long term.*

***Keywords:*** *encryption, cryptography, cryptology, algorithm, cryptanalysis, AES, 3DES*

## 1. Introduction

It may be surprising to discover that encryption has been known for thousands of years, and methods have varied from those simply based on paper and pencil to others using more complex and specialized mechanical equipment, and today has resulted in the use of computer techniques, encryption applications, and digital signatures.

4000 years ago, the Egyptians used hieroglyphic symbols to confuse the reader and this is believed to be the first attempt at cryptography. Several other ancient civilizations have also been found to have used cryptography techniques. For instance, the Arabic civilization discovered cryptanalytic techniques and were the first to publish a systematic analysis of cryptography. Another example is the great civilization of India, which has been shown to have used numerous forms of cryptographic communication. They used a finger communication system similar to the sign language or signing used by the hearing and speech impaired today [7]. Cryptography is derived from the Greek word crypto, which means secret, hidden, or concealed. The idea of cryptography is to allow two people to communicate using a secure method in such a way that prevents an outsider from understanding their messages. It is the art of secret writing which allows the passage of information in hidden form so that only authorized people are able to understand it.

In the present day, any secure communication environment would not be complete without cryptographic methods. Cryptology can provide a high level of security to any sensitive information that needs to be protected, such as in emails, file transfers, saved information on hard disks, backups, and so on. Cryptography is extremely important in wireless communication because it is easier to break into than a hard-wired network.

The goal of this paper is to present the reader with an introduction to traditional encryption, the benefits and drawbacks of encryption to the non-professional user, the security provided by the data encryption algorithm 3DES against attackers, and to discuss its merits in comparison with one of the first cyphers, AES. In this section, the world of cryptography is introduced and a brief description of its history is mentioned. In the second part, the advantages and disadvantages of using different encryption systems are discussed. In the third part, the 3DES system and its security issues are explained. Finally, I have introduced the reader is introduced to a comparison between 3DES and AES.

ISSN: 1738-9976 IJSIA

## 2. Encryption Methodology

There are many reasons why we might want to encrypt data. For instance, individuals may share the same work space with people they don't trust. Another reason, in the business world, is as an extra security layer for a company's sensitive data, such as financial data, because this information might be of benefit to its competitors. Furthermore, two people might want to ensure privacy in an email conversation, transporting important information on a hard disk or a computer could be easy prey to competitors without encryption, and companies might use encryption to store sensitive personal data on their clients, such as credit cards information, and medical records.

Cryptology consists of both encryption and decryption; the original information is referred to as "plaintext", and the encrypted information as "ciphertext". To convert the plaintext to ciphertext an algorithm needs to be implement using a secret key to guarantee security and create a digital signature. To encrypt plaintext to ciphertext, two types of keys are available: symmetric or asymmetric.

### 2.1 Symmetric Key Encryption

Symmetric or single secret key encryption is one of the oldest encrypting methods and is usually as simple as shifting the letters of the text by a specific number. Symmetric keys provide only a single key for the encryption and decryption processes which can be a number, a word, or random letters, and anyone with the key will have the ability to decrypt the ciphertext. The difficulty in this process is delivering the key from the sender to the recipient and ensuring that the recipient has received the key. If the key is lost or obtained by a third party then the encrypted data become unavailable. One of the great benefits of the secret key system is the ability to translate passwords easily with the key and the speed of encryption. When compared to the asymmetric key system, the symmetric key system is an attractive method since its application doesn't require the external involvement of users.

### 2.2 Asymmetric Key Encryption

The asymmetric key system, also known as public key encryption, is more secure because it is necessary to use two keys, a public and private one, to encrypt and decrypt a text. The public key can be known to anyone, and the receiver will give the sender his public key and the sender will use it to encrypt the text to be sent. The receiver will receive the ciphertext and decrypt it using his private key. The private key is never distributed, which is why the threat from a third party is considerably reduced because without the private key the text can't be decrypted [2]. In order to get the public key to the other person, a digital certificate is needed, which is a data package containing information such as the organization name, certificate issued date, user's email and country, and the public key that determines the personal identity of a user or server. When a securely encrypted communication is required, a query will be sent over the network to the receiver which will send back a copy of the certificate. The public key of the receiver can be extracted from the copy which can also be used to identify the holder [6].

Even though the public and private keys in asymmetric cryptography have solved the security problem of sending the key, it still has drawbacks in the area of security. Firstly, public key encryption is much slower than single secret key encryption. Secondly, it is only efficient for a small amount of data such as email, but not for bulk encryption. Another disadvantage is the key validation problem; the published public-key could be created for a specific person A but by another person B, so when someone wants to send an encrypted message to A using his public key it will be sent to B instead. B can then decrypt it with his private key and read a message. If we assume that B knows the real public key of A then he could re-encrypt the message and send it again to A after changing the context of the message. In theory, we can say that B is sitting in the middle

 

of the conversation of two people and he has the ability to delete and modify the content of the messages.

### 2.3 Digital Signatures

The importance of a signature, whether digitally or on paper, to confirm and document the identity of the sender, especially in the sensitive and confidential correspondence, cannot be overstressed. A digital signature does not mean the same thing as a written signature, which may show information such as the sender's name and telephone number. A digital signature is used to authenticate the identity of the sender and, for the encryption mechanism, consists of the following steps. First, the sender generates a text message hash, which uses certain algorithms not to encrypt the text but to generate a unique hash. Changing one character of text (even by just one bit) will change the hash and it would never generate the original text of that hash again. Secondly, the sender will encrypt the generated hash for the text using his secret key and sends the message. Third, the receiver will decrypt the hash using the public key of the sender. Finally, the receiver will generate a new hash for the text and he will compare the two hashes; if they match, it will mean that the sender is certainly the owner of the sender's public key and if they don't that will mean that the message has been hacked. Digital signatures depend on the secret key of the signer which can only be generated by him or herself [1].

## 3. Encryption Algorithms

### 3.1 Data Encryption Standard (DES)

On May 15, 1973, the Data Encryption Standard (DES) was developed at IBM as an improvement on an older system called LUCIFER. DES was designed to work better in hardware than software and is an algorithm which encrypts text in 64-bit blocks with a 56-bit key. The algorithm is applied in three stages. First of all, the plaintext is constructed by permuting the bits of the text $\chi$ based on initial permutation IP which is applied as $x\ 0 = IP\ (\ x\ ) = L\ 0\ R\ 0$ , where $L\ 0$ is the first 32 bits and $R\ 0$ is the last 32 bits. Secondly, sixteen iterations of a specific function that includes permutation and substitution phases are applied. We can write $L_i = R_{i-1}\ R_i = L_{i-1}$ XOR $f\ (R_{i-1}\ ,\ K_i\ )$, where K is the key and f is the function. Finally, an inverse permutation $IP^{-1}$ to the sixteen bit string R and L to obtain the ciphertext using the $y$ = IP -1 ( $R$ 16 $L$ 16 ) formula is utilized [12].

It might seem to be an extremely complicated scheme and the decryption using DES would require a completely different approach, but it might be a surprise to discover that the same algorithm would work to decrypt the same text, the only difference being that the process in decryption is applied in reverse [3].

Since the time DES was adopted in 1977, backdoor DES crackers have been developed that can decode DES messages in less than a week. For instance, a “brute force” attack tries as many keys as possible to decrypt ciphertext into plaintext by attaching a special parallel computer using a million chips that try a million keys each per second. Another attack was recorded in 1998, under the direction of John Gilmore of the EFF( Electronic Frontier Foundation). A machine costing $220,000, called Deep Crack, was built to be able to go through the whole 56-bit key and break it within 5 days by using 46 chips that could test 90 billion keys a second [8].

### 3.2 Double DES

Because DES has already proved that a very competent algorithm can be considered highly insecure and unreliable, methods were sought to reuse it by making it stronger and

more secure, rather than writing a totally new algorithm. Two main improvements have resulted in Double DES and Triple DES or 3DES.

Double DES essentially does twice what DES does with two keys uses in one encryption process. If the attempt to crack the key in DES is $2^{56}$, then the attempts to crack two different keys consisting of n bits is $2^{2n}$. However, that is not quite true since the concept of the meet-in-the-middle attack has been introduced which involves encryption from one end and decryption from the other and matching the outputs in the middle.

### 3.3 Triple or 3DES

With the idea that Double DES may not be strong enough to prevent a meet-in-the-middle attack has led to the development of 3DES, which was developed in 1999 by IBM by a team led by Walter Tuchman [11]. This type of attack is one of the main reasons why double DES was replaced by Triple DES or 3DES, which is DES with three different keys. It is essential to avoid having the same key for the encryption steps since the output will only be a slower version of DES. 3DES has two forms, one requiring three completely different keys and the other only two completely different keys.

The first method uses three keys to encrypt the plaintext, firstly using key k1, followed by encryption with key k2, and lastly a third encryption is carried out with key k3. We perform the operation C = EK3(EK2(EK1(P))) to encrypt the plaintext and P = DK3(DK2( DK1(C))) for decryption. PGP and S/MIME are examples of products that use the three keys 3DES. Even though 3DES uses three keys to provide a high level of security, it still has a drawback since its required 56 * 3 = 168 bits for the keys, which can be difficult to make work in practical situations. Because of this, the method of 3DES using two keys has arisen.

In 3DES with two keys, encryption is applied using key k1, the output of the previous step is decrypted using key k2. Finally, encryption of the output of step 2 is encrypted again using key k1. We perform the operation C = EK1(DK2(EK1(P))) to encrypt the plaintext and P = DK1(EK2(DK3(C))) for decryption. This method is also referred to as Encrypt- Decrypt- Encrypt (EDE) [3].

3DES has advantages over previous algorithms in that it is easy to implement and more secure, but may still not be completely secure. Another advantage is that 3DES can perform single DES encryption if k3= k2= k1, which is sometimes desired in implementations which also support single DES for legacy reasons. 3DES is very efficient in hardware but not particularly in software. It is popular in financial systems as well as for protecting biometric information in electronic passports [8].

However, when addressing security, 3DES has a flaw. With three independent keys, an overall key length of 168 bits is generated, which is a summation of three 56 bit keys that can face a meet-in-the-middle attack. For 3DES with two independent keys, the overall key length is reduced to 112 bits, which might not be sufficient. Nevertheless, this vulnerability will only come into effect with chosen plaintext or known plaintext attacks. In addition, another vulnerability exists that could give an opportunity to a hacker to retrieve a key and reduce the length of it, subsequently reducing the amount of time needed to crack the key.

Attacks on two key 3DES have been documented but the required data made it impractical due to the strong interdependency between the keys [4, 13]. It is still possible to make a successful attack only if the keys are secure enough and a connection between the security of the keys and the text can be made. Another attack was made in 1994 by Matsui and Yamagishi called linear cryptanalysis (LC). This attack was one of the most prominent plaintext attacks against block ciphers. LC uses a linear approximation to describe the behavior of the block cipher and, given sufficient pairs of plaintext and its corresponding ciphertext, key information can be obtained and increasing the data usually

 

gives rise to a higher probability of success. Matsui has successfully obtained a key with 243 known plaintexts [7].

Besides, 3DES is not practical when used to encrypt large messages, and there is the issue of unsafe key transmission between the users. It is considered slow by todays standards and outdated when compared to modern algorithms such as RC6 and Blowfish.

### 3.4 Advanced Encryption Standard (AES)

On January 1997 in the US, the National Institute of Standards and Technology (NIST) announced a contest to develop a new encryption system and asked for some important restrictions. The developed system had to be publicly disclosed, unclassified, free for use worldwide, usable with 128, 192, and 256 bit key sizes, and symmetric block cipher algorithms for blocks of 182 bits [10]. On 26 May 2002, 3DES was replaced by Advanced Encryption standard (AES) [9]. AES and 3DES are commonly used block ciphers, and which one to choose depends on the requirement. AES outperforms 3DES both in software and in hardware.

AES is based on the Rijndael algorithm, created by Joan Daemen and Vincent Rijmen, which is a combination of a strong algorithm with a strong key. The Rijndael block cipher can use different block and key lengths, such as 128, 192, and 256 bit. This versatility can produce faster and more secure symmetric block ciphers. Another algorithm which might be considered as an alternative to the Rijndael block cypher is the Twofish algorithm, which can use blocks of 128 bits with keys up to 256 bits. The Rijndael algorithm's combination of security, performance, efficiency, implementability, and flexibility made it an appropriate selection for AES [7].

## 4. A Comparison of 3DES and AES

In this section, the differences between the two encryption standards are highlighted in terms of security and performance. AES uses three common key lengths, 128, 192, and 256 bits, whereas for 3DES the encryption key is still limited to 56 bits, according to the DES standard. However, since it is equivalent to DES applied three times, the implementer can choose to have either 2 or 3 different 56 bit keys, meaning that 3DES can have encryption key lengths of 168, 112, or 56 bits. However, due to certain vulnerabilities when reapplying the same encryption three times, a 168 bit key has a reduced security equivalent to 112 bits, and using 112 bits has a reduced security equivalent to 80 bits. The bottom line is that 3DES uses identical encryption to DES whereas AES uses a completely different one, 3DES has a shorter length and weaker encryption keys when compared to AES, and 3DES repeatedly applies encryption keys while AES does not.

AES is strongly resistant to differential, truncated differential, linear, interpolation and Square attacks, in contrast to 3DES which is vulnerable to differential and linear cryptanalysis and it has weak substitution tables. In addition, the time required to check all possible keys at 50 billion keys per second in AES for a 128-bit key is 5 x 1021 years, whereas 3DES with a 56 bit key would take 400 days. In addition, 3DES uses a block length of 64 bits which is half the size of an AES block length of 128 bits.

Another drawback when using 3DES is the need to switch encryption keys after every 32 GB of data transfer to reduce the possibility of leaks. Conversely, using AES provides additional insurance since it is difficult to decypher data from identical blocks. The process of 3DES encryption using 3DES is much longer than AES, because repeating the same encryption process three times in 3DES takes some time when compared to the AES encryption process which is much faster. However, this rule does not apply when we include software and hardware. If we used 3DES with accelerated hardware that departs to software implemented by AES, the results might be slower. In this case we have to measure each one's speed separately.

## 5. Conclusions

When it comes to security, the winner is undoubtedly AES as it is considered unbreakable in practical use. After discussing the flaws of DES, thus of 3DES as well, it may seem that DES is insecure and no longer of any use, but that is not the case. The 1997 attack required a great deal of cooperation and the 1998 machine is too expensive to implement, and so the DES and 3DES algorithms are still beyond the capability of most attacks in the present day. However, the power of computers is increasing and stronger algorithms are required to face hacker attacks. The response to that requirement is AES. It has been designed in software and hardware and it works quickly and efficiently, even on small devices such as smart phones. With a larger block size and longer keys using a 128 bit block and with 128, 192 and 256 bit keys, respectively, AES will provide more security in the long term.

In conclusion, I am pretty confident that I have learned and introduced the main concepts of traditional cryptography through these four parts. I also believe that I have a general understanding of Triple Data Encryption Standards and its security issues comparing with Advanced Encryption Standards.

## References

[1] H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications", Springer-Verlag, Berlin Heidelberg New York, **(2007).**
[2] M. E. Flannagan, R. Fuller and J. Khan, "Best Damn Cisco Internet-working Book Period", Syngress Publishing, Rockland, **(2003).**
[3] A. Kahate, "Cryptography and network security", The Tata McGraw-Hill publishing company limited, New Delhi, **(2003).**
[4] R. C. Merkel and M. E. Hellman, "On the Security of Multiple Encryption", Communications of the ACM, vol. 24, no. 7, **(1981).**
[5] E. Maiwald, "Network Security: A beginner's Guide", Osborne-McGraw Hill, **(2001).**
[6] Microsoft support, Description of Symmetric and Asymmetric Encryption, ‹http://support.microsoft.com/›, **(2007).**
[7] R. A. Mollin, "Codes: The Guide To Secrecy From Ancient To Modern Times", Chapman and Hall/CRC, Boca Raton, **(2005).**
[8] C. Paar, J. Pelzl and B. Preneel, "Understanding Cryptography: A Textbook for Students and Practitioners", Springer Heidelberg Dordrecht, Bochum, **(2010).**
[9] V. K. Pachghare, "Cryptography and information security", PHI learning Private limited, New Delhi, **(2009).**
[10] C. P. Pfleeger and S. L. Pfleeger, „Security in Computing", Pearson education, Inc., New Jersey, **(2003).**
[11] T. Sobh, K. Elleithy and A. Mahmood, "Novel Algorithms and Techniques In Telecommunications", Automation and Industrial Electronics. Springer Science+ Business Media B. V., Bridgeport, **(2008).**
[12] D. R. Stinson, "Cryptography", Theory and Practice. CRC Press, Inc., Boca Raton, **(1995).**
[13] P. Van Oorschot and M. J. Wiener, "A Known-Plaintext Attack on Two-Key Triple Encryption", Springer- Verlag, Berlin Heidelberg New York, **(1990).**

 