ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ANALYSIS OF THE SECURITY OF AES, DES, 3DES AND IDEA NXT ALGORITHM

Prashant Kumar Dey*, Tarun Kumar Dey
* Department of Electronics (ETC), KIIT University, Bhubaneshwar-751024, Odisha, India.
Post Graduate Department of Physics,L.S College, B.R.A Bihar University,Muzaffarpur-842001, Bihar, India.

ABSTRACT

In the modern cryptography symmetric encryption is widely used since it is faster than public key encryption therefore it is used in various internet communication like Transport Layer Security (TLS) and Internet Protocol security (IPSec) use for session keys, used for sending confidential mail etc. So it becomes important to take major action for the security of symmetric key encryption. In the present paper, we have discussed the various forms of symmetric encryption and their security. We have further analysed the common attacks on these symmetric encryptions.

KEYWORDS: cryptography, encryption, security.

INTRODUCTION

Cryptography, an art which protects information from undesirable individuals by converting it into such a form which cannot be recognized by attackers when it is being transmitted or is stored [1]. The cryptography consists of two main term, plain text and the cipher text. The plaintext is referred to the actual text which is to be encrypted into the cipher text. While method for changing the plaintext into cipher text is called as cipher, the term Encryption is just the implementation of the cipher. Another word associated is the Decryption which is just the reverse of encryption i.e., transforming the cipher text back into readable plain text. Doing this helps us to achieve four primary security goals (before it was three), Confidentiality, Integrity, Availability and Non-Repudiation. Confidentiality also known as Privacy, this ensures that computer related information can only be accessed by the authorized party. This prevents unauthorised disclosure. Availability means that the information is only accessible to the person who is authorized for it and all the time they need it. Integrity makes sure that the information can only be modified by the authorized parties or in an authorized way. Non-repudiation is usually used when message and content are binded to individuals. Modifications in the message includes writing, changing, deleting and creating.

Modern Cryptography includes two form of encryption, symmetric key encryption and asymmetric key encryption. In symmetric key encryption, same key used to encrypt and decrypt information. The keys may be identical or share some information which is common in both the keys. Here both the parties are required to have the key in order to encrypt or decrypt. On the other hand, Asymmetric cryptography is a method in which a pair of keys is used to encrypt and decrypt a message to stay secure. Initially, a user gets a different public and private key pair from a certificate authority. Any user who wants to send an encrypted message can get the public key of the intended recipient from a public directory. User uses this key to encrypt the message and send it to the recipient. Recipient gets the message and decrypt it with private key, which no one else can have access to.

REASON OF THE WORK

In our present work, we will be discussing the various forms of symmetric key algorithm and will emphasize on their security. We have mainly two types of symmetric key encryption, Stream cipher and Block cipher. Stream ciphers encrypts each byte of a message at a time. Block ciphers take a number of bits at a time and then encrypt them as a single text, the plain text are padded so that it is the size of multiple blocks.

Symmetric keys are very common and are reused in many day to day computing. It is used in session keys for confidential online communications like Transport Layer Security (TLS) and Internet Protocol Security (IPSec) protocols. They are much faster than public key encryption, it is estimated to be 100 to 1,000 times faster. Symmetric keys are also used to encrypt large amount of data like emails and files like Secure/Multipurpose Internet Mail

Extensions (S/MIME), and also symmetric keys used by Encrypting File System (EFS) to encrypt files for confidentiality.

We will discuss only the security of some of the major encryption of symmetric block cipher.

DATA ENCRYPTION STANDARD

DES (Data Encryption Standard) developed in 1970s at IBM, based on an earlier design by Horst Feistel. In DES both block size and key length are of 64 bits each. 8 bits are used for checking parity, so effective key length is 56 bits. This has been depicted in Fig 1.

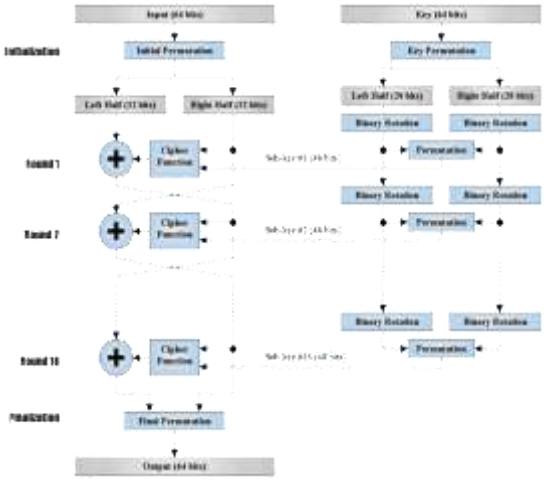

Fig. 1: Analysis of DES

Due to small key size of 56 bits it was very much vulnerable to brute force attacks. In January 1999, DES was publicly broke in just 22hours 15 min. There are other theoretical attacks like Differential cryptanalysis (DC), linear cryptanalysis (LC) and Davies Attack (DA).

TRIPLE DES

Triple DES was developed to address the obvious flaws in DES. 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. In Triple DES no serious flaws have been uncovered, and it is used in a number of Internet protocols [2], [3]. This has been depicted in Fig 2.

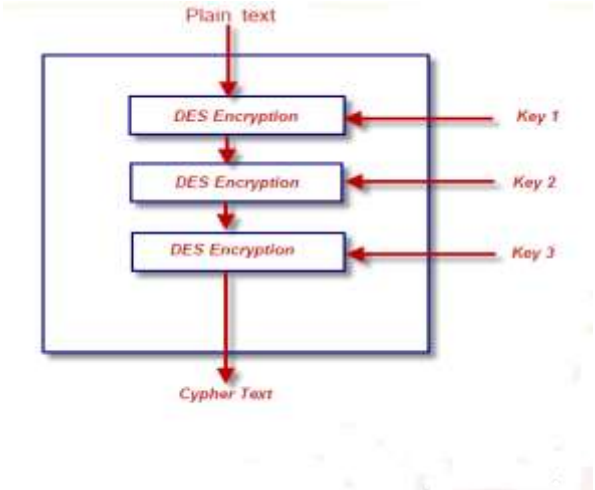

Fig. 2: Working of Triple DES Algorithm

The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV).

Microsoft OneNote,[4] Microsoft Outlook 2007[5] and Microsoft System Center Configuration Manager 2012[6] use Triple DES to password protect user content and system data.

ADVANCE ENCRYPTION STANDARD

AES (Advance Encryption Standard) is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major method matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Cycle of repetition varies as per key length, i.e 10, 12, 14 cycles for 128 bits, 192 bits and 256 bits respectively. Until May 2009, the only successful published attacks against the full AES were side-channel attack on some specific implementations.

INTERNATIONAL DATA ENCRYPTION ALGORITHM:

International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard(IPES), is a symmetric-key block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES). IDEA is a minor revision of an earlier cipher, Proposed Encryption Standard (PES).

IDEA operates on 64-bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a *round*, see the illustration) and an output transformation (the *half-round*). The processes for encryption and decryption are similar. IDEA derives much of its security by interleaving operations from different groups — modular addition and multiplication, and bitwise eXclusive OR (XOR) — which are algebraically "incompatible" in some sense. In more detail, these operators, which all deal with 16-bit quantities, are:

[1] Bitwise eXclusive OR (denoted with a blue circled plus ⊕).
[2] Addition modulo 2^{16} (denoted with a green boxed plus ⊞).
[3] Multiplication modulo $2^{16}+1$, where the all-zero word (0x0000) in inputs is interpreted as 2^{16} and 2^{16} in output is interpreted as the all-zero word (0x0000) (denoted by a red circled dot ⊙).

After the eight rounds comes a final “half round”, the output transformation illustrated below (the swap of the middle two values cancels out the swap at the end of the last round, so that there is no net swap):

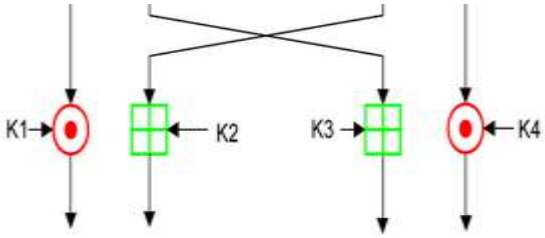

Fig. 3: Working of IDEA

The designers analysed IDEA to measure its strength against differential cryptanalysis and concluded that it is immune under certain assumptions. No successful linear or algebraic weaknesses have been reported. As of 2007, the best attack which applied to all keys could break IDEA reduced to 6 rounds (the full IDEA cipher uses 8.5 rounds).[7] Note that a "break" is any attack which requires less than 2^{128} operations; the 6-round attack requires 2^{64} known plaintexts and $2^{126.8}$ operations. This has been depicted in Fig 3.

In 2011 full 8.5-round IDEA was broken using a meet-in-the-middle attack.[8] Independently in 2012, full 8.5 round IDEA was broken using a narrow-bicliques attack, with a reduction of cryptographic strength of about two bits, similar to the effect of the previous bicliques attack on AES.

IDEA NXT

IDEA NXT algorithm (previously known as FOX) is a block cipher designed by Pascal Junod and Serge Vaudenay of EPFL (Lausanne, Switzerland). It was conceived between 2001 and 2003, the project was originally named FOX and was published in 2003. In May 2005 it was announced by MediaCrypt under the name IDEA NXT. IDEA NXT is the successor to the International Data Encryption Algorithm (IDEA) and also uses the Lai-Massey scheme. MediaCrypt AG holds patents on elements of IDEA and IDEA NXT. The cipher is specified in two configurations: NXT64 (with block of 64 bits, key of 128 bits, 16 rounds) and NXT128 (with block of 128 bits, key of 256 bits, 16 rounds). This has been depicted in Fig 4.

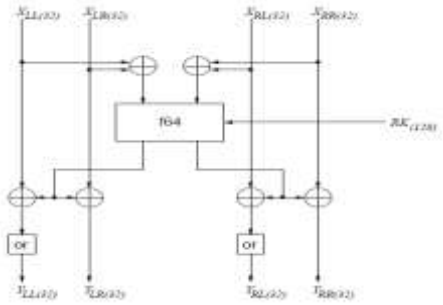

Fig. 4: Working of IDEA NXT

COMPARISON

We have gone through the main symmetric encryption techniques. Through the table we can conclude that AES is widely used algorithm and can be used for the transmission of data effectively and securely rather than using DES or 3DES which can be broken. DES was broken in 1999 within 22 hours and 15 minutes while 3DES was broken using the meet-in-the-middle attack. IDEA NXT which is successor of IDEA has been patent under MediaCrypt and is considered as one of the most secure algorithm as of now. The comparison between DES, 3DES, AES and IDEA NXT has been tabulated in the table 1 below.

Table 1: Comparison between DES, 3DES, AES and IDEA NXT.

	DES	**3 DES**	**AES**	**IDEA NXT**
Developed	1977	1978	2000	2003
Key Length	56 bits	112 bits (k1 and k2) 168 bits (k1, k2, and k3)	128, 192, or 256 bits	0-256 bits
Cipher Type	Symmetric Block cipher	Symmetric Block cipher	Symmetric Block cipher	Symmetric Block cipher
Block Size	64 bits	64 bits	128, 192, or 256 bits	64 or 128 bits
Security	Proven Inadequate	Broken by meet-in-the-middle attack	Considered Secure	High Level of security

CONCLUSION

In this paper a new comparative study between DES, 3DES, AES and IDEA NXT were presented in to five factors, Which are developed, key length, cipher type, block size, security, these eligible proved the AES is better than DES and 3DES and IDEA NXT is also considered as secure but since it has been patent, so one need to take permission before using this.

ACKNOWLEDGEMENTS

We are thankful to Dr. Sucheta Priyabadini, Director Student Services, KIIT University and Avik Gorai, Faculty and Projector Coordinator of Department of electronics, KIIT University for proper guidance on this paper. We are also thankful to Sushant Sagar, Department of Computer Science, Souvik Hazra, Department of Electrical, KIIT University for their continuous support.

We are also thankful to Avinash Singh and Ashutosh Raj from InternetGenx.com who provided us with hosting and domain and encouraged us in this project.

REFERENCE

[1] Tanenbaum, A. S., Computer Networks. New Delhi, Prentice Hall Inc. 2004.
[2] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "Novel Approach for Cover File of 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, Aug 2009, USA.
[3] M. Abomhara, Omar Zakaria, Othman O. 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.
[4] Daniel Escapa's OneNote Blog - Encryption for Password Protected Sections, November 2006
[5] Microsoft - Encrypt E-mail Messages, Outlook 2007
[6] Microsoft TechNet product documentation - Technical Reference for Cryptographic Controls Used in Configuration Manager, October 2012
[7] "IDEA NXT Technical Description" (PDF). MediaCrypt. Archived from the original (PDF) on 28 September 2007
[8] Biham, E.; Dunkelman, O.; Keller, N. "A New Attack on 6-Round IDEA". Springer-Verlag, 2007.