International Research Journal of Computer Science (IRJCS)
Volume 1 Issue 2 (October 2014)
ISSN: 2393-9842
www.irjcs.com

Comparison of Various Encryption Algorithms and Techniques

Ravishankar Belkunde
Senior Database Administrator & Researcher
Boston, Massachusetts, 02108

Abstract: Information Public Sector is more venerable to data theft. To prevent data theft and cyber-attack proper encryption algorithms should be used in the applications and in the relational database management system. In this paper we will see different algorithms used in public sector.

Keywords: Data security, Encryption, Decryption

I. INTRODUCTION

Public sector applications require data security. The data security is achieved at different level using different methods. To secure information data is encrypted. Encryption process converts plaintext into the encoded format cipher text using encryption algorithm. The encrypted data is safe until data is decrypted using decryption algorithm with the encryption key. Here we will see different encryption algorithms used in public sector.

II. ENCRYPTION ALGORITHMMETHODOLOGY

i. Data Encryption Standard(DES)

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations.

ii. International Data Encryption Algorithm (IDEA)

IDEA is a block cipher designed by James Massey and Xuejia Lai and was first described in 1991. It uses 128 bit key length which operates on 64 bit blocks. It consists of a series of eight identical transformations based upon bitwise exclusive-or, addition and multiplication modules. It is based upon symmetric cipher and has very weak key design method therefore security level of the algorithm is very poor as compared to the DES. IDEA not becomes so much popular due to its complex structure.

iii. Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention. Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public, and can be freely used by anyone." Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

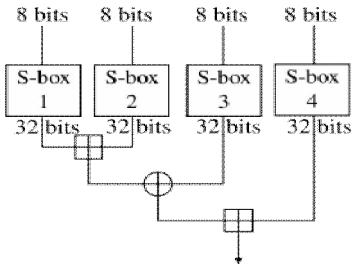

Fig 3: Blowfish Cryptographic Algorithm

iv. Triple DES(TDES)

It was developed in 1998 and derived from DES. It applies the DES cipher algorithm three times to each of the data blocks. Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block.

The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards: All keys being independent Key 1 and key 2 being independent keys All three keys being identical Key option #3 is known as triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.

v. Advanced Encryption Standard (AES)

It is a symmetric 128-bitblock data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM.

While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

vi. Twofish

It was derived from blowfish by Bruce Schneier in 1998. It is freely available in the public domain as it has not been patented. It is a symmetric key block cipher having key sizes 128,192 and 256 bits used to encrypt the 128 bit block size data in 16 rounds. The algorithm making use of S- Boxes and makes the key generation process very complex and secured.

vii. RSA

RSA is a public key system designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. The RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. Two distinct prime number say p&q has been selected randomly and then by using the mathematical properties such as Euler's function, Chinese remainder theorem, hamming weight and exponential functions key has been generated and then encryption process takes place. Decryption has been done in the receiver section by using the public key concept.

RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p&q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p&q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES.

Further, the algorithm also requires of similar lengths for p&q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the systems overheads by taking more processing time.

viii. Diffie-Hellman

Whitfield Diffie and Martin Hellman introduce the key exchange technique in 1976. In 2002, Ralph Merkle's contributed his work in the key exchange program and the technique named as Diffie Hellman Merkle key exchange. In order to tackle man in the middle attacks the Diffie Hellman introduces password authenticated key agreement (PAKE) which was based on generating matrix. When hacker uses single password attack in the iteration; immediately the key structure becomes changed, thus allows only maximum of single password attack in the each iteration by the hacker. This technique helps in achieving better security even in the presence of weak password.

ix. Elliptic Curve Cryptography (ECC)

In 1985, Neal Koblitz and Victor S. Miller suggested the use of ECC for the encryption of data. There are four ECC techniques and stated as: the elliptic curve Diffie Hellman key agreement scheme which uses the key exchange approach suggested by Diffie Hellman scheme and based. Upon the public key cryptography. Second, the Elliptic Curve Integrated Encryption Scheme (ECIES) in which encryption and key generation takes place in one step. Third scheme was based upon the digital signature algorithm and is known as Elliptic Curve Digital Signature Algorithm. MQV key agreement scheme has been used in the ECMQV. The security pattern of ECC is quite remarkable and does not affect by the side channel attacks .Variable key lengths have been used for the encryption and are varied in accordance with the data blocks to provide sufficient amount of cover the data.

x. Pretty Good Privacy (PGP)

In 1991 the Philip Zimmermann developed Pretty Good Privacy (PGP) public key cryptography programs. The algorithm was supported by Linux and Window operating systems. It combines the private and public key cryptography to maintain the appropriate confidential level. The technique can be used to encrypt the e-mail messages with the help of hash and MD5.

xi. Public key infrastructure(PKI)

It is an unsymmetrical cryptography technique used to encrypt the e- mails. The public keys of the users are covered up with the certificates created by trusted third party. From the root level different keys were designed for different users and are always kept unknown from each other.

The first key was generated by the algorithm for the encryption and always kept secret; the second key was generated by the CA on the request of the users and publicly circulated. The user can update their keys and the duplicate copy of the new key was stored at CA.

III. CONCLUSION

We have analyzed different encryption algorithms. The algorithm encrypt data in their own way; one algorithm provides security using extensive hardware resources, other is more secure but use multiple keys where decryption issues may occur, the other have more execution time. One algorithm can't fit all needs, as per the requirement of the applications and business needs encryption algorithms will change, if we fit most secure encryption algorithm in all we may achieve best data security but fail to use them in real time.

REFERENCES

[1]. Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp.5-9.
[2]. Diffiee,W.,andHellman,M.,"NewDirectionsinCryptography",IEEETransactionInformationTheoryIT-2,(Nov.1976),pp. 644-654.

