An Analysis of Symmetric Cryptography Algorithms

Mr. S. Dilip Kumar[1] Mr. V.RamaKrishnan[2]
1Research Scholar [2]Assistant Professor and Head,
[1, 2] Department of Computer Applications
[1, 2] Vidyasagar College of Arts and Science, Udumalpet, India

Abstract— The evaluation of networking and wireless networks has come forward to grant communication anywhere at any time. Security of wireless networks is main aspect and encryption algorithms play an important role to provide the security to the wireless networks. This paper provides a fair performance comparison between the various cryptography algorithms on different settings of data packets.

Keywords: - Cryptography, AES, Blowfish, DES, 3DES, RC2, RC6.

I. Introduction

In recent years internet applications are exploring day by day such as online banking, online shopping, stock market and bill payments etc. Without security these applications are impossible, Encryption Algorithms provides the security to the information which is exchange over internet. The encryption algorithms are usually summarized into two popular types: Symmetric key encryption and Asymmetric key encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt data. The key is distributed before transmission between entities. Therefore, key plays an important role in Symmetric key encryption. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using shorter key.

The representative Symmetric key cryptography algorithms include RC2, DES, 3DES, RC2, RC6, Blowfish, and AES, which use certain- or variable-length key. Asymmetric key encryption is used to solve the problem of key Distribution. In Asymmetric key encryption, private key and public key are used. Public key is used for encryption and private key is used for decryption. However, public key encryption is based on mathematical functions, and is not very efficient for small mobile devices. All the algorithms are extensively used for security of Wireless networks. It is essential to evaluate their performance to ensure their domain applications. It is also significant to facilitate the process of the encryption algorithm.

II. Description Of Various Cryptography Algorithms

Brief definitions of most common Encryption techniques are given as follow:

DES: DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST. DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher.

3DES: 3DES (Triple DES) is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods. Blowfish is block cipher 64-bit which can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish: Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to two fish.

AES: AES is a block cipher .It has variable key length of 128,192, or 256 bits; default 256. It encrypts data blocks of 128bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. This study evaluates four different encryption algorithms DES, 3DES, Blowfish and DES.

III. Comparison Between Aes, 3des, Des, Rc2, Rc6 And Blowfish

DES is the old "data encryption standard" from the seventies. Its key size is too short for proper security (56 effective bits; this can be brute-forced, as has been demonstrated more than ten years ago). Also, DES uses 64-bit blocks, which raises some potential issues when encrypting several gigabytes of data with the same key (a gigabyte is not that big nowadays). 3DES is a trick to reuse DES implementations, by cascading three instances of DES (with distinct keys). 3DES is believed to be secure up to at least "*2112*" security (which is quite a lot, and quite far in the realm of "not breakable with today's technology"). But it is slow, especially in software (DES was designed for efficient hardware implementation, but it sucks in software; and 3DES sucks three times as much).

Blowfish is a block cipher proposed by Bruce Schneier, and deployed in some softwares. Blowfish can use huge keys and is believed secure, except with regards to its block size, which is 64 bits, just like DES and 3DES. Blowfish is efficient in software, at least on some software platforms (it uses key-dependent lookup tables, hence performance depends on how the platform handles memory and caches).

AES is the successor of DES as standard symmetric encryption algorithm for US federal organizations (and as standard for pretty much everybody else, too). AES accepts keys of 128, 192 or 256 bits (128 bits is already very unbreakable), uses 128-bit blocks (so no issue there), and is efficient in both software and hardware. It was selected through an open competition involving hundreds of cryptographers during several years. Basically, you cannot have better than that. A block cipher is a box which encrypts "blocks" (128-bit chunks of data with AES). When encrypting a "message" which may be longer than 128 bits, the message must be split into blocks, and the actual way you do the split is called the mode of operation or "chaining". The naive mode (simple split) is called ECB and has issues. Using a block cipher properly is not easy, and it is more important than selecting between, e.g., AES or 3DES.

After analyzing the most popular symmetric algorithms AES(Rijndael) was found the most secure, faster and better among all the existing algorithm with no serious weaknesses, there are some flaws in symmetric algorithms such as weak keys, insecure transmission of secret key, speed, flexibility, authentication and reliability i.e. in DES, four keys for which encryption is exactly the same as decryption. This means that Original plain text can be recovered, if the encryption is applied twice with one of these weak keys. DES is very slow when implemented in software; the algorithm is best suited to implementation in hardware. Similar is the case in IDEA that involves large class of weak keys facilitating the cryptanalysis for recovering the key. DES and IDEA have the same encryption speed on. Triple DES does not always provide the extra security that might be expected making use of double and triple encryption as well as it is very slow when implemented in software as it is derived from DES and DES on software is already slow, so Triple-DES might be considered safest but slowest. In Blow Fish there are certain weak key that attacks its three-round version, further it is also exposed to a differential attack against its certain variants, it also slow in speed but much more faster than DES and IDEA. While looking at the five finalists of AES no serious weakness was found, however few feeble aspect was highlighted that might be exploit as a molest in near future, such as in AES(Rijndael) a numerical property of the cipher might be exposed into an attack, full RC6 arbitrariness is not achieved, Serpent a bit slower and complex, Twofish possibly suspected to chosen-key attacks and MARS relatively complex to analyze.

IV. Advantages And Disadvantages

A. DES

For many years the well-known cipher DES (Digital Encryption Standard) was the cryptographic standard for unclassified use within the USA. DES has been applied in banks as well as in many software- and hardware products for more than 20 years. One could say that this algorithm is the most widespread cipher at all. Some experts warned that some trapdoor might be built in because the secret service NSA was consulted during the design. Such a trapdoor was never found, although significant theoretical weaknesses which could hardly be exploited in practice were identified shortly after DES was adopted.

The weak point of DES is not its design, but its key size of only 56 bit. This corresponds to about 72,000,000,000,000,000 possible keys. In the seventies (when DES was introduced), this was an astronomical number. Meanwhile hardware has become very fast. In summer 1998 an organization named EFF built and demonstrated a special computer, Deep Crack, that could decrypt a DES-enciphered text within an average time of 4.5 days1. Crypto experts were not surprised, but politically it was a shame: As late as in February 1998 an “expert” explained to the U.S. Congress that DES was practically unbreakable.

B. 3DES

The business community did not believe this, however, and instead started to apply the more secure Triple-DES (3DES) algorithm. 3DES is a threefold DES encryption in which two 56-bit keys are applied. That means a practical security of 112 bits in strength which, as far we know today, should be reasonably secure. Since 1998 the PIN of ATM cards (at least in Germany) is probably computed by 3DES.

C. 3DES over AES

- AES in Galois/Counter Mode (GCM) is challenging to implement in software in a manner that is both performant and secure.
- 3DES is easy to implement (and accelerate) in both hardware and software.
- 3DES is ubiquitous: most systems, libraries, and protocols include support for it.

D. AES over 3DES

- AES is more secure (it is less susceptible to cryptanalysis than 3DES).
- AES supports larger key sizes than 3DES's 112 or 168 bytes.
- AES is faster in both hardware and software.
- AES's 128-bit block size makes it less open to attacks via the birthday problem than 3DES with its 64-bit block size.
- AES is required by the latest U.S. and international standards.

I do not recommend the use of 3DES over AES. DES is considered antiquated, even as 3DES prolongs its life.

E. Blowfish

Blowfish is known to be susceptible to attacks on reflectively weak keys. This means Blowfish users must carefully select keys as there is a class of keys known to be weak, or switch to more modern alternatives like the Advanced Encryption Standard, Salsa20, or Blowfish's more modern successors Twofish and Threefish. Bruce Schneier, Blowfish's creator, is quoted in 2007 as saying "At this point, though, I'm amazed it's still being used. If people ask, I recommend Twofish instead." The FAQ for GnuPG (which features Blowfish as one of its algorithms) recommends that Blowfish should not be used to encrypt files that are larger than 4 Gb.

F. RC2

RC2 is a block cipher that encrypts data in blocks of 64 bits. A block cipher is an encryption algorithm that divides a message into blocks and encrypts each block. The RC2 key size ranges from 8 to 256 bits. SAS/SECURE uses a configurable key size of 40 or 128 bits. (The NETENCRYPTKEYLEN= system option is used to configure the key length.) The RC2 algorithm expands a single message by a maximum of 8 bytes. It can be used in all the modes that DES can be used. A proprietary algorithm developed by RSA Data Security. The algorithm expands a single message by up to 8 bytes. RC2 is a block cipher that encrypts data in blocks of 64 bits.

G. RC6

RC6 is very similar in its design to RC5 and it can be viewed as interweaving of two parallel RC5 encryption processes. The cipher follows the Feistel's approach encryption and its main design goal was to improve its predecessor's security parameters. The original submission of the cipher to the AES contest uses the standard block size

of 128 bits, key lengths of 128, 192 or 256 bits, and it uses twenty encryption rounds. However, similarly to RC5, the cipher has a more general design and it admits a wide variety of block sizes, key lengths, as well as different numbers of rounds. The use of twenty encryption rounds is believed to provide a good security margin and linear cryptanalysis, as well as it was reported to be effective only up to 16 rounds, while differential cryptanalysis theoretically can be used to break up to 12 rounds.

The main performance limitation of RC6 is its reliance on specialised hardware support for multiplication and rotation that is not available on many CPUs, in particular, on RISC and low-end processors. Thus, there is a considerable variety in the cipher's performance results across different hardware platforms. On the other hand, RC6 has favourable memory requirements that make the cipher suitable for implementation on limited-resource devices such as smartcards (although Rijdael still fares better in this respect).

V. Conclusion And Future Scope

This paper presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, RC2, RC6 Blowfish and DES. Firstly it was concluded that Blowfish has better performance than other algorithms followed by AES.3DES has least efficient of all the studied algorithms. In future we can use Encryption techniques in such a way that it can consume less time and power furthermore; I will try to develop stronger Encryption Algorithm with high speed and minimum energy consumption.

References

[1] W.Stallings, ‘’Cryptography and Network Security 4th Ed,’’Prentice Hall, 2005, pp. 58-309.
[2] Ruangchaijatupon, P. Krishnamurthy, ‘’Encryption and Power Consumption in Wireless LANs-N,’’ The Third IEEE Workshop on Wireless LANs -September 27-28, 2001-Newton, Massachusetts.
[3] Coppersmith, D. “The Data Encryption Standard (DES) and Its Strength against Attacks. IBM Journal of Research and Development, May 1994, pp. 243 - 250.
[4] W. Stallings, “Cryptography and Network Security 4th Ed,’’Prentice Hall 2005.
[5] Diaa Salama Abdul. Elminaam, Hatem Mohamed AbdulKader, Mohie Mohamed Hadhoud, “Performance Evaluationof Symmetric Encryption Algorithms”, International Journalof Computer Science and Network Security, Dec 2008.
[6] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” 2005.

