International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 7, July 2013 ISSN 2319 - 4847

Comparative Study of Different Symmetric Key Cryptography Algorithms

Apoorva[1], Yogesh Kumar[2]

[1]M.Tech Student, University Institute of Engineering & Technology, Rohtak, Harayana
[2]Assistant Professor, University Institute of Engineering & Technology, Rohtak, Harayana

Abstract

Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to nonsense. In order to avoid unwanted persons being able to read the information, senders retain the ability to decrypt the information. There are three type of Cryptography: Asymmetric-key cryptography, symmetric key cryptography and hashing. Encryption methods in which both the sender and receiver share the same key is referred to as symmetric key cryptography.

This thesis provides a fair comparison between three most common symmetric key cryptography algorithms: AES, Twofish, CAST-256 and Blowfish. The comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used, as our main concern here is to study the performance of algorithms under different settings,. The comparison is made on the basis of these parameters: speed, block size, and key size.

Keywords: Cryptography, Symmetric key, AES, CAST-256, Blowfish, Twofish.

1. Introduction

In the era of information technology, the possibility that the information stored in a person’s computer or the information that is being transferred through network of computers or internet being read by other people is very high. This causes a major concern for privacy, identity theft, electronic payments, corporate security, military communications and many others. We need an efficient and simple way of securing the electronic documents from being read or used by people other than who are authorized to do it. Cryptography is a standard way of securing the electronic documents.

Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.

Cryptography has been derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". People who study and develop cryptography are called cryptographers and the study of cryptography is called cryptanalysis, or code breaking. Cryptography and cryptanalysis are sometimes grouped together under the umbrella term cryptology, encom-passing the entire subject. There are three type of Cryptography: Asymmetric-key cryptography, Symmetric key cryptography and Hashing.

A class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext is called symmetric key cryptography. The keys may be identical or there may be a simple transformation to go between the two keys. In order to maintain a private information link this algorithms uses key that represent a shared se-cret between two or more parties. This is also called as private key cryptosystems or secret key cryptosystem.

Asymmetric cryptosystems use one key to encrypt a message and a different key to decrypt a message and is also called as public key cryptosystems. Public key systems use two keys such that the public key can be used to encrypt some text that can then only be decrypted using the securely-held private key.

Hash functions, also called message digests and one-way encryption, are algorithms that use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash functions, then, provide a measure of the integrity of a file.

2. Proposed Work

The different types of symmetric key cryptosystem that have been compared have been discussed in this section.

2.1 AES

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. AES does not use a Feistel network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES works on a 4×4 array of bytes, termed as the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that converts the input plaintext into the final output of ciphertext.

Each round consists of several processing steps, including one that depends on the encryption key. To transform ciphertext back into the original plaintext using the same encryption key, a set of reverse rounds are applied.

2.2 BLOWFISH

Blowfish is a secret-key block cipher. It is a 64-bit block cipher with a variable key length varying from 32 bits to 488 bits. It is a 16-round Fiestal network. It is much faster than IDEA and DES, unpatented and royalty free.

This algorithm consists of two parts: a key-expansion part and a data- encryption part. Variable-length key of at most 56 bytes (448 bits) is converted into several sub key arrays totaling 4168 bytes by Key Expansion. Data encryption occurs via a 16-round Feistel network. A key-dependent permutation and a key- and data-dependent substitution both are contained in each round of data encryption. The additional operations are four indexed array data lookups per round. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub keys are stored in cache.

2.3 TWOFISH

Twofish is a 128-bit block cipher that accepts key of length varying up to 256 bits. The cipher is a 16-round Feistel network with a bijective F function made up of four key-dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum distance separable matrix over GF(28), a pseudo-Hadamard transform, bitwise rotations, and a carefully designed key schedule. A fully opti-mized implementation of Twofish encrypts on a Pentium Pro at 17.8 clock cycles per byte, and an 8-bit smart card implementation encrypts at 1660 clock cycles per byte. Twofish can be implemented in hardware in 14000 gates. A wide variety of tradeoffs between speed, software size, key setup time, gate count, and memory is permitted by the design of both the round function and the key schedule. We have extensively cryptanalyzed Twofish; our best attack breaks 5 rounds with 222.5 chosen plaintexts and 251effort.

Twofish Characteristic:

i. A 128-bit block cipher.

ii. Key lengths can be of 128 bits, 192 bits and 256 bits.

iii. No weak keys.

iv. Efficiency and speed on both, software (PIII pro etc.) and hardware (smartcard etc.) platforms.

v. Flexible design

vi. Accepts additional key lengths (all key lengths up to 256 bits with leading zeros filled in).

vii. Implementable on variety of platforms.

viii. Suitable for stream-ciphering also.

ix. Also usable for hash function and MAC (Message Authentication Codes)

2.4 CAST-256

It is an extension of CAST-128. This algorithm uses 8×32-bit S-boxes based on bent functions, modular addition and sub-traction, key dependent rotations and XOR operations adapted for a block size of 128 bits as its component. Key sizes that are accepted are 128, 160, 192, 224 or 256 bits. This algorithm is composed of 48 rounds, sometimes described as 12 "quad-rounds", arranged in a generalized Feistel network.

3. Implementation

The comparison between these algorithms is based on encryption time and decryption time. As we know that we transmit data of varied length and different data type across the network, the time taken to encrypt and decrypt also varies. The study of variation in time with respect to different data has been implemented in Visual Studio .Net framework, C# win-dow application as language and MS- Access as our backend.

4. Results

On comparing the above algorithms the following result was obtained.

It can be clearly seen in the graph that the blowfish is superior to other algorithms as it takes less time.

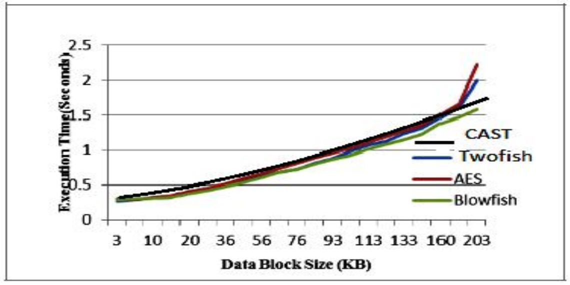

Figure 1 Performance Result

Although when the data size is very small this difference is not clearly visible. But for file having size greater 100KB it is very clearly visible.

References

[1.] Bruce Scheneir, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996

[2.] S. William, Cryptography and Network Security: Principles and Practice. Prentice Hall, 2010

[3.] S. Hebert, “A Brief History of Cryptography”, an article available at http://cybercrimes.net/aindex.html

[4.] Hager, C.T.R., “Performance & energy efficiency of block ciphers in personal digital assistance”. Pervasive Computing and Communications,Third IEEE International Conference, March 2005

[5.] Kumar, Nagesh; Thakur, Jawahar and Kalia, Arvind. “Comparative analysis of performance efficiency and security measures of some encryption algorithms”. An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4

[6.] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, “Performance analysis of symmetric key cryptography algorithms”. Interna-tional Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

[7.] Goyal, Shivangi. ”A Survey on the Applications of Cryptography”. International Journal of Science and Technology Vol-ume 1 No. 3, March, 2012

[8.] Diaa Salama Abd Elminaam, et.el., “Evaluating the performance of Symmetric Encryption algorithm”. International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010

[9.] Ayushi, “A Symmetric Key Cryptographic Algorithm”. International Journal of Computer Applications (0975 - 8887), Vol. 1, No. 15, 2010

[10.] Singh, Simar Preet and Maini, Raman. “Comparison of data encryption Algorithms”. International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[11.] M. Anand Kumar and Dr.S.Karthikeyan , “Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms”. International Journal of Computer Network and Information Security, 2012, 2, 22-28

[12.] Singhal, Nidhi and Raina, J P S. “Comparative Analysis of AES and RC4 Algorithms for Better Utilization”, Internation-al Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[13.] Thakur, Jawahar and Kumar , Nagesh. “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis”. International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011

[14.] A. Nadeem. “A Performance Comparison of Data Encryption Algorithms”. IEEE Information and Communication Technologies, pp. 84-89, 2006