# Performance Analysis of Cryptography Algorithms

Rishabh Arora

Department of Computer Science,
Guru Nanak Dev University, Amritsar

Sandeep Sharma, PhD
Associate Professor
Department of Computer Science,
Guru Nanak Dev University, Amritsar

## ABSTRACT

File is a collection of information that computer uses. The information is sensitive part of the organization. Any loss or threat to information can prove to be great loss to the organization as well to people. There are various means to protect the files from various threats. This paper describes various symmetric algorithms like Advanced Encryption Standard (AES), Blowfish, and DESX, a stronger variation of Data Encryption Standard (DES) to protect various types of files such as EXE, DOC, WMV and AVI files. The comparison of these algorithms is done in terms of Encryption and Decryption Throughput.

## General Terms

Cryptography, Blowfish, AES, DESX.

## Keywords

Executable file, Document file, AVI file, WMV file, key size, Throughput.

## 1. INTRODUCTION

Cryptography algorithms play an important role in providing security to networks. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. Symmetric algorithms can be divided into two categories: block ciphers and stream ciphers. The block ciphers operate on data in groups or blocks. Examples are DESX, a variation of Data Encryption Standard (DES), Blowfish and Advanced Encryption Standard (AES) On the other hand, stream ciphers only operate on a single bit at a time which makes them more suitable for real time applications such as multimedia. Example is RC4.

DESX uses one 128-bit key [8] while AES uses various 128, 192 or 256 bit keys [6] [12]. Blowfish uses various 32-448 default 128 bits [1] [11]. Encryption algorithms consume significant amount of computing resources such as CPU time, battery power etc. Battery power is subjected to the problem of energy consumption due to encryption algorithms. The decision regarding battery consumption needs to be taken to reduce the consumption of battery powered devices.

## 2. DESCRIPTION OF VARIOUS ALGORITHMS

### 2.1 DESX

DESX is a stronger variation of the DES encryption algorithm [7]. In DESX, the input plaintext is bitwise XORed with 64 bits of additional key material before encryption with DES and the output is also bitwise XORed with another 64 bits of key material [9].

### 2.2 Blowfish

It was developed by Bruce Scheiner. It is unpatent, license free and is available free for all of the users. It has key length that vary from 32 to 448 bits and uses default 128 bits [2] [10]. That key is used to generate 18; 32 bit sub keys and four 8X 32 S-boxes containing a total of 1024 32-bit entries. The total is 4168 bytes that makes it most conventional algorithm. Security of Blowfish is unchallenged and is successor to Twofish.

### 2.3 AES

It is approved by US government in 2000 for encryption of sensitive but unclassified data. It has variable key length of 128, 192 or 256 bits [5]. It has 10, 12 or 14 rounds depending on the size of the key. It is fast and flexible. It is well suited for implementation in hardware and software.

## 3. EFFECT OF CRYPTOGRAPHY ALGORITHMS ON EXECUTABLE FILE BASED ON VARYING KEY SIZE

The results are carried out using two simulations Crypt4free and Cript AES. Using these simulations Encryption and Decryption throughput can be determined.

### 3.1 Encryption Throughput

The encryption throughput can be determined by calculating the total plaintext encrypted on total encryption time of various encryption algorithms. Increased throughput results in decrease of power consumption. The results are shown with respect to key size variation and describes that Blowfish algorithm is superior of all algorithms. AES has advantage over DESX in terms of throughput. DESX has low performance in terms of power consumption and throughput than AES and Blowfish. The horizontal axis denotes algorithm and vertical axis key size.

**Table 1.** Throughputs of encryption algorithms for executable file (megabyte/sec)

**.EXE file of size 82.9 MB**

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 7.54 | - | 5.53 |
| **64** | 11.85 | - | 5.53 |
| **128** | 9.22 | 7.07 | 5.53 |
| **192** | 10.37 | 7.07 | - |
| **256** | 8.29 | 6.53 | - |
| **448** | 8.29 | - | - |

**3.2 Decryption Throughput**
Decryption throughput can be determined by calculating the total cipher text decrypted over the decryption time. It is clear from the figure that Blowfish algorithm is superior of all algorithms. AES has advantage over DESX as it can be seen over 128 bit key size and DESX has low performance in terms of power consumption and throughput than AES and Blowfish.

**Table 2**. Throughputs of decryption algorithms for executable file (megabyte/sec)

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 11.84 | - | 5.53 |
| **64** | 9.2 | - | 5.53 |
| **128** | 6.90 | 5.92 | 5.53 |
| **192** | 7.53 | 5.53 | - |
| **256** | 9.21 | 5.53 | - |
| **448** | 7.53 | - | - |

# 4. EFFECT OF CRYPTOGRAPHY ALGORITHMS ON DOCUMENT FILE BASED ON VARYING KEY SIZE

**4.1 Encryption Throughput**
A Document file is a text or binary file for storing documents on storage media especially for use of computers. In case of 128 bit key size, AES has highest throughput as compared to DESX and Blowfish. AES and Blowfish has same throughput in case of 192 bit key size. In all other cases Blowfish has highest throughput.

**Table 3.** Throughputs of encryption algorithms for document file (megabyte/sec)

**.DOC file of 9.8 MB**

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 9.8 | - | 4.9 |
| **64** | 9.8 | - | 4.9 |
| **128** | 4.9 | 9.8 | 4.9 |
| **192** | 4.9 | 4.9 | - |
| **256** | 9.8 | 4.9 | - |
| **448** | 9.8 | - | - |

**4.2 Decryption Throughput**
In decrypting the document files Blowfish algorithm is superior of all the algorithms in terms of power consumption and throughput. AES and DESX has same throughput in all cases. Blowfish has double throughput as compared to AES and DESX as it takes less time to decrypt the document file.

**Table 4.** Throughputs of decryption algorithms for document file (megabyte/sec)

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 9.8 | - | 4.9 |
| **64** | 9.8 | - | 4.9 |
| **128** | 9.8 | 4.9 | 4.9 |
| **192** | 9.8 | 4.9 | - |
| **256** | 9.8 | 4.9 | - |
| **448** | 9.8 | - | - |

# 5. EFFECT OF CRYPTOGRAPHY ALGORITHMS ON WINDOW MEDIA VIDEO (WMV) FILE BASED ON VARYING KEY SIZE

**5.1 Encryption Throughput**
Window Media file (WMV) is developed by Microsoft as non standard version of MPEG format. Now it is standardized as unique format. It allows compressing large videos retaining high quality. In encrypting WMV files, Blowfish performs superior followed by AES and DESX. AES has advantage over DESX in terms of throughput and power consumption. DESX has low performance as compared to Blowfish and AES

**Table 5.** Throughputs of encryption algorithms for WMV file (megabyte/sec)

**.WMV file of 38.9 MB**

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 9.68 | - | 5.53 |
| **64** | 12.91 | - | 5.53 |
| **128** | 12.9 | 6.48 | 5.53 |
| **192** | 12.9 | 6.48 | - |
| **256** | 9.68 | 6.48 | - |
| **448** | 12.9 | - | - |

### 5.2 Decryption Throughput

In Decrypting WMV file, AES and DESX both have the same throughput. Blowfish performs superior as compared to AES and DESX in terms of throughput. Blowfish has approximately double throughput than AES and DESX.

**Table 6.** Throughputs of decryption algorithms for WMV file (megabyte/sec)

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 12.9 | - | 5.53 |
| **64** | 9.72 | - | 5.53 |
| **128** | 12.9 | 5.53 | 5.53 |
| **192** | 12.9 | 5.53 | - |
| **256** | 12.9 | 5.53 | - |
| **448** | 12.9 | - | - |

## 6. EFFECT OF CRYPTOGRAPHY ALGORITHMS ON AUDIO VIDEO INTERFACE (AVI) FILE BASED ON VARYING KEY SIZE

### 6.1 Encryption Throughput

Audio Video Interleave (AVI) file is multimedia container format introduced by Microsoft and contains both audio and video in a file container that synchronous audio with video playback. In encrypting AVI file, DESX has low performance as compared to Blowfish and AES in terms of throughput. AES has an advantage over DESX and Blowfish has superior performance as compared to AES and DESX.

**Table 7.** Throughputs of encryption algorithms for AVI file (megabyte/sec)

**.AVI file of 76.8 MB**

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 9.6 | - | 5.49 |
| **64** | 10.98 | - | 5.49 |
| **128** | 10.98 | 6.98 | 5.91 |
| **192** | 10.98 | 6.98 | - |
| **256** | 10.98 | 6.40 | - |
| **448** | 12.81 | - | - |

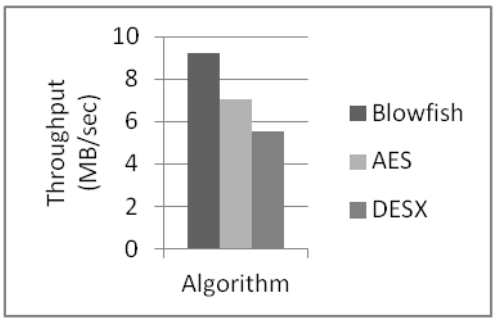
### 6.2 Decryption Throughput

In decrypting AVI files, AES has slightly more throughput than DESX. Blowfish has double throughput as compared to AES and DESX. DESX still has low performance than AES and Blowfish.

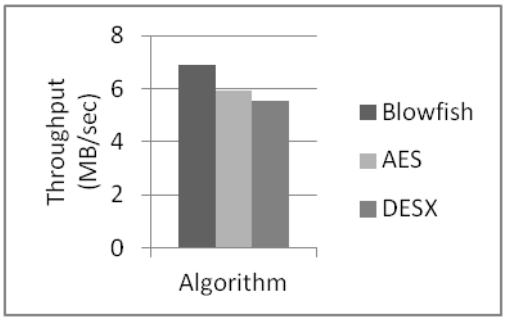
**Table 8.** Throughputs of decryption algorithms for AVI file (megabyte/sec)

| | **Blowfish** | **AES** | **DESX** |
|---|---|---|---|
| **32** | 10.98 | - | 5.49 |
| **64** | 9.6 | - | 5.49 |
| **128** | 10.98 | 5.91 | 5.49 |
| **192** | 10.98 | 5.49 | - |
| **256** | 9.6 | 5.91 | - |
| **448** | 10.98 | - | - |

## 7. GRAPHICAL COMPARISON OF VARIOUS ALGORITHMS FOR VARIOUS FILES FOR 128 BIT KEY

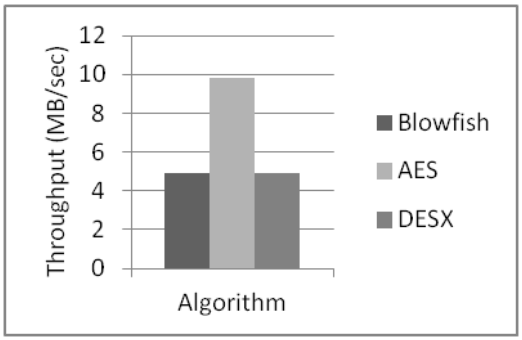



**(a)**

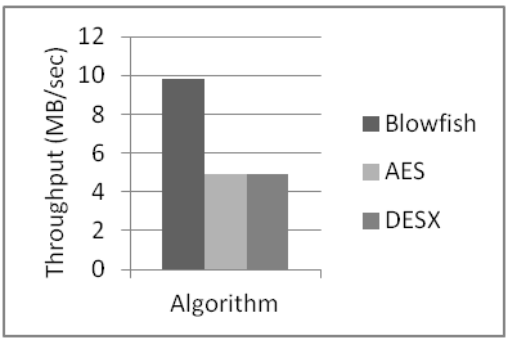



**(b)**

**Figure 1: Graph showing (a) encryption throughput and (b) decryption throughput for EXE file**

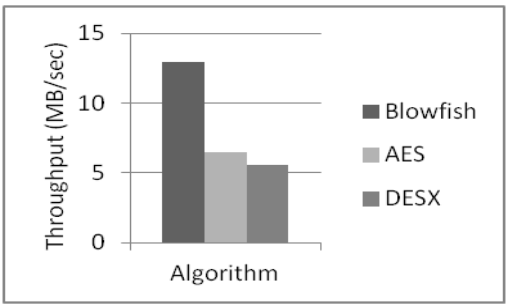



**(a)**

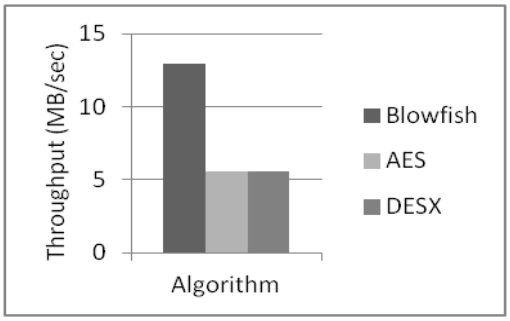



**(b)**

**Figure 2: Graph showing (a) encryption throughput and (b) decryption throughput for DOC file**

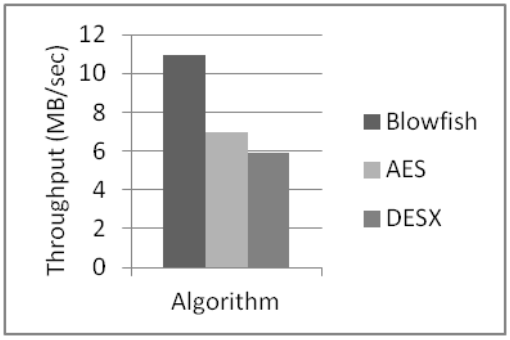



**(a)**

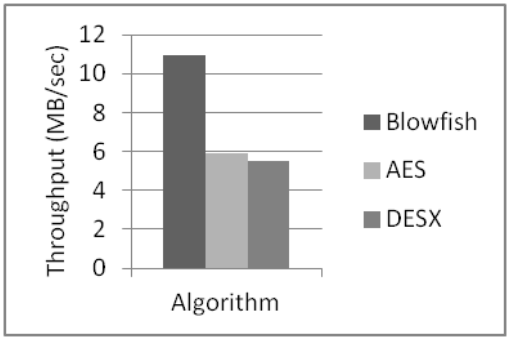



**(b)**

**Figure 3: Graph showing (a) encryption throughput and (b) decryption throughput for WMV file**




**(a)**




**(b)**

**Figure 4: Graph showing (a) encryption throughput and (b) decryption throughput for AVI file**

## 8. CONCLUSION

This paper presents the performance evaluation of various cryptographic algorithms for various types of files. The algorithms are Blowfish, DESX and AES. In Encrypting and Decrypting .EXE files, Blowfish has superior performance than other algorithms and DESX has low performance and AES has advantage over DESX. In Encrypting .DOC files, AES is superior than other algorithms. Blowfish and DESX both have same performance whereas in Decrypting .DOC files, Blowfish is superior. AES and DESX both have same performance in encrypting. WMV files, Blowfish is superior to DESX and AES. AES has advantage over DESX in terms of throughput whereas in Decrypting WMV files, Blowfish is superior than other algorithms. AES and DESX both have same performance. In Encrypting and Decrypting AVI files, Blowfish is superior to other algorithms. AES has advantage over DESX in terms of throughput. In order to consume less energy and power, it will be better to replace the algorithms that consume more energy, modification in the algorithms and to implement new design of algorithms.

## 9. REFERENCES

[1] Jason W. Cornwell, "Blowfish Survey", Department of Computer Science, Columbus State University, Columbus.

[2] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha, "A Study of New Trends in Blowfish Algorithm", International Journal of Engineering Research and Applications, Vol.1 pp 321-326.

[3] Marko Mali, Franc Novak and Anton Biasizzo, "Hardware Implementation of AES Algorithm", Journal of Electrical Engineering, Vol.56, 2005.

[4] Xinmiao Zhang and Keshab K. Parhi, "High Speed VLSI Architectures for AES Algorithm", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.9 Sep. 2004.

[5] Yibo Fan, Takeshi Ikenaga, Yukiyasu Tsunoo and Satoshi Goto, "A Low-cost Reconfigurable Architecture for AES Algorithm", Ambient SoC Global COE Program of Waseda University, Japan, 2008.

[6] Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare, Atul M. Borkar "Design of AES Algorithm using FPGA", International Conference on Advanced Computing, Communication and Networks'11Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[7] Manikandan.G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G, "A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.

[8] Duncan S. Wong, Hector Ho Fuentes and Agnes H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices", College of Computer Science, Northeastern University, Boston, MA 02115, USA.

[9] Gregor Leander, Christof Paar, Axel Poschmann and Kai Schramm, "New Lightweight DES Variants", International Association for Cryptologic Research, Germany.

[10] Michael C.-J. Lin, Youn-Long Lin, " A VLSI Implementation of Blowfish Encryption/ Decryption Algorithm", Department of Computer Science, National Tsing Hua University, Hsin-Chu, Taiwan 30043, R.O.C.

[11] Savita Devidas Patil and Ashish T.Bhole, " The Design and Implementation of Password Management System using Blowfish Algorithm", International Journal of Technology And Engineering System(IJTES): Jan - March 2011- Vol.2.No.2.

[12] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, " FPGA Implementation of AES Encryption and Decryption", International Conference on "Control, Automation, Communication and Energy Conservation -2009, 4th-6th June 2009.