JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JETIR
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Research on Performance Analysis of BLOWFISH, TWOFISH, DES and 3DES Symmetric Key Encryption Algorithms Using PCrypt

Pranjal Soni[1], Priyanka Prajapati[2]

[1] *Dept. of Computer Science and Engineering , Alpine Institute of Technology, Ujjain, M.P., India*

[2] *HOD,Dept. of Computer Science and Engineering , Alpine Institute of Technology, Ujjain, M.P., India*

Abstract --- *In this research, we are calculating the encryption or decryption time taken by four types of symmetric-key encryption techniques to encrypt or decrypt data which are DES, 3DES, BLOWFISH, and TWOFISH. Each technique possesses different size data with a fixed-size key and also in the case of a fixed size data with keys of different sizes to analyze the excellence of a technique that aids in the comparative study of an encryption technique and make us choose the efficient one. The time taken by symmetric-key encryption or decryption technique to encrypt or decrypt some data with some key varies from one technique to the other and depends on the data size, device configuration, key size, processor load, etc. This paper also assists in choosing an encryption or decryption technique to encrypt or decrypt some data with some key under certain scenarios by providing actual plots and statistics generated for DES, 3DES, BLOWFISH, and TWOFISH encryption techniques for encrypting or decrypting data under different situations with the help of our own web application "PCrypt" that is created by us using technologies such as JavaScript, Bootstrap, JpGraph, PHP, HTML, CSS, etc.*

Keywords --- DES, 3DES, BLOWFISH, TWOFISH, Key Size vs Execution Time Plots, Data Size vs Execution, Symmetric-key Encryption, Time Plots, PCrypt

INTRODUCTION

security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. The time taken by an encryption or decryption technique to encrypt or decrypt data of some size with a key of some size can be taken as a prominent parameter to decide the excellence of an algorithm in addition to its security. The quest for the best solution to offer necessary security from hacker attacks to the data that is exchanged over the internet or the other media types is currently in trend. As far as the security of data is concerned cryptography comes in rescue that deals with secret (crypto-) writing (-graphy) that is to conceal the data from the reach of all except the sender and the intended receiver. Cryptography encompasses numerous techniques that can be used to encrypt or decrypt some data. We have symmetric-key as well as asymmetric-key algorithms. Even choosing a symmetric-key algorithm to secure the data opens a wide range of algorithms to choose from[11]. Our major concern is to choose the efficient one with good performance accompanied by good security. Studying the performance and behaviour of such algorithms with varied sizes of data and keys helps us in choosing the right algorithm as per our needs and this is the major concern of this paper. This paper tries to provide a comparison among four symmetric-key algorithms namely DES, 3DES, Blowfish and Twofish. We have created and used our own web application i.e. PCrypt for the analysis purpose.

ENCRYPTION

Encryption process of cryptosystem converts plain text to a cryptic text that is "hidden" to secure it against hackers or data thieves[12] is shown in Fig1. At recipient end decryption process recovers original text, to be understood.

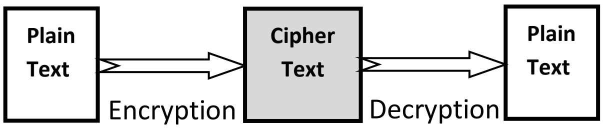


Fig.1 Encryption-Decryption Flow

Cryptographic system can be defined as C={ set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context"[13]. Cryptography definition defines the whole mechanism that provides the necessary level of security comprised of network protocols and data encryption algorithms.

LITERATURE REVIEW

Literature review presented here is for the comparison of various encryption algorithm to find out an efficient algorithm . Encryption Algorithm is the method of converting a message into unreadable form to secure the message from unauthorized access. There are different Encryption algorithms available for encrypting the message. Here is the survey of various researches on different Encryption Algorithms.

"A Comprehensive Analysis Between Popular Symmetric Encryption Algorithms"[1]

There are many different types of symmetric encryption algorithms such as DES, TDES, Blowfish, AES (aka Rijndael), Twofish. Asymmetric encryption uses two different keys namely the private key and the public key to help in achieving encryption or decryption. The sheer hostility of the network in question shows us the need to secure information before it to be transmitted over the network. The advantage key encryption is that the confidentiality of the data in question relies on the key and not the algorithm using the key. This means that even if the attacker knows the decryption algorithm, decryption isn’t possible unless the attacker knows the key as well. Encryption algorithms can be primarily divided into two types, symmetric and asymmetric key algorithms. Figure 5 shows the Encryption system Hierarchy. Symmetric encryption process uses only a single Private Key to encrypt as well as decrypt data. The different asymmetric encryption algorithms are PGP, RSA, SSH and many more. This paper primarily targets its research towards popular symmetric key Encryption algorithms based on specific criteria. Nowadays it is very important to protect the data transmitted over the internet due to the increasing number of cases in which data to confidential between two parties is stolen by intruders.

As per [1] The parameters that affect the selection of a certain cipher for a particular application are:

1) Architecture: Defines the basic structure that encompasses how a certain algorithm their respective plain text into its corresponding ciphertext. Based on the usage of a specific key (either secret or public key) we also are able to determine if the algorithm is symmetric or asymmetric.

2) Security: Defines how strong the encryption algorithm is against an attack. Encryption systems strive to satisfy this particular criterion and hence security has become an important criterion among these parameters. Secure encryption generally use bigger key sizes than its less secure counterparts.

3) Efficiency: A major criterion on which encryption algorithms are analysed. Efficiency basically depends on two factors such as speed of execution and memory utilization.

4) Limitations: Defines the already known attacks that the encryption is vulnerable to. Helps to decide whether the encryption algorithm must be used or not for a specific application.

"Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems" [2]

By increasing the speed of data processing process by computer systems, the Blowfish Algorithm is capable of creating and developing a larger and larger length that ensures system security. In Cryptography, Twofish algorithm it's symmetrical block algorithm whose block size it's 128 bits, and the key size changes to 256 bits. This algorithm associated with the predecessor Blowfish algorithm. Blowfish is a variable-length key algorithm with 64-bit block cipher; was created in 1993 by Bruce Schneider to replace the DES (Data Encryption Standard).

"S-DES: An efficient & secure DES variant," [3]

The design criteria for DES were not published and some modifications were introduced, which reduced the security level of DES such as reducing the size of the secret key from 128 to 56 bits. This modification was the reason behind breaking DES after 20 years. DES uses the classic uniform Feistel Network and has a block size of 64 bits and a key size of 56 bits. The secret key consists of eight bytes, however, one bit of each byte is dropped, which means that the key size is effectively 56 bits. The input block (64 bits) is separated into 2 sub-blocks (words): the 32 leftmost bits part L and the 32 rightmost parts R . Then, the round function is applied 16 times and for each round a new L and R are produced. The proposed S-DES variant should be strong enough to guard against the most known types of attacks such as statistical, differential, chosen/known plain-text, and brute-force attacks. In fact, doubling the size of the data block and the secret key doubles its resistance against analytical and brute force attacks. The original DES cipher scheme suffers from several security weaknesses, while 3DES suffers from performance issues. This motivated the work to define a new efficient and secure DES variant, S-DES. Indeed, the newly proposed variant employs an extended FN with a 125-bit block size. In addition, the size of the secret key of S-DES is 112-bite. Therefore, S-DES provides better resistance against attacks such as brute-force, differential, and linear cryptanalysis.

"Enhancing data security using DES-based cryptography and DCT-based steganography,"[4]

One of the main problems in digital communication is the security of the data was transmitted over the internet network. Data can be stolen or accessed by attackers with certain techniques. Therefore, it is the necessary application of reliable data security techniques for data exchange via internet media. Cryptography and Steganography are two of the most commonly used to secure digital data. Cryptography is a technique for securing data where the original data is randomized in such a way that it is difficult to understand. Original data can only be opened by a specific person using predefined custom keys. The applications generated in this research[4] are able to secure data or document files such as word files (.doc, .docx), excel files (.xls, .xlsx), powerpoint (.ppt, .pptx) files, and pdf files. Meanwhile, the combination of the DES cryptographic and DCT steganographic methods proved to improve data security because it has two levels of security. Based on the experiment can also be concluded that the stego-image quality can still be in a good category with an average value of PSNR of 46.9 dB. The combination the two methods resulted in a computation time of 0.75 milliseconds/bytes. The computational time still needs to be improved in the future research. Overall, the success rate of the proposed method in securing the data was 58%. The success of the data security process depends on the resolution of the cover image used. In this study, it is recommended to use a cover image resolution of 1024 x 720 or more. One research[4] provides a data security application that can be useful for improving the security of data files before being sent over the public network. In the next study, the computation time needs to be optimized again so that it becomes faster. Also, an increase in file size of 4.79 times can be reduced by adding a compression method or optimizing the encryption algorithm used.

"Fast software implementation of des for lightweight platforms"[5]

Many lightweight cryptography protocols have not designed to be efficient on software platforms, since designers are usually focused on hardware requirements. This study addresses this problem. We present a new design architecture for improving the software implementation of the DES. The DES is a family of block ciphers. It is efficient in hardware but its design was not oriented for software platforms. Aim of our proposed design is to find a block cipher architecture design for lightweight applications. Data Encryption Standard (DES) is a symmetric key encryption algorithm. The importance of DES is the most commonly used block encryption algorithm in the world for 30 years. It was accepted as a standard in 1976, and this standard published as FIPS 46 in 1977[5].

"An efficient implementation of enhanced key generation technique in data encryption standard (DES) algorithm using VHDL"[6]

The need of cryptography is emerges to keep the private data from unapproved individual. Security of the information or framework is relies on upon both cryptographic calculation and key utilized for encryption/decryption. Cryptography is required in different areas like banks, military, railroads, media transmission and so forth. In electronic reserve exchange like ATM cards, computer passwords, electronic passwords likewise require the security. The route toward changing over plain substance to figure content is known as encryption and the count which encodes the data is known as encryption computation. In the present day cryptography, a mix of both open key and regular symmetric cryptography is used. The reason behind this is open key encryption arranges are computationally genuine versus their symmetric key accomplices. Due to the dynamic key generation unit secrecy of the key get increased. Simulation results are shown for both encryption and decryption. Using proposed design, we can achieve high speed and reduced logic complexity which gives enhanced DES algorithm. According to this enhanced DES algorithm has broad application area in secure data communication and transmission. In future, we can execute this framework for greater security in various applications, for example, Smart card security Database administration framework, Set top box, Wireless correspondence security, Content insurance. The security of any type of algorithm is dependent on the secrecy of the key[6].

"Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations"[7]

One of the significant issues is file management. Secure file management has become an important technology along with the increasing use of computer systems. The recommended file security is storing encrypted files to be inaccessible to irresponsible people. With the rapid development of network technology, attacks over the Internet are also diverse, traditional encryption algorithms (single data encryption) is not enough to ensure information security on the internet. According to [7], AES (Advanced encryption standard) is the best encryption algorithm, that was proposed by NIST. On the other hand, Blowfish is the fastest algorithms, but the security level is lower than that of AES. Message Digest 5 (MD5) hash function is proposed by Rivest to improve the previous version MD4 and published in 1992. MD5, similar to other cryptographic hash algorithms, retrieves messages of a free size and produces fixed-size output (128 bit). Blowfish was designed by Bruce Schneider in 1993 as an alternative algorithm for rapid encryption. Blowfish is included in 64-bit Chipper block encryption with a key length of at least 32-bit to 448-bit. Made for use on computers with large microprocessors (32-bit and above with large data cache). In this study, the authors tried to compare the combination of Blowfish and AES 256 algorithms with AES 256 and Blowfish for the fastest time of encryption and decryption. Differences in the order of combinations of algorithms will be observed at their safety level.

"An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing"[8]

The adventure and consumers have transferred the information using cloud facility to minimize the data execution cost and cost of the storage facility. However, the information is lost due to sensitivity, to reduce the information drop the information are encrypted before loading the information into the cloud. The conversion of plain text to cipher text is called encryption, and the reverse process is called decryption. Privacy as a Service is used to protect storage and handling of users' private data[8]. The AES based cipher text retrieval provides more security. But the proposed system using elliptic curve key for key generation and encrypt the data using blowfish. So the blowfish algorithm provides high throughput than others. During the implementation, we notice that proposed approach achieved the efficiency at the Data Owner side and user side. This work allows a user to search keyword over the encrypted data. So the blowfish encryption is important in storage and retrieval of outsourced cipher textThen the Blowfish decryption algorithm is used to get the plain text. It provides security for outsourced data, and the performance of the proposed work showed better efficiency regarding of low computation and communication costs. To search the ciphertext content effectively, Porter stemming based index has generated and the data stored on a cloud as encrypted form. Here Blowfish encryption and elliptic curve keys are used for secure data transmission. When the authorized user generates a query to the cloud, the relevant files are sent to the user in an encrypted format. Then the user gives the private key for decryption process, and blowfish decrypt the files. This proposed method provides better performance by comparing with the conventional algorithms in the way of retrieval efficiency and less time-consuming[8].

"Comprehensive study of symmetric key and asymmetric key encryption algorithms"[9]

Cryptography attracted many researchers. Reversion this cipher data to original data called decryption process. Cryptography is widely used to secure data in cloud computing. Due to the extensive use and sharing of data in the Internet, it is necessary to protect data from hacking, noise, and interference.It is used for protecting information during transmissions between users. It alters the content of transmitted data to unreadable form, once received by the receiver, it is converted back to its original form. Encrypting data results to an unreadable format called cipher-data. Cryptography had a set of security goals to ensure the privacy of data. These goals are confidentiality, authentication, data Integrity, non-repudiation and access control[9].

It is classified into Symmetric (private-key) and Asymmetric (public key) keys encryption. Examples of Symmetric algorithms are DES, 3DES, AES, Blowfish and DSA (Digital Signature Algorithm), Elliptic Curve, Diffie- Hellman (key exchange) and RSA are examples of Asymmetric algorithms. Encryption is a technique for protecting sensitive data. It hides the sensitive data of users by using the same key to cipher and decipher the data.

The following four algorithms uses symmetric encryption -

A. Data Encryption Standard (DES)

B. Triple Data Encryption Standard (3DES)

C. Advanced Encryption Standard (AES)

D. Blowfish

One research proposed performance evaluation for four encryption algorithms (DES, 3DES, Blowfish and AES). They used different settings to evaluate encryption algorithms such as different sizes of data blocks and decryption speed under different hardware and software platform. All codes implemented in C++, .NET(2003) and run on a Pentium- 4, 2.1 GHz processor under Windows XP SP1. They showed that Blowfish was the best algorithm in case processing time and it had strong key size(448 bit). AES needed more processing time when data block size was relatively large. 3DES required more time than DES. Also, they showed that AES was the best algorithm in cases number of requests executed per second in different user loads, and in the response time in different user load situation performance results of stream cipher.

Another research made a comparison of the performance of algorithms (DES, AES, and Blowfish). They concluded that Blowfish gives the best results in various block cipher modes with minimum weak points. AES showed poor performance compared with other algorithms. In general, symmetric encryption algorithms are faster than asymmetric encryption algorithm but it had only one weak point that it is shared its key with other parties involved in the process. Asymmetric encryption has a strength point that it is used two different keys but it's required more processing time than symmetric encryption. In the survey[9], they give a detailed study of symmetric like AES, DES, 3DES and Blowfish also for asymmetric algorithms such as RSA, DSA, Diffie-Hellman and Elliptic Curve. According to an analysis section, we found that the efficiency of the various algorithms is affected by the difference parameter. In the current state of increasing demand on cloud application, it became necessary to provide efficiency, robust and high-security algorithms that suitable with the large scale of data in the cloud. Speed and security are the most important rules play on cloud applications[9].

"An Enhanced BlowFish (eBf) Algorithm for Securing x64FileMessage Content"[10]

Currently, there are various techniques and methods designed for specific problem. Encryption of data over the network is one of the key methods which translates information that only authorized user has the knowledge of the secret key. Everyday new techniques are developed with high security rate of protecting and securing confidential information. Over the years, the scope of cryptography has widen and evolved with the modern transactional requirements. The need to protect data has become more complex as computers were introduced and cryptanalysis has adapted to the increasing complexity of cryptography or the technique of enciphering and deciphering messages that maintains the privacy or security of data. There is a general need for enciphering all data sent between computers connected to a network. Computer systems must have a means to prevent unauthorized access to avoid any alteration or worse loss of data between devices connected to the network. Basically, blowfish encryption algorithm contains 16 rounds. Each round consists of XOR operation and a function (F).[10]

GOALS OF CRYPTOGRAPHY

The five main goals behind using Cryptography are-

Authentication: It means that the sender's and receiver's identity should be verified before sending and receiving data using the system.

Integrity: It means that the content of the communicated data is assured to be free from any type of modification between the end points that is between the sender and the receiver. The basic form of integrity is packet check sum in IPv4 packets[5].

Non-Repudiation: In non-repudiations neither the sender nor the receiver can falsely deny that they have sent a certain message.

Secrecy or Confidentiality: This means that only the authorized people are able to interpret the message (data) content and nobody else[14].

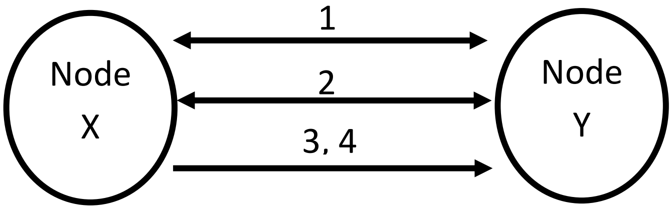
Service Reliability and Availability: Since systems which are secure usually get attacked by intruders, which may affect their availability and type of service to their users. This type of systems should provide a way to grant their users the quality of service they expect.

CATEGORIES OF DATA ENCRYPTION ALGORITHMS

There are majorly two categories of data encryption algorithms based on the type of security keys used for encryption/decryption namely Symmetric key encryption and Asymmetric key encryption algorithms.

SYMMETRIC KEY ENCRYPTION

Symmetric key encryption is considered when the sender and receiver both use a shared secret key to encrypt and decrypt the data respectively. Fig. 2 shows how symmetric key encryption/decryption takes place.



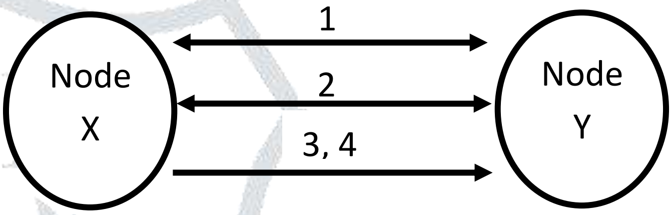
1. Node X and Y agree on a common cryptosystem
2. Node X and Y agree on a key to be used for encryption/decryption.
3. Node X encrypts data using the shared key.
4. Node Y decrypts the ciphered data using the shared key.

Fig.2 Symmetric Key Encryption

Major issue behind this type of encryption is the sharing of secret key between two devices. If the secret key gets revealed any how then the entire system may get failed.

ASYMMETRIC KEY ENCRYPTION

In asymmetric key encryption/decryption we use two keys. It follows the concept of Public and Private Key. The Public Key is known to public and the private key is only known to the user[16]. This is may be known as Public Key Cryptography . Here the first key can encrypt only what second key can decrypt and vice versa. Fig. 3 illustrates how asymmetric key encryption takes place.



1. Node X and Y agree on a common cryptosystem.
2. Node Y sends its public key to X to encrypt data.
3. Node X encrypts data using the negotiated cipher and Node Y's public key.
4. Node Y decrypts the ciphered data using its private key and the negotiated cipher.

Fig.3 Asymmetric Key Encryption

Asymmetric key encryption solves the issue of secret key management that arises in symmetric key encryption. On the other side the usage of public key encryption is more vulnerable. Asymmetric key encryption requires more computational processing power[17].

COMPARED ALGORITHMS

We have analyzed below 4 encryption/decryption algorithms/techniques -

Blowfish: Blowfish is a symmetric-key encryption algorithm which has 64-bit block size and variable key length between 32-448 bits. It is also known as 16-round Feistel cipher[23]. It resembles CAST-128 in structure which uses fixed S-boxes. It uses large key-dependent S-boxes.

Blowfish algorithm uses block size of 64-bit and a variable length of key 32 bits to 448 bits. It is also called 16-round Feistel cipher and this uses large key-dependent S-boxes[25]. which uses fixed S-boxes. Blowfish is a fast block cipher, except when it changes keys. It is freely available to anyone and this thing has made it more popular one.

Twofish: Twofish is similar to the block cipher Blowfish. Twofish was designed by David Wagner, John Kelsey, Bruce Schneier , Niels Ferguson, Doug Whiting, and Chris Hall, and the "extended Twofish team"[27]. It has been one of the 5 finalists of the AES contest, still it was not selected for standardization[28]. It has features of the use of pre-computed

S-boxes which are key-dependent, and a relatively complex key schedule. In this for the actual encryption an n-bit key is used at first half and to modify the encryption algorithm n-bit key is used at the second half.

DES: Data Encryption Standard (DES) is a very old symmetric-key encryption algorithm. At present, DES is considered to be insecure since it is not so that much strong. It was developed at IBM in 1970s and has its origin in the design by Horst Feistel. DES was published by the National Bureau of Standards in January 1977[18]. It uses the block size of 64 bits. A key is used in DES for the customization of transformation and the decryption can only be done by the person who has this key. The key has 64 bits but only 56 of these bits are used by the algorithm. 8 bits are used for parity checking, and are thereafter discarded. The effective key length is 56 bits. The key is transmitted or stored in 8 bytes, each with odd parity[19].

3DES: Triple DES (3DES) stands for Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher. It applies the DES (Data Encryption Standard) cipher algorithm three times to each data block so it has been named 3DES. 3DES gives a way to increase the key size of DES for protection without making it necessary to design an entirely new encryption algorithm[21]. It uses a key bundle that has 3 DES keys say K_1, K_2 and K_3. Each key is of 56 bits excluding extra parity bits. The encryption algorithm is:

$$\text{ciphertext} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$$

Here DES encrypt with K_1, then DES decrypt it with K_2, and after that DES encrypt it with K_3.
The decryption just opposite to the encryption:

$$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$$

Means, decrypt ciphertext with K_3, encrypt it with K_2, and at last decrypt it with K_1.
A block of 64 bits of data is encrypted by 3DES.
In all cases the middle operation is the reverse of the first and last operation[22].

METHODOLGY

Choosing an efficient symmetric key encryption techniques has been an issue. To choose the best symmetric encryption algorithm from a list of symmetric key encryption algorithms such as DES, 3DES, Blowfish and Twofish, we can analyze or compare them first to get the best out of them. But for that we need some tool to analyze or compare their working. Also there should be some parameters like encryption/decryption time, key size, data size, power consumption etc for judging which one is the best among them.

PROPOSED METHOD

We may analyze these symmetric key encryption algorithms using the web application – PCrypt, which provides actual statistics generated during encryption or decryption in different cases. There are total 4 type of cases for encryption and decryption and It provides 20 types of graphs and 16 types of analysis tables that aid in the analysis of these algorithms in a convenient manner.

The 4 cases/categories of graphs supported by PCrypt are as follow:

Category I : Data size vs execution time graphs for encryption using a single key and 5 different data files.

Category II : Data size vs execution time graphs for decryption using a single key and 5 different data files

Category III : Using a fixed sized data and 5 different key files a graph between Key size and execution time for encryption.
Category IV : Using a fixed sized data and 5 different key files a graph between Key size and execution time for decryption.

PARAMETERS FOR ANALYSIS OF SYMMETRIC KEY ENCRYPTION ALGORITHMS

We have considered the following parameters throughout this paper.

Encryption/Decryption time- This time depends on the complexity of algorithm, processor speed, RAM and other factors of the operating environment. Algorithm which has lesser encryption/decryption time is considered to be better.

Throughput- It is calculated by dividing the total plaintext in MB encrypted/decrypted by total encryption/decryption time for each algorithm. Greater the throughput lesser the power consumption. The technique which has maximum throughput will be most efficient.

Key size- key size is often considered to be proportional to security level. It may also result in greater encryption/decryption time.

Data size- Larger data size may result in increased encryption/decryption time.

IMPLEMENTATION

PCrypt has been created by us using some web technologies such as PHP, HTML, CSS, JavaScript, Bootstrap and JpGraph. Adobe Photoshop has been used for a little designing purpose. The home screen of PCrypt provides 4 categories of graphs which again has 5 subcategories making it able to produce overall 20 types of graphs. The home screen also has a link to download the test files for keys and data. When we click on the button of any category, the user is redirected to the concerning page where one may asked to provide data files, key, key files etc depending on the category the user has selected. Then after feeding all the information, tables and graphs are generated that can be seen in the "Analysis Results" section of this paper.

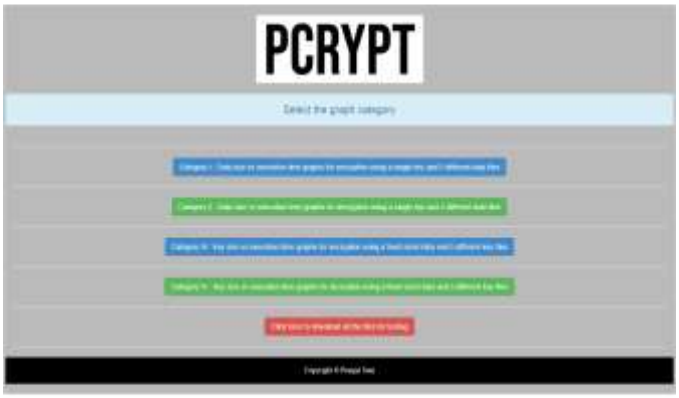


Fig. 4 : Home screen of PCrypt application

ANALYSIS RESULTS

There has to be various combinations of data of different size and keys of different size to analyze the performance of these encryption/decryption techniques. We have taken a random set of data files and key files with different sizes for this analysis. Some of our analysis results match with results obtained by other researchers[29]. The different results achieved in the form of different graphs and tables for various categories are given below.

Category I : Data file size vs execution time analysis for encryption using a single key and 5 different data files

Inputs:

Key: abcdefgh
Key size:8 bytes
Data files supplied-

File	Data File Size
1	99.03125 kb
2	199.0625 kb
3	299.09375 kb
4	399.125 kb
5	499.90234375 kb

Outputs:

Individual Results for DES, 3DES, Blowfish and Twofish :

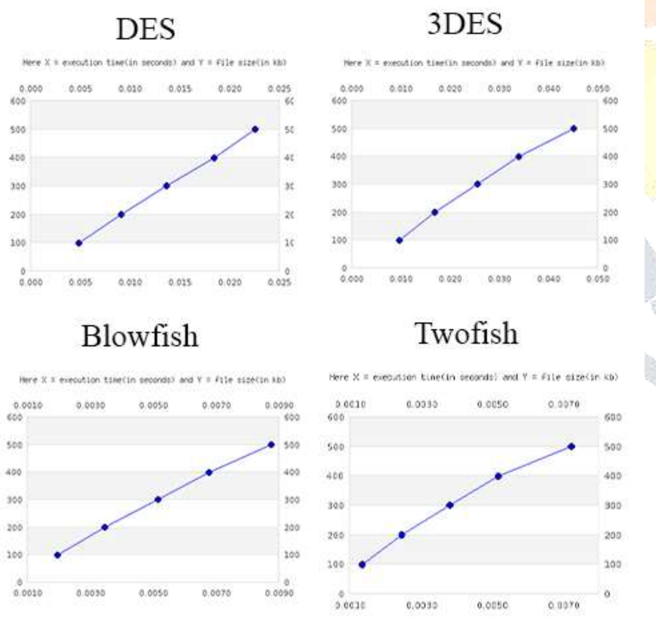


Fig. 5 : Execution time (in s) [X axis] vs file size (in kb) [Y-axis] graph for encryption using DES, 3DES, Blowfish and Twofish

Comparative graph for all :

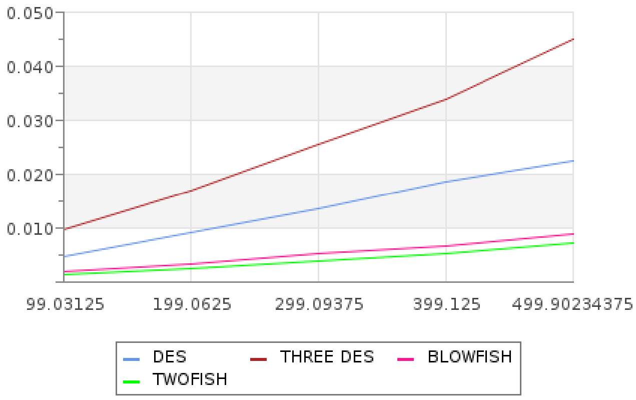


Fig. 6 : File size (in kb) [X axis] vs execution time (in s) [Y-axis] comparative graph for encryption using DES, 3DES, Blowfish and Twofish

Category II : Data size vs execution time analysis for decryption using a single key and 5 different data files

Inputs:

Key: abcdefgh
Key size:8 bytes
Data files supplied-

File	Data File Size
1	99.03125 kb
2	199.0625 kb
3	299.09375 kb
4	399.125 kb
5	499.90234375 kb

Outputs:

Individual Results for DES, 3DES, Blowfish and Twofish :

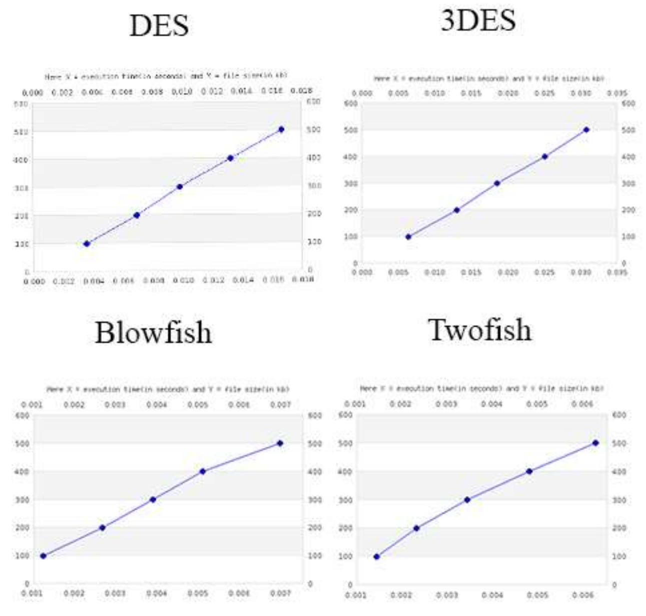


Fig. 7 : Execution time (in s) [X axis] vs file size (in kb) [Y-axis] graph for decryption using DES, 3DES, Blowfish and Twofish

Comparative graph for all :

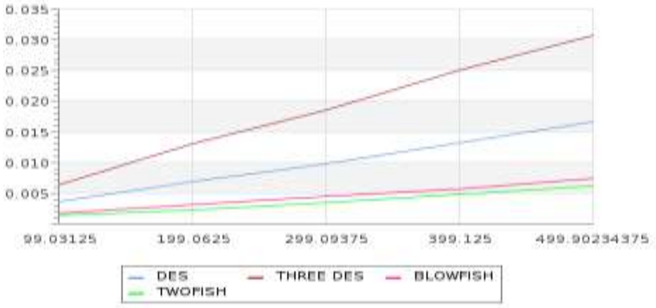


Fig. 8 : File size (in kb) [X axis] vs execution time (in s) [Y-axis] comparative graph for decryption using DES, 3DES, Blowfish and Twofish

Category III : Key size vs execution time analysis for encryption using a fixed sized data and 5 different key files

Inputs:

Data size: 499.90234375 kb

Key files supplied –

File	Key File Size
1	8 bytes
2	24 bytes
3	40 bytes
4	48 bytes
5	56 bytes

Output:

Comparative graph for all :

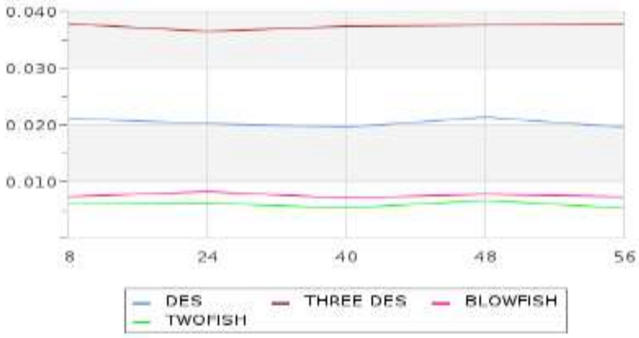


Fig. 9 : Key size (in bytes) [X axis] vs execution time (in s) [Y-axis] comparative graph for encryption using DES, 3DES, Blowfish and Twofish

Category IV : Key size vs execution time graphs for decryption using a fixed sized data and 5 different key files

Inputs:

Data size: 499.90234375 kb

Key files supplied –

File	Key File Size
1	8 bytes
2	24 bytes
3	40 bytes
4	48 bytes
5	56 bytes

Output :

Comparative graph for all :

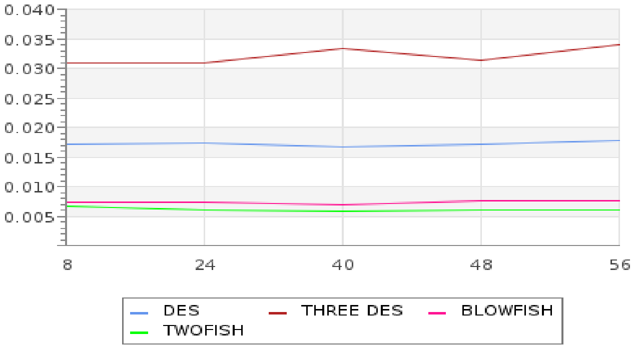


Fig. 10 : Key size (in bytes) [X axis] vs execution time (in s) [Y-axis] comparative graph for decryption using DES, 3DES, Blowfish and Twofish

CONCLUSIONS

After thorough analysis done above using PCrypt if we choose the speed as a prominent factor to decide the efficiency of these techniques to encrypt/decrypt data of different sizes using same key or data of fixed size using different keys with different sizes, we can draw below conclusions –

1) Twofish took the least time for encryption and decryption in all size combinations of data and key.
2) Blowfish and Twofish have a very close result in efficiency.
3) 3DES is least efficient because it took the maximum time in all cases on encryption/decryption time parameter among these algorithms.
4) The encryption/decryption time taken by these techniques in ascending order is Twofish--Blowfish--DES--3DES when we encrypt/decrypt different data with different size with the same key and also in the case when we encrypt/decrypt a fixed size data with different keys with different sizes.
5) If we calculate the throughput for Twofish with the analysis data obtained above, it will be the maximum and hence Twofish will consume least processing power. Also in this case 3DES will consume the maximum processing power with minimum throughput.

SIMULATION SETUP

The simulation has been done on a laptop with the specifications and environment mentioned below –

Company	Samsung
Model	NP350V5X-S01IN
Processor	Intel i5-3230M (3^{rd} generation) with 2.6GHz clock speed
RAM	4 GB
HDD	500 GB
Graphics	4 GB
Number of processor cores	2
OS	Windows 7 Ultimate (64 bit)
Browser	chrome

LIMITATIONS

The results shown here are suggestive and random. Since the operations are done here in some milliseconds so each time the result may slightly vary. As we know that each device may have different load at different time that can affect the speed of encryption/decryption so the results given here is not constant. Moreover PCrypt can only analyze DES, 3DES, Blowfish and Twofish algorithms on the already discussed parameters. At this moment it cannot analyze other techniques nor it can compare them for now since it is only build for these 4 algorithms as of now. Also PCrypt cannot operate upon input data with size above 2MB for now. The input data files provided to PCrypt should not exceed 2MB in size and maximum key size supported is 56 bytes. But in spite of these limitations PCrypt works really well for analysis of these 4 techniques.

FUTURE ENHANCEMENTS

Analysis on these techniques can be done using some other parameters as well. If we shall have results using all the parameters then we shall be able to dive more into the details. PCrypt can be made to operate on big data and key sizes. Moreover it can be extended to analyze or compare other symmetric encryption/decryption techniques. It can also be extended to analyze asymmetric encryption/decryption techniques as well. It is extensible and can be deployed on environment such as Windows, LINUX or Mac. The results can also be calculated for other devices with different configurations.

ACKNOWLEDGEMENT ``

We are pleased to see the contribution of other researchers in this field which helped us in cross-checking some of the results obtained by our own web application PCrypt. We are also thankful to PHP's official website and JpGraph library makers.

REFERENCES

[1] S. S. Ghosh, H. Parmar, P. Shah and K. Samdani, "A Comprehensive Analysis Between Popular Symmetric Encryption Algorithms," *2018 IEEE Punecon*, Pune, India, 2018, pp. 1-7.

[2] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, A. Fesenko and A. Abisheva, "Comparison and Hybrid Implementation of Blowfish, Twofish and RSA Cryptosystems," *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Lviv, Ukraine, 2019, pp. 970-974.

[3] M. Noura, H. N. Noura, A. Chehab, M. M. Mansour and R. Couturier, "S-DES: An efficient & secure DES variant," *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*, Jounieh, 2018, pp. 1-6.

[4] Solichin and E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," *2017 3rd International Conference on Science in Information Technology (ICSITech)*, Bandung, 2017, pp. 618-621.

[5] F. Özkaynak and M. I. Muhamad, "Fast software implementation of des for lightweight platforms," *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, Malatya, 2017, pp. 1-4.

[6] P. M. Chabukswar, M. Kumar and P. Balaramudu, "An efficient implementation of enhanced key generation technique in data encryption standard (DES) algorithm using VHDL," *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, 2017, pp. 917-921.

[7] M. A. Muin, M. A. Muin, A. Setyanto, Sudarmawan and K. I. Santoso, "Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations," *2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, Semarang, 2018, pp. 137-141.

[8] S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, 2017, pp. 267-271.

[9] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," *2017 International Conference on Engineering and Technology (ICET)*, Antalya, 2017, pp. 1-7.

[10] G. L. Dulla, B. D. Gerardo and R. P. Medina, "An Enhanced BlowFish (eBf) Algorithm for Securing x64FileMessage Content," *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM)*, Baguio City, Philippines, 2018, pp. 1-6.

[11] William Stallings - "Cryptography and Network Security Principles and Practices", Third Edition, Pearson Education Inc., 2003.

[12] Diaa Salama et al — "Performance Evaluation of Symmetric Encryption Algorithm", IJCSNS, 2008.

[13] E. Surya and C. Diviya - "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks, Vol. 2(4), 475-477.

[14] Michal Halas, Ivan Bestak, Milos Orgon, and Adrian Kovac - "Performance Measurement of Encryption Algorithms and Their Effect on Real Running in PLC Networks", IEEE, 2012.

[15] Monika Agrawal and Pradeep Mishra - "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering, Vol. 4, No. 05, May 2012.

[16] Mansoor Ebrahim, Shujaat Khan and Umer Bin Khalid - "SymmetricAlgorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975– 8887) Volume 61– No.20, January 2013.

[17] Prashanti G. Et al - "A Novel Approach for Data Encryption Standard Algorithm", IJEAT, ISSN:2249-8958, Volume-2, Issue-5, June 2013

[18] Gurjeevan Singh et al - "Performance Evaluation of Symmetric Cryptography Algorithms", IJECT 2011

[19] Shah Kruti R.and Bhavika Gambhava - "New Approach of Data Encryption Standard Algorithm".

[20] Dr. Mohammed M. Alani — "Improved DES Security", International Multi-Conference On System, Signals and Devices, 2010.

[21] The DES 15 years of public scrutiny. Dorothy E. Denning. http://faculty.nps.edu/dedennin/publications/DES-15Years.pdf

[22] Gurpreet Singh et al - " A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", IJCA Journal 2013, Vol 67-Number 19

[23] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari - "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Student's Conference on Electrical, Electronics and Computer Science, IEEE, 2012.

[24] Fei Shao, Zinan Chang and Yi Zhang - "AES Encryption Algorithm Based on the High Performance Computing of GPU", 2010 Second

International Conference on Communication Software and Networks DOI 10.1109/ICCSN.2010.124, IEEE, 2010.

[25] Dhanraj, C.Nandini, and Mohd Tajuddin - “An Enhanced Approch for Secret Key Algorithm based on Data Encryption Standard”, IJRRCS, August 2011

[26] G Poonam - “ Memetic Algorithm Attack on Simplified Data Encryption Standard algorithm”, proceeding of International Conference on Data Management, February 2008

[27] Schaefer E - “A Simplified Data Encryption Standard Algorithm”, Cryptologia, Vol .20, No.1, pp. 77-84, 1996.

[28] Bruce Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, http://www.schneier.com/twofish.html

[29] [A. Nadeem] Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005