A Comparative Analysis of Symmetric and Asymmetric Data Encryption Techniques with Existing Vulnerabilities

Samantha Barua Chowdhury
Department of Electrical and Computing Science, University of Alberta
Edmonton, Alberta, Canada
sc12@ualberta.ca

1 Abstract

In this project, a comparative analysis of symmetric and asymmetric encryption techniques is performed, that highlights the working process of each algorithm and also points out cases, where these perform the best or if they fail. Study of this project gives the reader an idea about the sustainability of each algorithm when faced with modern challenges. This also points out the algorithms that will be considered "outdated" in near future and alternatives that can be used instead.

2 Introduction

Modern technologies enable users to perform various tasks online, such as, bill payment and money transfer with great speed. As much as this provides efficiency to the users, the security breach and improper handling of these information can pose serious threat and huge loss due to information theft. Besides, with limited resources and in specific time-constraints, the study of algorithms can enable developers to design efficient systems. For example, the Triple DES works very well for encryption. But if one decides to build a protocol with it, then it can be insecure due to its small(64 bit) key size [21]. Hence, comparison on the following characteristics is performed in order to distinguish algorithms suited to the user's purpose: **i.**Block size, **2.** Key size, **3.** Speed, **4.** Complexity and **5.** Attacks.

3 Background and Terminology

Key size: The number of bits used in forming the key of an encryption algorithm is called its key size. The security of an algorithm is directly dependent on its key size since a higher key size denotes that it is more difficult to break by a brute force attack.

Block size: The size of bit streams taken by an algorithm for encryption of data is called its block size. This denotes the efficiency of an algorithm. According to the birthday paradox, once an algorithm of 64 bit block size accumulates block of 2^{32} x 8 = 32 GB of data, then there occurs a 50% chance of two or more blocks being the same that can lead to a leak of information.[18]

4 Overview of Approach

Both theoretical and practical approaches were aimed to perform comparisons among encryption algorithms. The detailed timeline followed to complete the project is presented as follows:

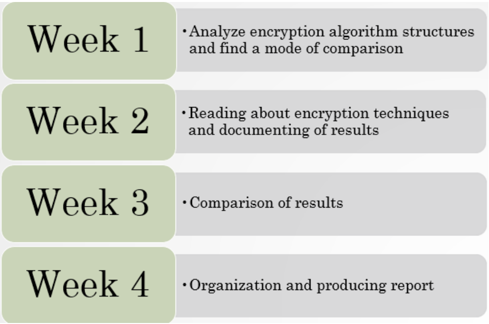
Week 1
•Analyze encryption algorithm structures and find a mode of comparison
Week 2
•Reading about encryption techniques and documenting of results
Week 3
•Comparison of results
Week 4
•Organization and producing report

Figure 1. Timeline of the Project

The algorithms were run in a Windows x64 processor using the following:
Tools: Python libraries
Inputs: Random test inputs generated in Python consisting of alphanumeric and special characters. Inputs of sizes upto 5MB was tested to demonstrate the speed of the symmetric encryption algorithms.

5 More Details about Approach

5.1 Symmetric Encryption Algorithms

5.1.1 DES: . Data is ciphered taking 64 bits block of data at a time and performing permutations and substitution on it

Conference'17, July 2017, Washington, DC, USA
© 2020 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM. . . $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Samantha Barua Chowdhury
Department of Electrical and Computing Science, University of Alberta
Edmonton, Alberta, Canada
sc12@ualberta.ca

with the help of secret key. The process occurs in 16 rounds, where each encrypted block is dependent on all other previous blocks. [31]
Block Size: 64 bit
Key Size: 56bit. Of them, 8 bits are used for parity, which leaves 48 bits for encryption, making it more vulnerable to attacks.
Speed: 8.34197s
Complexity: O(2^{55})
Attacks:

1. Since the key size determines the number of possible keys, by brute force, it would take an attacker a maximum of 2^{56} or 72,057,594,037,927,936 attempts to find the correct key. [31].
2. More vulnerable to Linear cryptanalysis than differential cryptanalysis, using 2^{43} pair of known plaintexts, though it's claimed to be quite impractical in reality.[12]

Uses:

1. Due to simplicity,it is used in smart cards, SIM cards and other embedded systems.
2. Encryption in network devices including modem, settop boxes and routers are often done with DES. [31]

5.1.2 Triple DES: .

It uses a key bundle consisted of 3 DES keys as, **K1, K2, K3**, each with size 56 bits. The encryption algorithm is[22]:

$$ciphertext = E_{K3} D_{K2} E_{K1} plaintext \tag{1}$$

3DES applies the DES technique 3 times to each block, thus providing an increase in key size without having to introduct a new cipher algorithm.
Block Size: 64 bit [22]
Key Size: 3x56 = 168 bits in 3TDES with keys K1, K2 and K3.
2x56 = 112 bits in 2TDES with keys K1 and K2. [19]
Speed: 0.7277s
Attacks: According to the draft guidance published by NIST (National Institute of Standards and Technology) on July 19, 2018, it was proposed that 3DES would be deprecated for all new applications and usage will be disallowed after 2023 due to the possibility of cryptanalysis by birthday paradox. [24]
Uses: The current uses of 3DES include:

1. Encryption of in-transit and at-rest data.
2. Ensuring protected credit card transaction by encrypting EMV keys. [24]

5.1.3 IDEA (International Data Encryption Algorithm):

IDEA encrypts data by 4 complete rounds and 1 half round of operations, where each complete round does the following operatons.[1]

1. Bitwise XOR
2. Addition modulo (2^4)
3. Multiplication modulo (2^4)+1

Block Size: 64 bits [2]
Key Size: 123 bits [2]
Attacks:

1. In 2011, it was broken by a meet-in-the-middle attack.
2. Full 8.5 round IDEA was broken by a narrow-bicliques attack in 2012. [2]

Uses: Immune to differential cryptanalysis which makes its use a lot diverse.

5.1.4 Rijndael:

This algorithm is used as the AES that aims to provide resistance to all attacks with high speed and simple algorithmic design.[13]
Block Size: 128 bits [13]
Key Size: 128 bits, 160 bits, 192 bits, 224 bits and 256 bits [17]
Speed: 0.038s
Complexity: It requires 9 rounds for 128 bits, 11 rounds for 192 bits and 13 rounds for 256 bits during encryption.[3]
Attacks:

1. Weak to an attack called the "Square Attack" based on matrix multiplication.
2. Theoretical vulnerability to side-channel attack and biclique attacks were presented.

However, none of these attacks were imposed on practical terms. [16]
Uses: Requires less memory due to which it can run efficiently on computing platforms such as, smart cards, desktop systems and mobile devices. [13]

5.1.5 Blowfish:

This algorithm is used as the AES that aims to provide resistance to all attacks with high speed and simple algorithmic design.[13]
Block Size: 64 bits.
Key Size: 32 to 448 bits of variable size. [4]
Speed: 0.00204s. One of the fastest algorithms, except when changing keys.[5]
Complexity: For each key, encryption routine runs 522 times.[6]
Attacks: Small block size makes it more vulnerable to birthday attacks compared to the 128 bits used in AES.[20]
Though key scheduling protects against brute force attacks, it has never been hacked till date. [6]
Uses: Used in processors of mobile phones, notebook and desktop computers, for example, the product SplashID uses Blowfish. [5]

5.1.6 Twofish:

To replace the DES algorithm, Twofish with a Feistel network was developed. In each round, half of the text block is sent through an F-function and the other half is XOR-ed.[14]
Block Size: 128 bits.
Key Size: 128 bits, 192 bits, 256 bits. [15]
Attacks: Cryptanalysis include theoretical attacks with 2^{64} chosen plaintexts under each key involving 2^{32} work. But it

is not very practical to implement [15]

Uses:

1. Password management tools, such as, KeePass, Password Sage, use Twofish that deals with generation and storage of passwords for communication.
2. Encryption of contents of email used by PGP (Pretty Good Privacy) software.
3. Protection of files on devices using TrueCrypt encryption software.[26]
4. Used in network applications when there is little to no RAM or ROM available. [15]

Parameter	Symmetric Encryption Technique					
	DES	3DES	IDEA	Rijndael	Blowfish	Twofish
Block Size	64 bit	64 bit	64 bit	128 bit	64 bit	128 bit
Key Size	56 bit	168 bit	123 bit	128 bits 256 bits	32 bits - 448 bits	128 bits - 256 bits
Speed	8.3412s	0.7277s		0.038s	0.00204s	
Attacks	Vulnenrable due to short key	Birthday attack	Meet in-the middle, narrow bi-cliques attack	Matrix multiplication based "Square attack"	Small block size-birthday attack	Theoretical attaks - 2^{64} plaintexts, 2^{32} work
Uses	Embedded Systems	In-transit & at-rest data	Diverse use for immunity to differential cryptanalysis	Can run on less memory -smart cards mobile devices	SplashID-notebooks, computers	Network, manage password, encrypt emails

Table 1. Performance evaluation for Symmetric-key Encryption Algorithms

5.2 Asymmetric Encryption Algorithm

5.2.1 RSA (Rivest-Shamir-Adlemann):

5.2.1 RSA (Rivest-Shamir-Adlemann): The security of RSA is based on the difficulty of factoring large integers. It allows sending of encrypted messages without any prior exchange of secret keys and also verification of an authorised sender. [7]

Key Size: 1024 bits, 2048 bits, 4096 bits.

Attacks:

1. Discovery of public key resulting from poor key generation by taking primes p and q too close to each other.
2. An attacker can launch side channel attacks observing the decryption of timing on target devices and using information from RSA implementation. This can be mitigated by cyptographic blinding, by adding an off-value to remove the correlation.[8]

Uses:

1. Implementation of digital signature where origin of messages is verified.
2. Encryption during information transfer. [8]

5.2.2 Diffie-Hellman): This algorithm helps to generate a shared secret such that it cannot be noticed from observing the communication. It provides encryption of traffic with the public key which ensures that finding our the key by analyzing traffic is not possible. [25]

Key Size: 1024 bits, 2048 bits, 4096 bits.

Attacks: Vulnerable to man-in-the-middle attack for which it needs authentication implementation. [9] **Uses:**

1. Securely develop shared secrets.
2. Safe disrtibution of keys. Frequently used in security protocols such as, TLS, Ipsec, SSH, etc. [9]

5.2.3 Cramer-Shoup Cryptosystem: This computationally efficient cryptosystem is one of the few CCA-2 secure systems without requiring zero knowledge proofs.Its in tractability assumptions are limited to DDH and hash functions when using hybrid encryption. [27]

Key Size: 1024 bits, 2048 bits, 4096 bits.

Complexity: Ciphertext is twice as large as in El-Gamal.

Attacks:

1. It is the first efficient scheme proven to be secure against adaptive chosen ciphertext attack.
2. Non-malleable against resourceful attacker by using collision-resistant hash functions and performing additional computations. [10]

5.2.4 El-Gamal: Due to the probabilistic nature of the El-Gamal cryptosystem, a single plaintext can be encrypted into many ciphertexts. This produces an expansion of size from plaintext to ciphertext in the ratio 2:1. [23]

Key Size: 1024 bits, 2048 bits, 4096 bits.

Attacks:

1. Not secure under chosen ciphertext attack. [23]
2. Security is based on the complexity during computation of discrete logs in a large prime modulus. [11]

Uses: Establishments of secure channel for sharing of keys.

Parameter	Asymmetric Encryption Technique			
	RSA	Diffie-Hellman	Cramer Shoup	El-Gamal
Attacks	Poor key generation	Man-in the-middle attack	Secure against adaptive chosen ciphertext attack	Chosen ciphertext attack
Uses	Digital signature	Security protocols-SSH, TLS	Ensure non-malleability against resourceful attacker	Secure channel for sharing keys

Table 2. Performance evaluation for Asymmetric-key Encryption Algorithms

6 Evaluation

The time taken for the symmetric algorithms to encrypt a 5 MB data is shown below:

All the codes were run using python libraries from pycryptodome and PYPI. The comparison shows that Blowfish

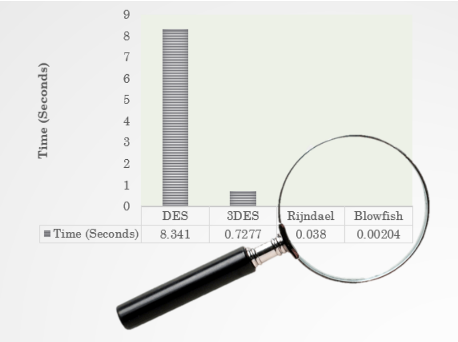

Figure 2. Time Comparison - 1

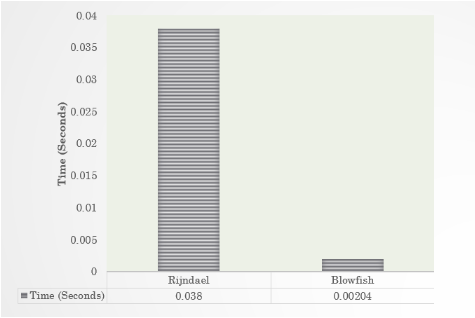

Figure 3. Time Comparison - 2

has the highest speed of all symmetric algorithms. The performance of all the algorithms can be improved my implementing these in C language.

7 Related Work

A rich study of encryption techniques have been done in the preceding years that are closely in line with the proposed work. The authors of the paper [28] have provided a well-thought-out study that explains the idea of symmetric encryption techniques and makes a comparison among them depending on the block size, key size, algorithm structure, rounds and attacks faced by them.

In [29], a performance comparison of symmetric encryption techniques is done using the VHDL platform.

The papers [33], [30] and [32] include a detailed comparison of both symmetric and asymmetric encryption techniques that successfully provide an idea about vulnerabilities of various algorithms and countermeasures.

However, some new encryption methodologies have emerged in the recent years, the analysis of which might yield users with a deeper insight into the use of these methods. So, comparison including the following algorithms were done in this project which could not be found in any of the aforementioned papers. These are:

1. Twofish
2. Cramer-Shoup cryptosystem
3. El-Gamal encryption

Besides, description of the measure of speed of symmetric algorithms, attacks each algorithm is vulnerable to and uses are provided in the study of this project which were not found in the papers studied.

Yet a lot of scope remains in improving the study by incorporating the speed of asymmetric encryption algorithms and exploring faster methods of implementing them, for example, using C language.

8 Conclusion

This project gives a brief idea about symmetric and asymmetric encryption techniques. It shows that almost all the techniques are applicable for real time encryption and also the security level they provide. Future work on this project can include the effect of hybrid encryption techniques on the speed and security of encrypted messages.

References

[1] [n.d.]. https://www.geeksforgeeks.org/simplified-international-data-encryption-algorithm-idea/.
[2] [n.d.]. https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm.
[3] [n.d.]. https://searchsecurity.techtarget.com/definition/Rijndael.
[4] [n.d.]. https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/.
[5] [n.d.]. https://www.splashdata.com/splashid/blowfish.html.
[6] [n.d.]. https://study.com/academy/lesson/blowfish-encryption-strength-example.html.
[7] [n.d.]. https://www.di-mgt.com.au/rsa_alg.html.
[8] [n.d.]. https://www.drdobbs.com/security/the-twofish-encryption-algorithm/184410744.
[9] [n.d.]. https://doubleoctopus.com/security-wiki/encryption-and-cryptography/diffie-hellman-algorithm/.
[10] [n.d.]. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-cramer-shoup_cryptosystem.
[11] [n.d.]. http://homepages.math.uic.edu/~leon/mcs425-s08/handouts/el-gamal.pdf.
[12] [n.d.]. Ch-6, Data Encryption Standard. https://academic.csuohio.edu/yuc/security.
[13] 13 February, 2017. https://blog.finjan.com/rijndael-encryption-algorithm/.
[14] 1998. https://www.drdobbs.com/security/the-twofish-encryption-algorithm/184410744.
[15] 1998. https://www.schneier.com/academic/archives/1998/12/the_twofish_encrypti.html.
[16] 2000. https://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html.
[17] 2016. https://crypto.stackexchange.com/questions/31632/what-is-the-difference-between-key-size-and-block-size-for-aes.
[18] 2018. https://en.wikipedia.org/wiki/Block_size_(cryptography).
[19] 2018. https://www.tutorialspoint.com/cryptography/triple_des.html.
[20] 2018. https://www.commonlounge.com/discussion/d95616beecc148daaa23f35178691c35.
[21] 2019. https://crypto.stackexchange.com/questions/51629/is-triple-des-still-considered-safe-to-use.
[22] 31 January, 2019. Triple DES. https://en.wikipedia.org/wiki/Triple_DES.
[23] April 9, 2020. https://en.wikipedia.org/wiki/ElGamal_encryption.

[24] August, 2018. https://www.cryptomathic.com/news-events/blog/3des-is-officially-being-retired.

[25] July 7, 2019. https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english.

[26] March 7, 2019. https://choosetoencrypt.com/tech/twofish-encryption/.

[27] October 22, 2014. https://homepages.cwi.nl/~schaffne/courses/crypto/2014/presentations/Eileen_CramerShoup.pdf.

[28] Monika Agrawal and Pradeep Mishra. 2012. A comparative survey on symmetric key encryption techniques. *International Journal on Computer Science and Engineering* 4, 5 (2012), 877.

[29] Deepak Kumar Dakate and Pawan Dubey. 2012. Performance comparison of symmetric data encryption techniques. *IDEA* 128 (2012), 58.

[30] Yogesh Kumar, Rajiv Munjal, and Harsh Sharma. 2011. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. *International Journal of Computer Science and Management Studies* 11, 03 (2011), 60–63.

[31] Gurpreet Singh. 2013. Network Security Data Encryption Standard. https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard.

[32] Gurpreet Singh. 2013. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications* 67, 19 (2013).

[33] Ritu Tripathi and Sanjay Agrawal. 2014. Comparative study of symmetric and asymmetric cryptography techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC)* 1, 6 (2014), 68–76.