A Comparative Study of Different Data Encryption and Decryption Techniques

Sérgio Oliveira [21907522]

[1] Lusofona University of Porto,Portugal
a21907522@mso365.ulp.pt

Abstract. We all know the online world is getting more and more powerful and we all connected to it, in a way or another. The interconnection of computer networks is increasing and with it, the cyber-attacks are getting more and more sophisticated. With that being said, we need to find a way to keep the data safe and Cryptography is one of the ways. What Cryptography does is find a way to keep the confidentiality, integrity, authentication, and we can maintain the identification of the data user all secure and sealed, and the only people to have authorization are the user or an associate. Symmetric keys and public keys are well known in the Cryptography world. Symmetric key cryptography is a technique which secures an immense capacity of confidentiality and data security, using a communication channel with a common key to encrypt and decrypt. I tis also important to mention the Fundamentals of Cryptography and its algorithms and concepts. In this project I will focus on symmetric data encryption methods that are Data Encryption Standard (DES), Triple Data Encryption Algorithm (TDEA), Advanced Encryption Standard (AES) and adding up I will mention blowfish and twofish tactic. On the side of asymmetric data encryption, I will mention about RSA(Rivest-Shamir-Adleman) and TEA (Tiny Encryption Algorithm).

I will talk about their ability to secure data and efficiency to encrypt as well.

Keywords: Cryptography, DES, TDEA, AES, RSA, Symmetric key, Encrypt, Decrypt, Data, Blowfish

1 Introduction

Over the years, computer network and internet are more and more involved in our modern society. Online banking services, payment of bills, exponential growing of some applications on the network need a safe environment that guarantees privacy and confidentiality.

We can't leave these transactions and growing applications without security and control because it makes them vulnerable to violations, so, when we are dealing with transactions and applications that are carried throughout the public sector or wireless networks, we need to secure the network management and monitor the process to prevent any violations, so we need to make sure that we guarantee data authentication, integrity, privacy and integrity of data.

This makes us able to guarantee precision and consistency throughout the information lifecycle and it's critical to any system that stores, processes, or retrieves data. This is very important to confirm someone as authentic, that is, claiming the veracity of something or someone.

The act of transferring data through the internet is that there are many security aspects that we need to be aware of, from secure commerce and online payments to private communications and password protection. So that's when we include cryptography to make all this safe and secure. We use cryptography when we need to secure privacy during several online transfers as well as data [1].

Cryptography uses an algorithm that helps us prevent and secure the information against violations. This algorithm can classify into a symmetric key, which is also called a private key, and an asymmetric key, also called a public key [2]. This are used to prevent or delay unauthorized access so sensitive information with the purpose of secure and hiding information. When you use the same cryptography keys to encrypt and decrypt a message it's called symmetric key but when you use a different key to encrypt and decrypt a message it's called asymmetric key.

Today we need to connect cryptography to the open networks, where it will be used to keep the information confidential, because of the information transfer that goes on between people or organization [3].

2 Fundamentals of Cryptography

Cryptography is a fundamental information security system that as several important uses that guarantees confidentiality and integrity of the information or data. Actuality is a technique that aims to the point that every message sent is current, which is that it doesn't allow intruders to repeat old messages over and over, which also prevents the overflow of the system.

Cryptography also aims for the authentication that the sender and the receiver must have an account authenticated, integrity of data that the message sent and received is the same (not modified), confidentiality which is that the message cannot be read or understood by unauthorized people and neither the sender nor the receiver can deny that the information was sent by them.

2.1 Redundancy

Redundancy is usually referred as a technique aimed at preventing an intruder from trying to send data that could usually be considered valid by the recipient in a transmission.

We can ask ourselves: "Is redundancy a bad thing?". The answer is: "no", it isn't. Although not the most linguistically correct way, redundance somehow tries to force the user to focus on a certain idea, word or somewhat information.

An example of redundancy is the use of the word new, for example "new innovation", we are reenforcing the idea of an innovation when an innovation is already something new [4].

The graph below shows an experiment made by Vox that consists in rewriting old articles and turning them in new posts [5].

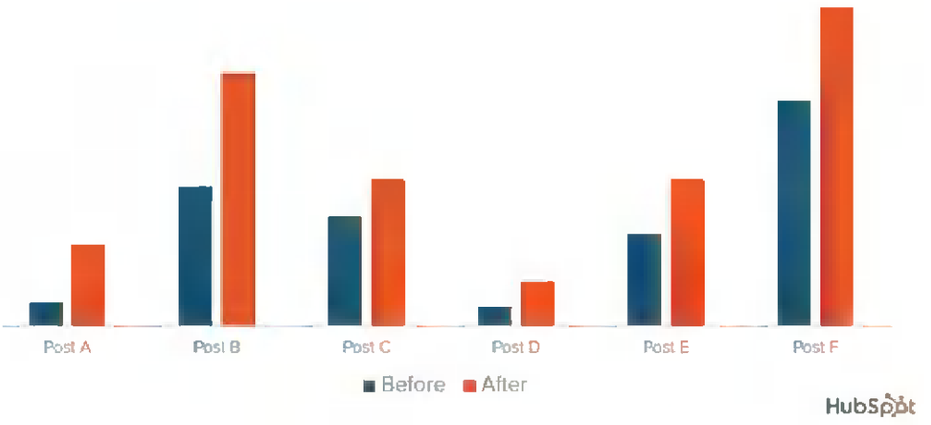

Fig.1- Monthly views from organic search before and after the update in 2015 made by Vox.

3 Cryptography Techniques

The most general security system in the online world is cryptography that secures and prevents unauthorized accesses.

3.1 What is the meaning of Cryptography?

The importance of not revealing secrets to the "outside world" started to intrigue people to develop a way to share messages that, only the person that sent and the person that received, be able to read its content.

Cryptography is also referred as secret writing. We use this term when we mean the transformation of messages using the mechanism of symmetric and asymmetric keys.

3.1.2 Symmetric and asymmetric keys

Symmetric keys and asymmetric keys serve the same purpose but in different ways. Starting with symmetric keys, they use the same key to encrypt and decrypt a message, making this a more secure and fast way. In the other hand, asymmetric keys use a

different key to encrypt and decrypt a message. In this case, as there are two different keys, the one used to encrypt is a public key and to decrypt. Another difference between this to encryption methods are that asymmetric algorithms are much slower than symmetric ones and it's not very effective to use them unless we have a big amount of data. As they are sometimes used together some experts call it hybrid encryption [6].

4 Cypher concept

When we talk about cryptography, a word that we hear a lot is cypher, but what is cypher? Cypher is an algorithm that is used to encrypt and decrypt messages to create a secret writing. There are different types of cyphers but what is common between most of them, is their ability to numbers or symbols for letters which is needed a key to decipher.

4.1 Plaintext

Plaintext is the input of a message, that is, the way that when you read a message it makes sense. This algorithm makes plaintext being transformed in ciphertext. The process is algo called encrypt and decrypt.

4.2 Ciphertext

Ciphertext is the transformation of the plaintext, which is, the transformation of the original message into an encrypted message. Ciphertext can't be read until it's converted back into plaintext, or in other words, being decrypted.

4.3 Substitution Cypher

The substitution cypher is a pre-defined system that are deciphered by inverse substitution. There are some types of cypher substitution such as:

- Simple substitution- Each letter is filtered one by one.
- Polygraphy replacement- Filtering is made from a group of letters.
- Monoalphabetic- Uses a single fixed substitution in the entire message.
- Polyalphabetic- Uses more than

Example of plaintext being transformed into ciphertext through substitution cypher:

Plaintext: GRAY FOX HAS ARRIVED
Ciphertext: UKQN YGB IQL QKKOCT

4.4 Transposition Cipher

Transposition Cipher proceeds to change the letter of the text to be ciphered to another letter. An example of this is columnar transposition where each character is written horizontally with specified alphabet width.

The following image shows an example of a transposition cipher where the message is written out in rows of a pre-defined length. The example is the word HACK (length 4).

The alphabetical order in this case will be "3 1 2 4" and in the end the message is read off in columns.

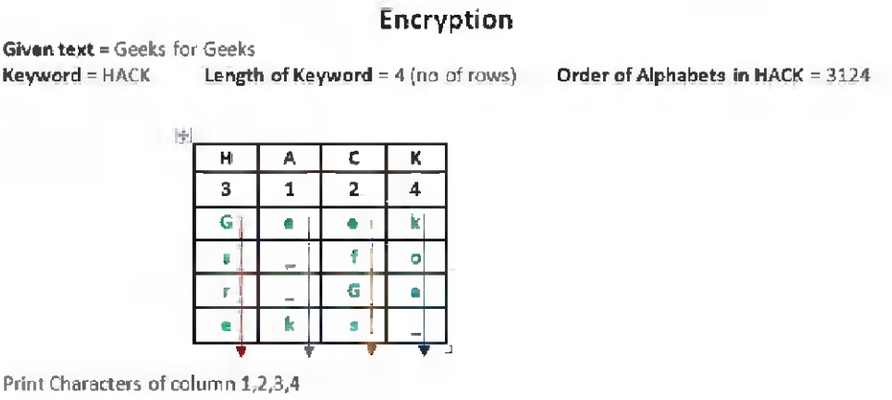

Fig.3- Example of encryption of the word "HACK" through transposition cipher

The final text after encryption will be: "e kefGsrekoe_"

4.5 Caesar's Cipher

Is one of the most used ciphers but is simple as well. It consists in choose a letter of the common alphabet and replace that same letter by its corresponding three places ahead, and that's it [7].

For example, the letter R is replaced by the letter Q, the letter D is A is replaced by the letter D, etc.

6

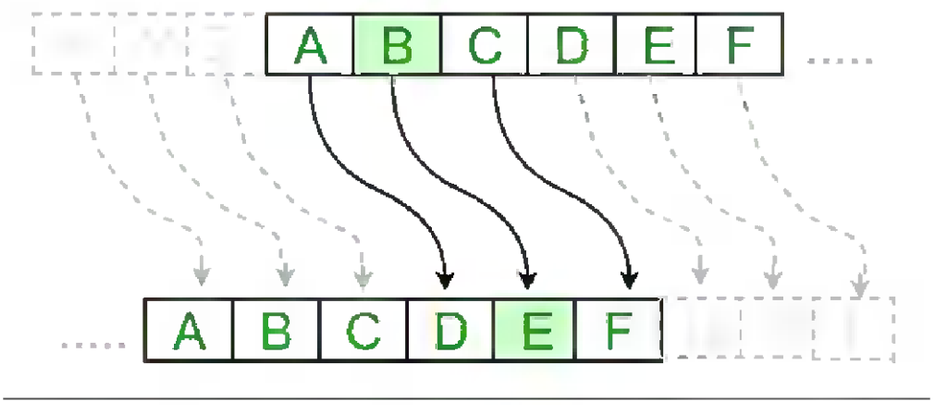

Fig.2- Example of Caesar's Cipher with a shift of three.

Although it's predefined as a shift of three it can also shift an integer between 0 to 25.

4.6 Vigenère Cipher

This cipher is based on Caesar's Cipher because it's based on the letters of the regular alphabet just as Caesar's Cipher. This works as the following explanation: If the number of characters in the key is lower than the number of characters of the message, the key will be repeated until both have the same number of characters.

Example:

Plaintext: attackatdawn
Keyword: LEMON ➔LEMONLEMONLE (after the length is equal)
Ciphertext: LXFOPVEFRNHR

4.7 The Vermam Cipher

The Vermam Cipher uses the Boolean system "XOR" (represented by "⊕") to cypher and decipher, and it's much stronger when used in numbers.

A	B	A ⊕ B
1	0	0
0	1	1
1	0	1
1	1	0

Fig.4- Table referring to the Vermam Cipher

Example of Vernam Cipher:

Plaintext: Hi! 1001000 1101001 0100001
Key: 0l;@ XOR 0110000 1101100 0111011 1000000
Ciphertext: 1111000 0000101 0011010 1000000

Only the symmetric key can decrypt the example.

5 Encryption Algorithms

5.1 Data Encryption Standard (DES)

Data Encryption Standard is an Algorithm that encrypts and decrypts data in 64-bit blocks using a key of 56 bit. Data encryption standard uses plaintext and ciphertext with both using inputs and outputs of 64-bit blocks, always operating in equal size.

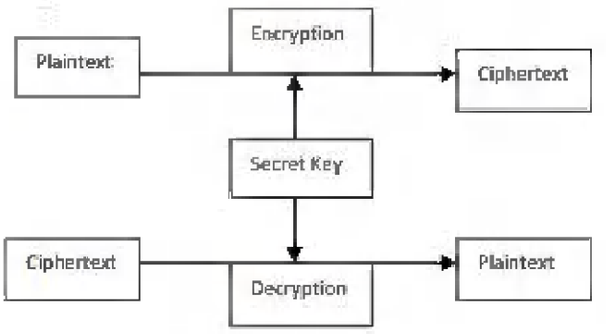

Fig.5- DES Encryption Process [8].

5.2 Triple Data Encryption Standard (TDES)

Triple Data Encryption Standard is a successor of Data Encryption Standard. It's also a symmetric encryption which applies the same algorithm as Data Encryption Standard but doing it three times each data block. This method is using to encrypt passwords and pins.

8

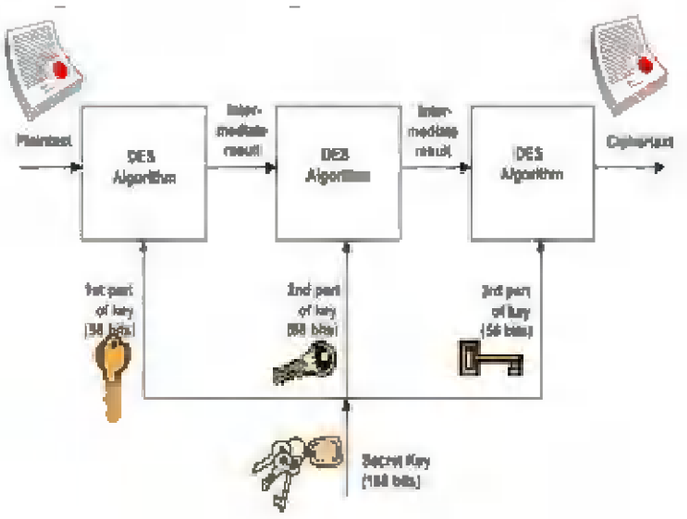

Fig.6- 3DES Encryption Process Block Diagram [9].

5.3 Advanced Encryption Standard (AES)

This is an algorithm that uses a 128-bit form, a 192-bit form and a 256bit-form for the most challenging encryption purposes.
This algorithm is known for his ability to block every attack except the attacks using brute force.

5.4 Blowfish

Blowfish is also an algorithm made to replace DES. This tool can break the message that is being sent into 64-bit blocks and encrypts each of them individually. It's used most for secure passwords and payments duo his speed and flexibility.

5.5 Twofish

Twofish is blowfish's successor that deciphers 128-bit data blocks and encrypts it in 16 rounds not depending on key size. It's known for his speed in software and hardware environments.

5.6 Rivest-Shamir-Adleman (RSA)

This is a slow asymmetric encryption algorithm that factorizes the product of two large prime numbers and the only way to decode the message in a successful way is having the knowledge of these two numbers.

5.7 Tiny Encryption Algorithm (TEA)

This is a simple, safe and effective algorithm that works using a 64-bit block that divides in two 32bit-blocks and uses a 128 bit-block key that divides itself in four smaller 32bits-key that is used in each one of four sub cycles [10].

```
void code(long* v, long* k)  {
      unsigned long y=v[0],z=v[1], sum=0,     /* set up */
                   delta=0x9e3779b9,   /* a key schedule constant */
                   n=32 ;

      while (n-->0) {                         /* basic cycle start */
            sum += delta ;
            y += ((z<<4)+k[0]) ^ (z+sum) ^ ((z>>5)+k[1]) ;
            z += ((y<<4)+k[2]) ^ (y+sum) ^ ((y>>5)+k[3]) ;
       }                                      /* end cycle */
      v[0]=y ; v[1]=z ; }
```

Fig.7- TEA Encryption Function

6 Simulation Analysis

"For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems" [11]. The next table will show how much faster blowfish algorithm to encrypt when all the algorithms (DES, 3DES, AES, Blowfish) with different text file sizes.

10

Text File Size (in Kbytes)	AES	3DES	Blowfish	DES
20	42	34	25	20
48	55	55	37	30
108	40	48	45	35
242	91	82	46	51
322	115	115	48	47
780	165	170	65	85
910	213	230	68	145
5501	260	310	120	250
7200	210	286	109	260
7838	1240	1470	122	1280
22335	1370	1800	155	1720
42000	1530	2300	165	2100
99000	1720	2750	190	2600
Average Time	542.38	742.31	91.92	663.31

Table 1- Comparative Encryption times (in ms) of various algorithms with different packet size

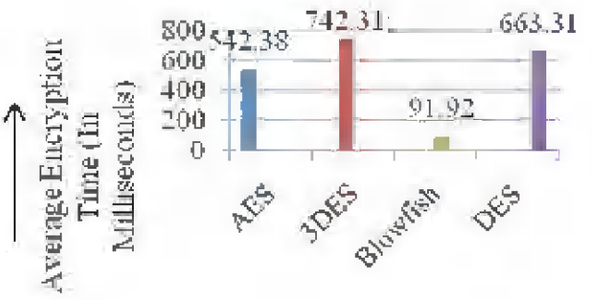

Fig.8- Encryption time of each Algorithm (in ms)

After analyzing both the table and the figure we can conclude that the algorithm with the fastest Encryption time is blowfish by far and the slowest one is 3DES with DES not far behind. We can see that in the beginning with the lighter files DES Encryption was faster than Blowfish but over 780kb the blowfish became faster. For last, the average time is much lower on blowfish algorithm than on AES, DES and 3DES.

Input size in (Kbytes)	AES	3DES	Blow fish	DES
49	63	53	38	50
59	58	51	26	42
100	60	57	52	57
247	76	77	66	72
321	149	87	92	74
694	142	147	89	120
899	171	171	102	152
963	164	177	80	157
5345.28	655	833	149	783
7310.336	882	1101	140	953
Average Time	242	275.6	83.4	246

Table 2- Comparative Decryption times (in ms) of various algorithms with different packet size

From this table we can easily see that Blowfish is a better option to decrypt than the other algorithms. We can also tell that AES is faster than 3DES and DES, and even though 3DES is a successor of DES it is still slower than it [12].

The values of the AES, 3DES and DES decryption time is similar, but once again blowfish is much lower than the others. We can see that from the beginning blowfish "leads" from the beginning the timer, making it faster and more efficient. AES starts with the most time to decrypt but over 899kb it is equal to 3DES but slower than DES.

When we get to the 5345.28kb, AES surpasses 3DES and DES, making it the second one with the lowest time to decrypt, so we conclude that decryption process is a little influenced by size.

7 Conclusion

This paper above presented is a Comparative Study of Different Data Encryption and Decryption Techniques. For this to happen it was explained first what cryptography was and how was this concept important for this study. It was studied how these methods work and how can they be useful to a society that is more and more dependent of the internet and online services. It was shown how their algorithms operate and their performance. The algorithms that were compared are AES, 3DES, Blowfish and DES and it was concluded that Blowfish is the most effective algorithm in terms of performance and sometimes is the most needed to serve a certain job. In the other hand, 3DES was shown as the least effective one, taking more time than the other to encrypt and decrypt. The speed and power of this symmetric algorithm is amazing. On the other hand, on the asymmetric side, RSA is the most used on online network duo his speed and security. The goal is to find an algorithm that is secure, fast and effective.

12

References

1. Kumar, A.Y. (2013) Comparative Study of Different Symmetric Key. International Journal of Application or Innovation in Engineering & Management, 2, 204-206
2. Abd Elminaam, D., Abdual Kader, H.M. and Hadhoud, M.M. (2010) Evaluation of the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, 10, 216-222.
3. Avithra, S. and Ramadevi, E. (2012) Study and Performance Analysis of Cryptography Algorithms. International Journal of Advanced Research in Computer Engineering & Technology, 1, 84
4. Nenchev, Dragomir N. "Redundancy resolution through local optimization: A review." Journal of robotic systems 6.6 (1989): 769-798.
5. Sarik,Marko (2015), Blogging Strategy That Works: Reduce, Reuse, Recycle Content To Attract A New Audience
6. Stallings, W. (2014) Cryptography and Network Security Principles and Practice. Sixth Edition, Prentice Hall, Upper Saddle River.
7. William Stallings (2003), Cryptography and Network Security, 3rd edition, Pearson Education
8. Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.
9. Adhie, Roy Pramono, et al. "Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC)." Journal of Physics: Conference Series. Vol. 954. No. 1. IOP Publishing, 2018.
10. Williams, Derek. "The tiny encryption algorithm (tea)." Network Security (2008): 1-14.
11. Mitali, Vijay Kumar, and Arvind Sharma. "A survey on various cryptography techniques." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3.4 (2014): 307-312.
12. Kansal, Shaify, and Meenakshi Mittal. "Performance evaluation of various symmetric encryption algorithms." 2014 international conference on parallel, distributed and grid computing. IEEE, 2014.