Combination of the “Data Encryption Standard” algorithm (DES) and the “Public-key encryption” algorithm (RSA) on the key-generation stage

Dr. Abdalilah G. Alhalangi [1], Dr. Galal Eldin A. Eltayeb[2]

[1,2] Asst. Prof. Department of Computer Science
Al-Rass College of Science & Arts
Qassim University, Kingdom of Saudi Arabia

Abstract

It is obvious that information is remarkably important and valuables however, it is exposed to danger of theft, hacking, abuse and violation every now and then. Therefore, protection of such valuable information has the attention of all – organization, firms and individuals. Recently, cyber and crimes had developed which exposes information to extreme threat. The dissemination of systems information crimes have spread in industrial countries and Saudi Arabia is no exception due to the development that the country has witnessed and its growing involvement of information systems in different economic and scientific fields besides the increasing use of the internet.Information protection has become crucial and this can be approached through a variety of means and methods. The most important of these means and methods is encryption. Encryption uses different algorithms [2]. This present paper will tackle two algorithms, namely: Data Encryption Standard (DES) and Public Key Algorithm (PKA). The paper also presents how the two algorithms operate, discuss the shortcomings of each of them and then proposes a model which merges the two algorithms in the stage of key generating to come up with solutions for their shortcomings.

Keywords: Encryption, Decryption, DES, PKA, RSA, Plain text, Cipher text, Combination.

1. INTRODUCTION

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption, this can be done by two techniques symmetric-key cryptography and asymmetric key cryptography [17]. Encryption is the science that uses math to hide the original text, and you can encrypt sensitive/important information to transfer over insecure networks such as the Internet and store it, so it can’t be read by anyone except the person who sent to him [1].

Encryption objectives

There are four objectives can be mentioned for encryption [6]:

- Secrecy or privacy (Confidentiality).
- Data combination (Integrity).
- Proof of identity (Authentication).
- Lack of ingratitude (Non repudiation).

Encryption and decryption algorithm code; sometimes called the code, which is a mathematical function that is used in the encoding and decoding process [3].

If the security of an algorithm based on the reserves or the way in which it operates algorithm called restricted algorithm, but this restricted algorithm used for simple information that we need to secure and commonly used by users who do not really care about high security.

The modern encryption system manipulates these problems by using the term key, mentioned here by the letter (K), such that this K can be any big number with space (range), and the range of the key called Key space, the encryption and decryption processes use this key and depend on it [4]. Some algorithms use different keys for encryption and decryption, so if we use K1 and K2, that mean K1 and K2 are different keys. The Security used in some of the algorithm depends on the key and do not depend on the details of the algorithm, and this means that it can be published and can be analyzed, and the components or parts of this algorithm can be defined. There is no problem if unauthorized person knows the algorithm because he could not know the key and thus can’t read the message [5].

Any modern encryption system should have ability to resist any attack by professional code analyst trying to hack the key, or attack the ciphertext using any way or another, and generally, an encryption algorithm is designed to withstand a known-plaintext attack. [6].

2. THE PROBLEM

Data Encryption Standard (DES) is characterized by high level of security and complex features algorithm [5], and analysis of this algorithm by attackers needs a very long time, but in spite of that, we find that this algorithm has a problem, which lies in the stability of the tables used in the process of encryption, such the keys tables and table of the first iteration, and the selection tables 1 and 2 and eight substitution-boxes, ... etc. This problem seems like an open port (security bug) can be attacked by code analysts to gain unauthorized access to the original text.

In public-key encryption system (RSA), the code analyzer may be able to know the public key n, e by analyzing n = (p×q) to find the values p and q, and that is a problem, so it is possible to calculate (using the calculator) ϕ (n) to find the secret key exchange p.

The selection of p and q as initial values with 100 decimal digits will provide reasonable security level as well as to ensure that the p-1 and q-1 has many small factors diminishes the seriousness of the analysis of the number n. And also we find the public key is using these digits, but the lack of these initial values and easy analysis of it will represents another problem for this algorithm [7].

3. PREVIOUS STUDIES

3.1. Study of Matt Blumenthal, 2010 [12], entitled "Encryption: Strengths and Weaknesses of public-key Cryptography (2010)" He studies the strengths and weaknesses in the public-key algorithm, the study concluded that it must integrate public-key encryption algorithm with symmetric to be more secure, he added that the use of digital signature with the key will add complementary data against hackers.

3.2. Study of Haitham Abdel Moneim Saffour, 2010,[9] entitled "Improved Security and Response Time by Using XML Web Service and Caching SSL Session Key", the study shows that using XML Web Services features and reusing cached SSL session keys can significantly improve or reduce client response time and enhance the security and enable clients to increase the efficiency of their mission-critical M-Commerce and e-business operations, and to reduce their risk. The time taken to download secured Web documents, in our tests, is reduced by 20% to 45% (up to load on the servers). The research findings suggest the implementation of this technique in the secured webs.

4.THE COMBINATION OF THE TWO ALGORITHMS

The steps to combine/integrate the (DES) algorithm and (RSA) algorithm together in one at the key-generation stage, we can follow:

a. Generating the (DES) algorithm using 64 bits.
b. Generating a public key algorithm is as follows:

1. Generates two big seed numbers as q and p each and every one of them the same size.
2. Calculate n = p * q
3. Public key algorithm is n and the private key is (p,q), then transforms the public key (n = pq) to 64 bits for this key.
4. Use the operation (or) and Exclusive Or (xor) to integrate the 64 bit, which is comes out from DES with the 64 bits which is comes out from (RSA).
5. Replace the original key of the standard encryption algorithm with the new comes out of the combination.
6. Before starting to encrypt messages by executing the new algorithm, we generate a public key as mentioned, then send the public key to a recipient messages to save it, distributes this key once, but if we replaced from attempt to another, then we generate a standard encryption key code DES and use scientific combination by XOR to integrate key generator of public RSA algorithm and then the message is encrypted with this new key using the standard DES encryption to destination.

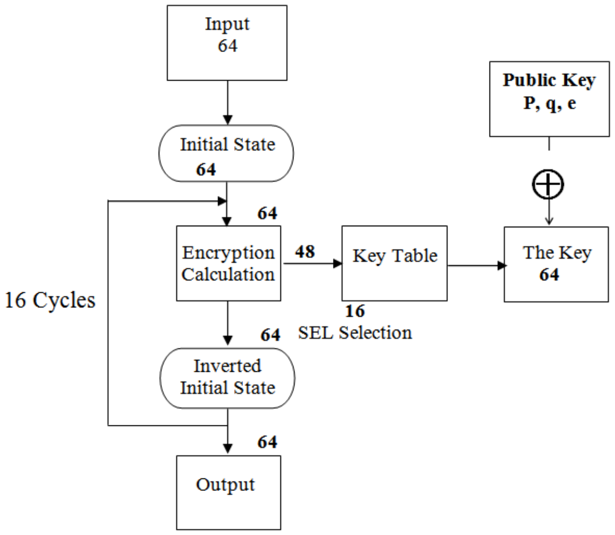

Figure 1: Drawing illustrates the algorithm form the DEA after combined keys

7. Dealing with the stability of the left shifts by generating a number of shifts to the left for each iteration using the random function, generation random number between 1 and 3, and kept shifts in a matrix of reference when the reverse process (decoded), so we have much complications in the problem of the key and the stability, which make it more safe and secure for both algorithms.
8. By this complicated algorithm, it's seems difficult to the code analyzer, who will hurt most by thinking in the tables of this algorithm, from the initial iteration to sixteenth one, analyzing these tables to seek for the bits locations.

For example, the following table represents the second iteration of the key generation, pointing out the bits positions:

Table 1: Second Iteration of the Key generation

Bit Position	PC -2					
1– 6	14	17	11	24	1	5
7–12	3	28	15	6	21	10
13–18	23	19	12	4	26	8
19–24	16	7	27	20	12	2
25–30	41	52	31	37	47	55
31–36	30	40	51	45	33	48
37–42	44	49	39	56	34	53
43–48	46	42	50	36	29	32

According to the bit positions in the table above, according to the organization and arrangement procedural algorithm standard encryption of the data, the code analyzer can detect that the first bit in this table is the position No.5. So he will continue with the rest of the iterations in the table, but may lack that this bit in the first position is not laying in the order of the original key of the algorithm, but the result of an operation (or/xor) with the key code of the public key, so he will be in loss, unless he discover the modification of the algorithm.

5. PRACTICAL RESULTS

1. An algorithm consists of more than an algorithm designed to raise the level of secrecy and complexity of the problem of the distribution of the results.

2. The algorithm included some original ideas in design or in implementation seeking for privacy.

3. The ability to generate code using RSA and combine it via XOR would not be considered by hackers and its combination by XOR operation unthinkable by the code analyzer. So he wasted his time in the key using all standard encryption algorithm analysis.

4. The new encryption key used in the combined algorithm is difficult because it is the product of two algorithms.

6. CONCOLUSION

In general, the concept of information security means "to make others away from doing any act we do not want it on our information" so techniques and methods must be taken to protect this information from the risks that threaten its security. The proposed model provided by this paper takes into consideration the stability of the standard encryption algorithm, which is represents a weakness of the algorithm, as well as taking a few initial numbers used to generate the public, that can make hackers works more difficult. The proposal treats the problem of the two algorithms by combining them into one.

REFRENCES

[1] Douglas Dedo, Pocket PC Security (2002) Mobile Devices Division, Microsoft Corporation.
[2] Scott Wilson, An Introduction to cryptography (2002)
[3] Kirk Job-sluder, cryptography: A guide to protecting your file for consultants, education and researcher Indiana university (2004)
[4] John & Sons, Inc (Applied Cryptography). Second Edition-New York, USA 1996.
[5] Frazier, R. E- (1998,1999) Yahoo.com) Data Encryption Techniques. www.softstrategies.com.
[6] William Stallings. Cryptography and Network Security Principles and Practices. Prentice Hall, November 16, 2005.
[7] Microsoft Course 2524c. (2003) Developing XML Web Services Using Microsoft ASP. NET.
[8] Introduction to Cryptography. www.ipsec.com. Words: 725
[9] Haitham Abdel Moneim SFOR study entitled "improve the response time and security using the Web service language extended coding and save SSL session key object in the Cache - (2013)
[10] Microsoft Application Consulting Team (2002) Performance Testing Microsoft.Net Web Application,.
[11] http://www.microsoft.com/miserver/techinfo/administration/MISsecurity.asp , Last Visit 4/11/2015
[12] Study "Matt Blumenthal entitled Encryption: Strengths and Weaknesses of public-key Cryptography" (2010)
[13] Bay Networks, Inc. (1997). Configuring Software Encryption. www.baynetworks.com.
[14] Biasci, L. (1999). Cryptology. www.whatis.com.
[15] Litterio, F., (1999). Cryptology: The Study of Encryption. www.world.std.com.
[16] SSH Communications Security, (1999). Cryptographic Algorithms. www.ipsec.com.
[17] Sunil K Maakar, and others. "A Performance Analysis of DES and RSA Cryptography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), June 2013
[18] Sung-Jo Han, Heang-Soo Oh, Jongan Park, The improved Data Encryption Standard (DES) Algorithm,Department of Electronic Engineering, Chosun University. South Korea.1996 IEEE.
[19] Charels Connell, An Analysis of New DES: A Modified Version of DES, Locust Street Burlington, USA, Boston MA 02215 USA

AUTHOR

Abdalilah G. Alhalangi is an Assistant Professor in computer science Dept. at Sciences and Arts College in Ar-rass, Qassim University, KSA. He received the PhD. In Information Systems Sudan and his M.S. degree in Information Technology from Al-neelain University at 2012, 2002 respectively.

Galal Eldin A. Eltayeb is an Assistant Professor in computer science Dept. at Sciences and Arts College in Ar-rass, Qassim University, KSA. He received the PhD. In Information technology from Al-neelain University at Sudan in 2010, and his M.S. degree in Computer Science from Khartoum University in 1999.