

Digital Image Encryption Based on RSA Algorithm

Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran

(IEEE senior member, Alexandria University, Egypt)

(IEEE senior member, Electrical Engineering Dept, Alexandria University, Egypt)

(Electrical Engineering Dept, Alexandria University, Egypt)

Abstract: Information Security has become an important issue in data communication. Cryptography has come up as a solution, and plays an important role in information security systems. This paper presents an introduction to the science of cryptography and explains the RSA cryptosystem. It also presents the comparison between RSA cryptosystem with DES and Blowfish cryptosystems applied on greyscale image.

Keywords: Cryptography, Information security, Image Encryption, RSA, DES, Blowfish

I. INTRODUCTION

The Concise Oxford Dictionary defines cryptography as the art of writing or solving codes. This definition may be historically accurate, but it does not capture the essence of modern cryptography. First, it focuses solely on the problem of secret communication. Second, the definition refers to cryptography as an art form. Indeed, until the 20th century (and arguably until late in that century), cryptography was an art. In the late 20th century, this picture of cryptography radically changed. A rich theory emerged, enabling the rigorous study of cryptography as a science. Furthermore, the field of cryptography now encompasses much more than secret communication, including message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronic auctions and elections, and digital cash [1].

Cryptography from Greek *kryptos* meaning hidden, secret and *graph* which means writing is the science of secret writings [2].

According to the type of keys used for encryption (k_e), respectively for decryption (k_d), the cryptosystems are symmetric (private key) or asymmetric (public key).

The creation of public key cryptography by Diffie and Hellman in 1976 and the subsequent invention of the RSA public key cryptosystem by Rivest, Shamir, and Adleman in 1978 are watershed events in the long history of secret communications. It is hard to overestimate the importance of public key cryptosystems and their associated digital signature schemes in the modern world of computers and the Internet [3].

II. Public-Key Cryptosystems

In public key cryptosystems there are two different keys: a public key, which is publicly known, and the secret key, which is kept secret by the owner. The system is called “asymmetric” since the different keys are used for encryption and decryption—the public key and the private key. If data is encrypted with a public key, it can only be decrypted using the corresponding private key, and vice versa. Public key cryptosystems do not need to have a shared secret between communicating parties. This solves the problem of large confidential communication network introduced earlier. In addition, public key cryptography opened door for ways of implementing technologies to ensure all goals of cryptography. By means of combining public key cryptography, public key certification, and secure hash functions, there are protocols that enable digital signatures, authentication, and data integrity [4].

Asymmetric ciphers are computationally much more expensive, but the public key can be distributed to everyone, just one person has to guard the secret part of the key [5].

III. RSA Cryptosystem

In 1978, a paper was published by R. Rivest, A. Shamir, and L. Adleman. In this paper they describe a public-key cryptosystem, including key generation and a public-key cipher, whose security rests upon the presumed difficulty of factoring integers into their prime factors. This cryptosystem, which has come to be known by the acronym from the authors’ names, the *RSA cryptosystem* has stood the test of time to this day, where it is used in cryptographic applications from banking, and e-mail security to e-commerce on the Internet [6].

There are many applications for RSA, but in practice it is most often used for [7]:

- Encryption of small pieces of data, especially for key transport,
- Digital signatures, for digital certificates on the Internet.

IV. Encryption and Decryption Process

- Choose two large distinct primes p and q and then form the *public modulus* $n = pq$.
- Choose *public exponent* e to be coprime to $(p - 1)(q - 1)$, with $1 < e < (p - 1)(q - 1)$.
- The pair (n, e) is the *public key*.
- The private key is the unique integer $1 < d < (p - 1)(q - 1)$ such that $ed = 1 \pmod{(p - 1)(q - 1)}$.
Encryption: Split a message M into a sequence of blocks M_1, M_2, \dots, M_t where each M_i satisfies $0 \leq M_i < n$. Then encrypt these blocks as

$$C \equiv E(M) \equiv M^e \pmod{n}; \tag{1}$$

Decryption: Given the private key d and the ciphertext C , the decryption function is:

$$D(C) \equiv C^d \pmod{n}; \tag{2}$$

Note that encryption does not increase the size of a message. Both the message and the ciphertext are integers in the range 0 to $n - 1$.

The encryption key is thus the pair of positive integers $(e; n)$. Similarly, the decryption key is the pair of positive integers $(d; n)$. Each user makes his encryption key public, and keeps the corresponding decryption key private.

III. Practical Work

We have implemented the code on MATLAB to simulate the algorithm of RSA. We applied RSA algorithm on *digital images* and also show difference in output (cipher) image for shorter or longer key lengths.

Key Generation

As we mentioned before, there are two different prime numbers P and Q used to generate n . We do create the code to generate them. As the length increase, it takes more time to generate relative prime numbers e and d . The following table shows the relation between numbers chosen for P and Q and its established time to generate it.

Table 1: Time established in seconds

Chosen Numbers		Time established (seconds)
P	Q	
7	5	0.010387
11	13	0.040969
17	23	0.124453
29	53	0.964863
47	59	3.504031
113	71	18.675820
239	173	590.455964

Now we used digital images as data to be encrypted. We used a grayscale image with size is 256 X 256. **PC specifications are:**

- System: Windows 7 Ultimate 64-bit Operating System
- Processor: Intel® Core™ i3 CPU M330 @ 2.13 GHz
- RAM: 4 GB



Fig 1: The used image

A relative prime e was chosen with different values and the following is the result:

Table 2: P, Q, E, D, and Time

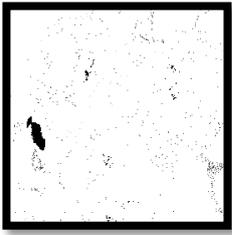
P	239	
Q	173	
E	27	
D	30323	
Time	3.774115	

Table 3: P, Q, E, D, and Time

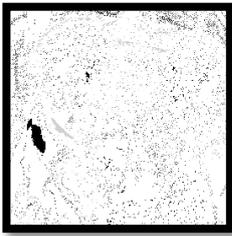
P	113	
Q	71	
E	6469	
D	589	
Time	4.240226	

Table 4: P, Q, E, D, and Time

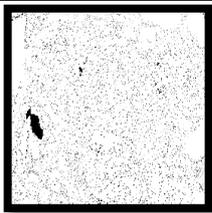
P	47	
Q	59	
E	21	
D	23885	
Time	3.762528	

Table 5: P, Q, E, D, and Time

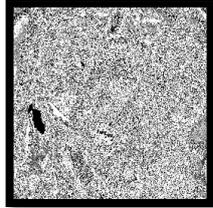
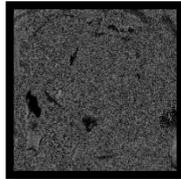
P	17	
Q	23	
E	109	
D	2661	
Time	3.681188	

Table 6: P, Q, E, D, and Time

P	11	
Q	13	
E	47	
D	743	
Time	3.691191	

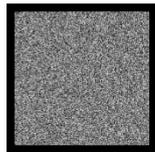
From previous results, it's clear that when the value of prime numbers becomes smaller, the result become poor (not similar) to the original image. So, it's better to choose large prime numbers, theoretically up to 200 digits power 200 digits.

IV. COMPARISON WITH OTHER CRYPTOSYSTEMS

Data Encryption Standard (DES)

Data encryption standard is one of symmetric algorithms developed in early 1970s at IBM and based on an earlier design by Horst Feistel. Now we will encrypt the same image with same size and see the difference between DES and RSA.

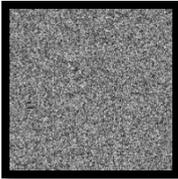
Table 7: Key generation time, encryption time, and decryption time

Key Generation Time	0.295829 seconds.
Encryption Time	56.385263 seconds.
Result	
Decryption Time	63.394748 seconds.
Result	

Blowfish

Blowfish, a new secret-key block cipher, is proposed. It is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place; the actual encryption of data is very efficient on large microprocessors.

Table 8: Key generation time, encryption time, and decryption time

Key Generation Time	7.201574 seconds.
Encryption Time	126.305795 seconds.
Result	
Decryption Time	110.416216 seconds.
Result	

So we can abbreviate the previous result in the following histogram:

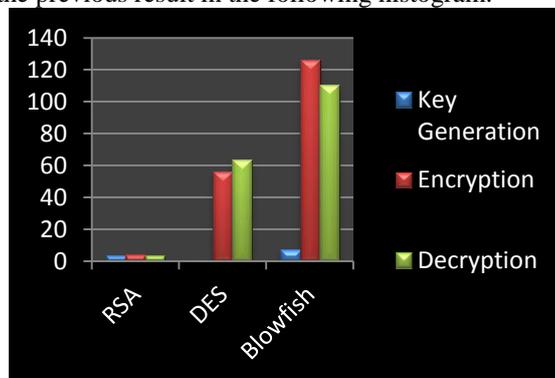


Fig 2: Difference in established time between RSA and other symmetric cryptosystems

VII. CONCLUSION

This paper provided a comparison between RSA cryptosystem which is one of asymmetric cryptosystems and the two symmetric systems, DES and Blowfish. The results showed that time taken using mathematical relations in RSA make steps faster implemented than DES and Blowfish algorithms and with more secured data than symmetric systems. But, in RSA the value of chosen prime numbers Q and P controls time in key generation so that it increases time taken due to makes it more secured that before.

REFERENCES

- [1] Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols", ISBN: 978-1-58488-551-1, 2008.
- [2] Monica Borda, "Fundamentals in Information Theory and Coding", ISBN: 978-3-642-20346-6, 2011.
- [3] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, "An Introduction to Mathematical Cryptography", ISBN: 978-0-387-77993-5, 2008.
- [4] Borko Furht, Darko Kirovski, "Multimedia Encryption and Authentication Techniques and Applications", ISBN: 0-8493-7212-7, 2006.
- [5] Andreas Uhl, Andreas Pommer, "Image and Video Encryption from Digital Rights Management to Secured Personal Communication", ISBN: 0-387-23403-9, Springer, 2005.
- [6] Richard A. Mollin, "Codes: The Guide to Secrecy from Ancient to Modern Times", ISBN-10: 1-58488-470-3, 2005.
- [7] Christof Paar, Jan Pelzl, "Understanding Cryptography", ISBN 978-3-642-04100-6, Springer, 2010.