Evaluation of Cryptographic Algorithms: RSA and Public Key Cryptography

Büşra Şafak Zırhlı
Student, Dokuz Eylul University,
Faculty of Engineering

***Abstract*— Cryptography is one of the most important tools to protect our information and data. We keep our information confidential using cryptographic techniques. Prevents loss of information and data. Prevents fraud and enables us to access accurate data. The security of the encryption and decryption algorithm is based on mathematical equations. The conversion of mathematical solutions into algorithms ensures confidentiality.**

The key in the encryption algorithm has a key position; this means that once captured, everyone can use it to encrypt and decrypt the information in the encryption system. This causes unwanted situations. The correct algorithm should be selected. In this article, it is proposed to implement RSA encryption / decryption solution based on RSA public key algorithm studies. Further, the encryption procedure and code implementation are described in detail.

***Index-Terms* —**
RSA Algorithm; encryption; decryption

I.INTRODUCTION

One of the main ways to protect private and sensitive information is to use encryption techniques. Ensures data privacy. It is used for storing confidential data, securing system security, authenticating credentials, digital signature checking, as well as running information privacy mechanisms. Our goal is to prevent fraud and forgery. Nowadays, the best-known and most widely used public key system was first developed by RL Rivest et al. This encryption system is an asymmetric (public key) encryption system based on number theory, which is a block encryption system.

RSA, a public key cryptographic system, is one of the best methods for public key cryptography used in digital signature standards and encryption techniques.

II. RELEATED WORKS

A. Brief Introduction on RSA and Public-key Cryptography

The encryption and decryption technique using two different keys is the main feature of the public key encryption system. It comes with two different keys: private key and public key. The private key cannot be generated from the public key that allows the encryption key to be issued. The most important approach of the public key cryptographic algorithm is Hidden Leakage Risk.

RSA that can withstand all known password attacks. The difficulty in predicting plaintext from the signal key and the encryption text is estimated to be equal to the decomposition of two large prime numbers of products. The RSA algorithm is used as a possible authentication method. At the beginning of a lock communication session, it communicates using the Diffie - Hellman algorithm, and the following steps generate the public keys to be used for the lock communication protocol.

Encryption is fast with this method. DES ce RSA key encryption mechanism works in this way because of its ease and security.

B. The Process of RSA Algorithm

The RSA method takes mode n. Defines the smallest processing line without a negative value. Primers p and q result n. The RSA encryption system and algorithm are defined as follows.

The procedure for generating the keys is as follows:

1) Randomly generate: 2 primes P and Q of length K / 2 bit;

2) The public key calculated;
   publicKey = P * Q;
   (public key's length is k-bit)

3) Random encryption generated;
key keyE, 2 <= keyE <= < φ(n) - 1,
where GCD(keyE, φ(n)) = 1;

keyE * keyD mod φ(n)=1,
φ(n) is known as the Euler function of n, the value is φ(n) = (P-1) * (Q-l);

4) The decryption key is calculated,
keyD = keyE - 1 mod(n),
keyE - 1 is inverse for the decrypt key keyD. The formula of the original equation is keyE * keyD mod φ(n) = 1;

C. The Implementation of RSA Cryptosystem

The RSA encryption process is followed by complex steps that produce large integer modular arithmetic of prime numbers and many mathematical calculations. This process is difficult. P and Q numbers are considered to be large prime numbers. p and q are large prime numbers. When searching for p and q prime by factoring, the difficulty is actually the same as attacking the RSA (parsing the large composite number), the computer.

Probabilistic algorithms are not intended to produce prime numbers, but first generate a random large odd number. Then it is determined whether this strange integer is a prime number likely to be probability algorithms. (This process is often called Priority Test)

D. RSA's Security

Whether theoretically equals integer factors in RSA security. It depends on the difficulty of the integer factor. Because there is no evidence that RSA breakage requires factoring. Suppose that there is a large number of non-factoring based algorithms: An integer must be transformed into a factoring algorithm. The most obvious attack method; n is the decomposition.

E. Digital Signature with RSA Algorithm

RSA can be used for authentication. It is not used for encryption only. That is generated compared to the mixed signature is stored as data only to the user. It is kept at a safe level.

Digital signature technology is actually achieved by the hash function.

The properties of the file represent the properties of the digital signature. If a digital signature or file changes, its values also change. Different signatures apply to different files. The hash function is open to both sides of the data. One of the simplest checksums is to add a set of values.

III. SOFTWARE DESIGN

A hierarchy was adopted in the design of the project. User must login as a form in the interface. The RSA algorithm is implemented with C # to create localized components in the local operating system. (This article discusses the C # language in the .NET framework. The calling procedure and design patterns of native components are described in almost the same.)

To take into account the burden of coding, software encryption and decryption of data is strictly incompatible with RSA standard PKCS # I. However, it can obtain a combination of encryption and decryption to meet predetermined design requirements.

IV. IMPLEMENTATION OF RSA ENCRYPTION

A. Realization of the Software

Software application is shown as Figure 1; encrypted file interface is shown as Figure 2; the decrypted file interface is shown as Figure 3; encrypted and decrypted main functions is shown as Figure 4-5-6.

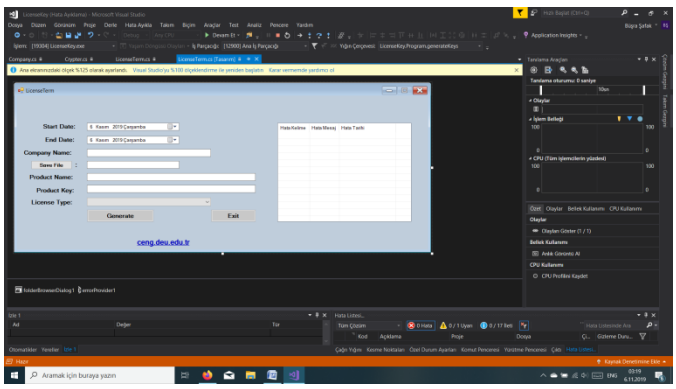

Figure 1: Software Form Application Interface

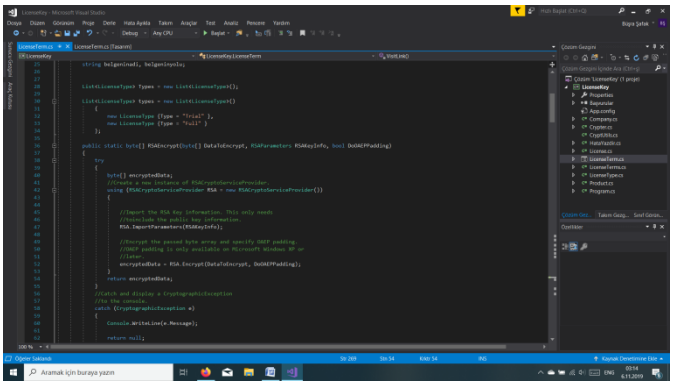

Figure 2: Encrypted File Interface

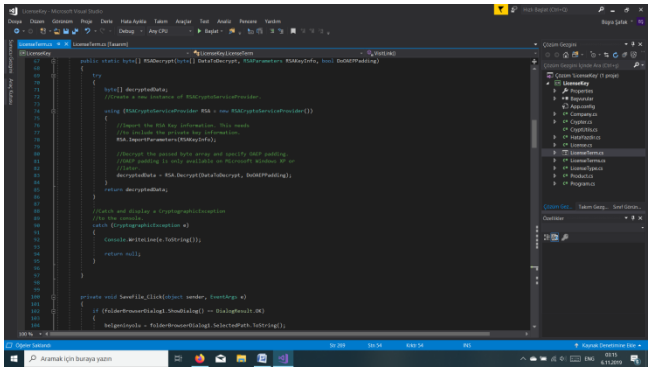

Figure 3: Source File Interface Before Encryption

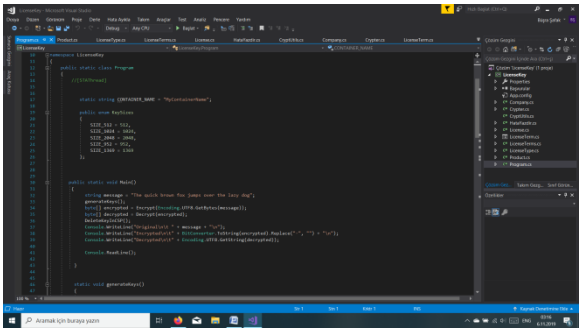

Figure 4: Main Functions

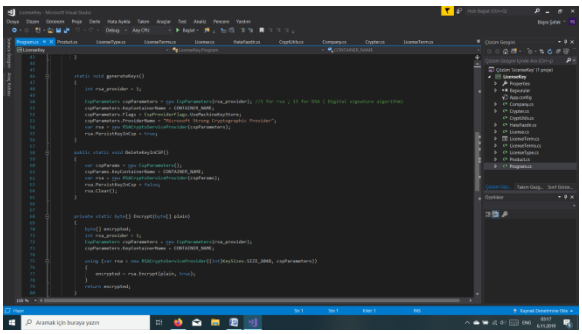

Figure 5: Main Functions

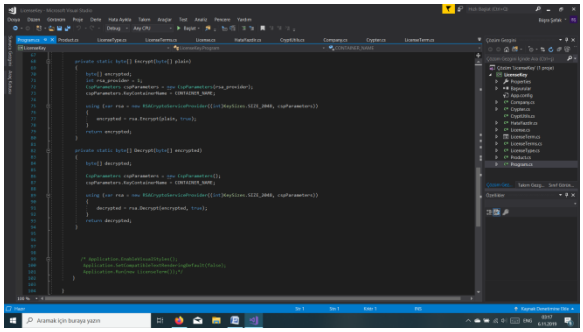

Figure 6: Main Functions

V. REFERENCES

[1] A study and performance of RSA algorithm, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139, ISSN 2320–088X

[2] Comparative Study of Symmetric and Asymmetric Cryptography Techniques by Ritu Tripathi, Sanjay Agrawal compares Symmetric and Asymmetric Cryptography Techniques using throughput, key length, tunability, speed, encryption ratio and security attacks. IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 ISSN (Online): 2231-5268

[3] Comparative analysis of performance efficiency and security measures of some encryption algorithms by AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram compares symmetric and asymmetric cryptography algorithms ISSN: 2248-9622

[4] Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures byYogesh Kumar, Rajiv Munjal, and Harsh ,(IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

[5] Data encryption and decryption by using triple DES and performance analysis of crypto system, Karthik .S ,Muruganandam .A, ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014