# VMAIL / AN APPLICATION FOR A SECURE E-MAIL TRANSMISSION USING ENCRYPTING TECHNIQUES

**Ahmet SERTBAŞ[1] and M. Nusret SARISAKAL[2]**

[1,2]*Istanbul University, Faculty of Engineering, Department of Computer Engineering, 34850, Avcilar, Istanbul, Turkey*

[1] e-posta: asertbas@istanbul.edu.tr [2]e-mail: nsarisakal@istanbul.edu.tr

***Key Words:*** *Encryption, Decryption, Secure E-Mail, RSA and IDEA algorithms, Vmail*

## ABSTRACT

***In this paper, the secure e-mail transmission problem is studied by using the encrypting techniques which are called as IDEA and RSA algorithms. As a secure data application, plaintext and attachments encrypted by IDEA algorithm and the signatured cipher key by RSA algorithm are transmitted on internet. The recieved e-mail is decrypted by using firstly RSA algorithm for the signatured cipher key, then IDEA algorithm for the encrypted plaintext and attachment at the reciever side.***

## 1. INTRODUCTION

In recent years, the data security on internet has become the most important problem. To transmit and recieve the secure data, a lot of encrypting, key chipering and decrypting algorithms have been presented in the literature.

As an usual way, the cryptographic techniques are used to provide the data security on internet On the other hand, in the base of SSL protocol used on internet communication, there are the most effective two cryptographic algorithms, RSA and IDEA. In this study, we present an application called Vmail for a secure e-mail transmission by using together the RSA and IDEA algorithms.

## 2. The RSA ENCRYPTION ALGORITHM

In the cryptography, there are two systems which are called as private-key and public-key system. On the other hand, RSA encryption algorithm is known as a fundamental application of public-key crypting method. It was realized by Rivest, Shamir and Adleman in 1977. In a short time, it has started to use as a main algorithm in digital signature systems, crypting systems on internet communication, Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) Protocols.

As well known, the transmitted data on internet is not completely secure. So, using this algorithm, it can be realized the communication beetween the sender and the receiver in a secure media.

RSA is based on large prime numbers and modular arithmetic.

In RSA, Private and Public-Key pairs are produced as the following [2].

1. Generate two large and different primes as P and Q (for example 1024 bit)
2. Compute N = P*Q and Z=(P-1)*(Q-1)
   Here, N is called as modul.
3. Choose a random number E such that the common division with Z is 1.
4. Public-Key is produced as [E,N].
5. Compute D number from $D=E^{-1} \bmod Z$.
6. If it is not public-key,
   Private-Key is produced as [D,N].

**Encryption:**
Suppose M is the encrypted message, this message can be decomposed to the k bit parts such that $2^k < \mathbf{N}$. For the all parts, the following computation is applied.

$$C(i) = M(i)^E \bmod N \qquad (i=1,2....n)$$

**Decryption:**
Using the Private-Key [D,N], decryption process is done as the below:

$$M(i)=C(i)^D \bmod N \qquad (i=1,2....n)$$

On the other hand, in a digital signature scheme, it is not need to encrypte the entire message as general. Instead, a small signature block to be composed of the message itself is used. After the signature block is formed, the least change in e-mail can cause to the access of unwanted users. However, the digital signature can be verified using a publicly known verification algorithm. Thus, the use of secure signature scheme will prevent the possibility of forgeries.

In this study, RSA algorithm is used to signature the chiper key of IDEA algorithm as a secure scheme.

Some remarks deal with using RSA algorithm:

♦ The choose of the prime numbers effects the producing time of the key pairs directly. So, P and Q should be in nearest bit lenght with each other [3].

♦ The key lenght of RSA algorithm is selected by regarding the value of the protected data, the protection time and the type of attack. In practise, the key lenght is chosen between 512 bit and 2048 bit[4].

## 3. IDEA - INTERNATIONAL DATA ENCRYPTION ALGORITHM

IDEA was produced in 1991 by James Massey and Xuejia Lai of ETH Zurich in Switzerland. It is used to provide privacy by encrypting the data using a 128-bit key.

In IDEA crypting algorithm, the crypting methods are designed as the result of the mix of the different algebraic groups. Its crypting structure can be used in both software and hardware applications.

An IDEA cipher function has two inputs, the text and keys. The key length is 128-bit, which is divided into 8, 16-bit sub-blocks which then again is used (in the key schedule) to generate 52 key sub-blocks (of 16 bits each). The decryption key is composed by computation of these 56 key sub-blocks.

In the algorithm, each round tour uses 6 subkeys (16 bit), in last transformation only 4 subkeys are used, as total 52 subkeys. These 52 subkeys are generated from the original 128-bit key as shown in Fig.1.

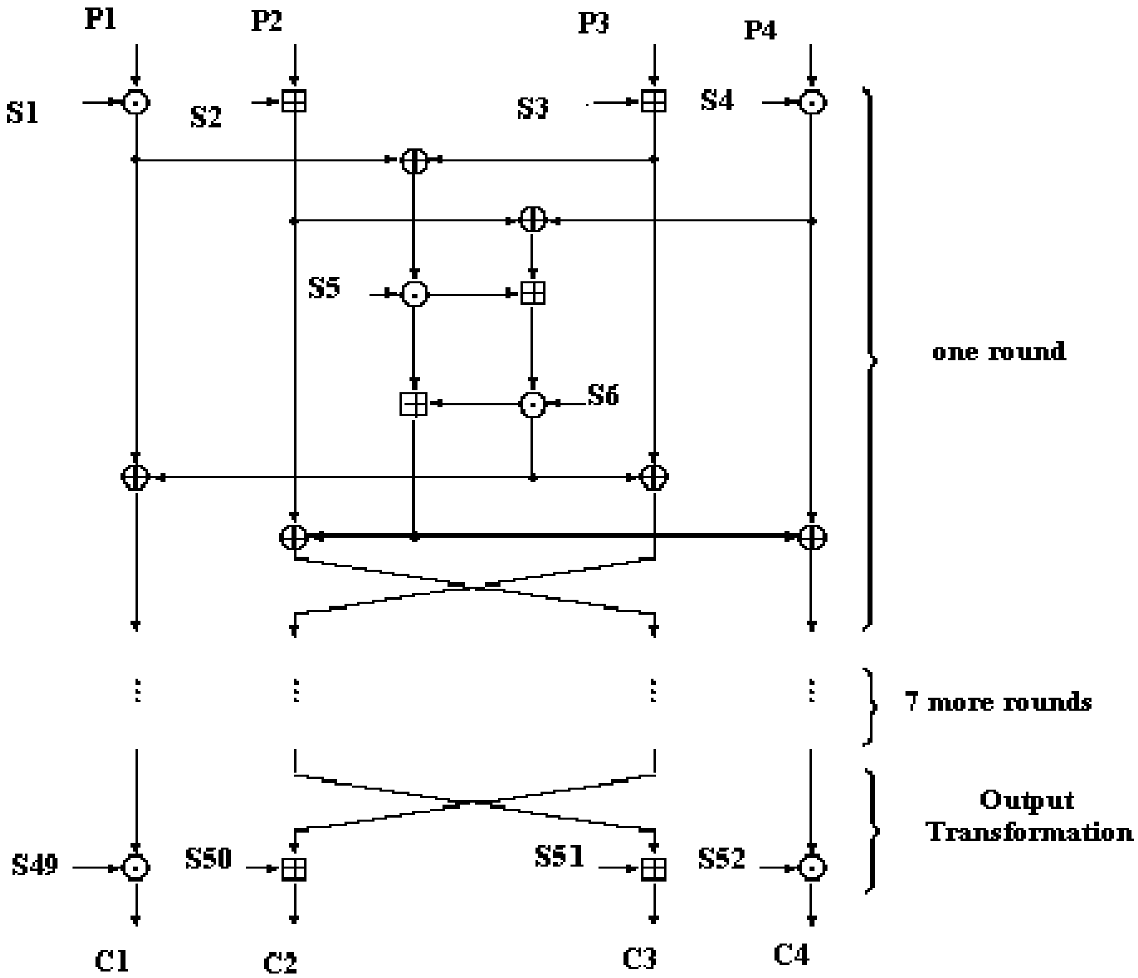


*Fig.1. IDEA Algorihtm*

**Encryption**

IDEA encrypting algorithm operates on 64 bit plaintext blocks. 64 bit input block is divided into four 16 bit blocks: X1, X2, X3, and X4 which become the input blocks to the first round of the algorithm. In each of the eight total rounds, the four sub-blocks are XORed, added, and multiplied with one another and with six 16 bit sub-blocks of key material.

We will not go into detail of the encryption and decryption process, only state that it is done during 16 rounds by doing three different group operations on pairs of 16-bit sub-blocks:

- bit-by-bit exclusive-OR of 16-bit sub-blocks; denoted as $\oplus$.
- addition of integers modulo $2^{16}$ where the 16-bit sub-block is treated as an unsigned integer; the resulting operation is denoted as $\boxplus$.
- multiplication of integers modulo $2^{16}+1$ where the 16-bit sub-block is treated as an unsigned integer except that the all-zero sub-block is treated as representing $2^{16}$; the resulting operation is denoted as $\odot$.

**Subkey generation**

The 128-bit key of IDEA is taken as the first eight subkeys, $S_1$ through $S_8$. The next eight subkeys are obtained in the same way, after a 25-bit circular left shift, and this process is repeated until all encryption subkeys are derived.

Consider that 64 bit plain-text is formed by 16 bit groups, represented by $P_1$, $P_2$, $P_3$ and $P_4$ respectively and the subkeys are sembolized as $S_1$, $S_2$, $S_3$, $S_4$, .... $S_{52}$ [6].

**Mathematical Represantation of The Encryption**

In Fig.1, the encryption consists of eight steps, the following process are realized in each step.

$P_1 \odot S_1$ --> $D_1$
$P_2 \boxplus S_2$ --> $D_2$
$P_3 \boxplus S_3$ --> $D_3$
$P_4 \odot S_4$ --> $D_4$
$D_1 \oplus D_3$ --> $D_5$
$D_2 \oplus D_4$ --> $D_6$
$D_5 \odot S_5$ --> $D_7$
$D_6 \boxplus D_7$ --> $D_8$
$D_8 \odot S_6$ --> $D_9$
$D_7 \boxplus D_9$ --> $D_{10}$
$D_1 \oplus D_9$ --> $D_{11}$
$D_3 \oplus D_9$ --> $D_{12}$
$D_2 \oplus D_{10}$ --> $D_{13}$
$D_4 \oplus D_{10}$ --> $D_{14}$

After this operation, $D_{12}$ and $D_{13}$ are changed with each other. Thus, $D_{11}$, $D_{13}$, $D_{12}$, $D_{14}$ are used as inputs for the next step. This procces is repeated for all steps in such that the output blocks $E_1$, $E_2$, $E_3$, $E_4$ are generated. After the steps in used the last four keys, the process is completed.

$E_1 \odot S_{49}$ --> $C_1$
$E_2 \boxplus S_{50}$ --> $C_2$
$E_3 \boxplus S_{51}$ --> $C_3$
$E_4 \odot S_{52}$ --> $C_4$

The last values $C_1$, $C_2$, $C_3$, $C_4$ are combined to produce 64-bit output block. The process continues until the all text are encrypted [7].

**Decryption**

How can the round in IDEA be reversed, since all four quarters of the block are changed at the same time, based on a function of all four of their old values. Well, the trick to that is that A xor C isn't changed when both A and C are XORed by the same value, that value cancels out, no matter what that value might be. And the same applies to B xor D. And since the values used are functions of (A xor C) and (B xor D), they are still available.

The decryption is the same with the encryption process. As similiar with encryption, in the decryption the ciphertext is used as input, but the subkeys are used differently. Decrypting subkeys $U_1$, ..$U_{52}$ are produced from the encrypting subkeys [6].

## 4. VMAIL - A SECURE E-MAIL APPLICATION

To show the efficiency of using together RSA and IDEA algorithms in the secure data transmission on internet, a new application, called Vmail is proposed.

Vmail system has an interface like MS Outlook Express. It uses the properties of Windows MAPI as the base. Well known that e-mail applications like Outlook Express, Netscape Mail and Eudora are supported by MAPI. In this application, incoming, saving and sending of e-mails are implemented by the available e-mail programming moduls supported MAPI.

After the available e-mail application is realized, V-mail program can be started.

**Encryption and E-mail Sending**

Having pressed the New Mail button, e-mail writing window is appeared shown in Fig.2. In this window, to whom the user send the e-mail, the header, text, attachments (if exit) and the encrypting method are selected.

The subject field is only the descriptive header, not contain the text data. Therefore it is send as decrypted. The message field comprises the main text of an e-mail, so it is sended as encrypted by IDEA algorithm with the attachments. By using the encryption alternative buttons, encryption parameters contain the encryption algorithms and cipher keys are selected.

In the sending process, firstly Vmail encrypts the text message and the attachments with respect to the chosen parameters, releases them onto MAPI. For the encryption, if only IDEA is used, the text and attachments is encrypted with the cipher key. But if also RSA together with IDEA are used in the encryption process as depicted in Fig.3, the cipher key used by IDEA is again encrypted with RSA, then the message text and attachments encrypted by IDEA and IDEA cipher key encrypted by RSA are transmitted to the reciever part.

### E-mail Receiving and Decryption

V-mail uses the same database with Outlook Express. It lists only the encrypted mails, when it is clicked on the listed mails, the text and attachments is decrypted with respect to the information on the header of the mail and appeared on screen as shown in Fig. 4.

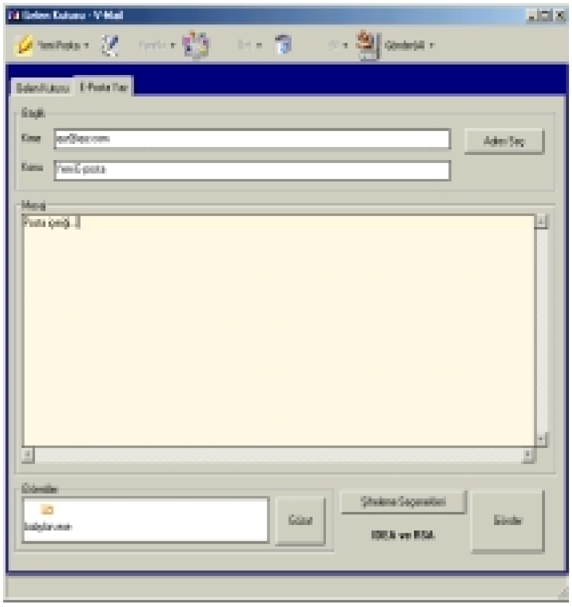

**Fig.2.** E-Mail, ready to send

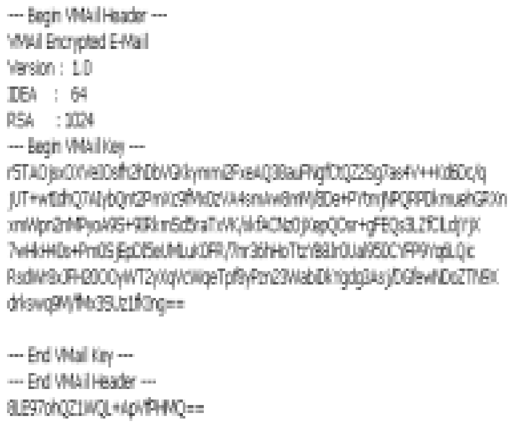


**Fig.3** E-Mail encrypted by RSA and IDEA

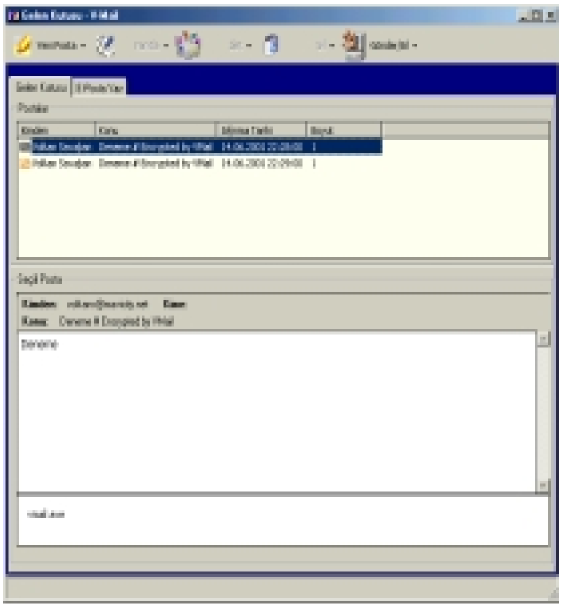

**Fig. 4** Decryption of the E-Mail

## 5. CONCLUSION

In this application, the fundamental reason for the using of IDEA is the highest security requirements along with easy software implementation. It permits effective protection of transmitted and stored data against unauthorized access by third parties.

In the previous paper, DES and SHA-1 message verification algorithms (TUGRA) were used for the secure e-mail application[8]. But, it is clearly seen that the performance of this application is better than the old method.

In IDEA, the used key lenght makes the decryption difficuilt. So, IDEA is more secure than DES algorithm. Also, IDEA utilizes a combination of 3 different operations that permits very complex inputs. This property causes to the crypto-analysis becomes more difficuit, compared with DES.

As a future work, transmitting the secure e-mail can be realized by using the encrption algorithms which have different cipher key lenghts and the combined algorithms.

## REFERENCES


1. Rivest R., Shamir A, Adleman L., 1978 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21,2 120-126.
2. Stinson D. R., Cryptography Theory and Practice, CRC Press, 1995, Florida
3. http://www.rsa.com
4. Ray Dillinger, “The RSA Algorithm”, Ağustos2000 http://www.sonic.net/~bear/rsa.htm
5. http://home.ecn.ab.ca/~jsavard/crypto/co0404.htm
6. http://www.momentus.com.br/PGP/doc/idea.html
7. William S., Network And Internetwork Security Principles And Practice, Prentice-Hall, Inc. 1995, New Jersey.
8. SARISAKAL M. N, KARAHOCA A, DES Algoritmasını Kullanan Güvenilir Bir E-Posta İletim Uygulaması: Tuğra, I.U. Engineering Faculty, Journal of Electrical & Electronics Vol. 1, No. 1, pp 23-31, 2001.