A Generaliztion of The RSA "Elatrash Scheme"

Dr. Fayik Ramadan EL-Naowk *

الملخص

تعتبر طريقة "آر إس إيه" في التشفير من الطرق الأكثر استخداماً. فـي هـذا البحث نقوم بتعميم هذه الطريقة من طريقة تستخدم الأعداد الصحيحة المحصورة بـين العددين صفر ،(ن- 1) حيث ن عبارة عن حاصل ضرب عددين أوليـين إلـى طريـق تستخدم حلقة المصفوفات المعرفة على حلقة البواقي للعدد ن و التي نـسميها "طريقـة الأطرش". ثم نعرض بعض ميزاتها

ABSTRACT

The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and (n – 1) for some n where n a product of two primes.

In this paper, we generalize RSA scheme in order to be applied to general linear group over the ring of integers modulo n and plaintexts and ciphertexts are k×k square matrices with entries in Zn (the integers modulo n) denoted by GL(k, Zn). We call it "Elatrash scheme".

Key words: RSA, Matrices, General linear group.

MSC2000 classifications: 14G50.

---

*Department of mathematics, Faculty of Science, Al-Aqsa University-Gaza, Palestine

Email: fayikrm@hotmail.com.

INTRODUCTION (Menezes and Vanstore 1996**)**

The pioneering paper in this work by Diffie and Hellman (Diffie and Hellman 1976) introduced a new approach to cryptography and challenged cryptologists to come up with cryptographic algorithm that met the requirements for public-key systems. One of the first responses to the challenge was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT publisled in 1978 (Rivest, Shamir and Adleman1978). The Rivest-Shamir-Adleman (RSA) scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n. In this short paper we take the plaintext and ciphertext from the general linear group of k×k matrices over Z_n, denoted GL(k, Z_n).

Amessage is a *plaintext* and denoted by m. The process of disguising a message in such a way as to hide its substance is *encryption*. An encrypted message is *ciphertext* denoted by c. A *key* is any thing needed to reveal the substance of the ciphertext.

The intractability of the RSA problem forms the basis for the security of the RSA public-key encryption scheme.

The RSA problem is the problem of finding an integer m such that $m^e \equiv c$ *(mod n) given a positive integer n which is a product of two distinct odd large primes p and q, a positive integer e such that gcd(e, n) = 1, and an integer c.*

In other words, the RSA problem is that of finding e^{th} *roots modulo a composite integer n. The conditions imposed on the problem's parameters n and e ensure that for each integer* $c \in \{0, 1, \ldots, n-1\}$ *there is exactly one m* $\in \{0, 1, \ldots, n-1\}$ *such that* $m^e \equiv c \pmod{n}$.

RSA cryptosystem is the most widely used public key cryptosystem. It may be used to provide both encryption and digital signatures.

The scheme developed by Rivest, Shamir, and Adleman (Rivest, Shamir and Adleman1978). Plaintext is encrypted in blocks, with each bolck having a value less than some number n. The Algorithm for key generation for RSA public-key encryption can be described such that each entity should do the following:

1. Generate two large random (and distinct) primes p and q, both roughly of the same size.
2. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3. Select a random integer e, $1 < e < n$, such that $gcd(e, n) = 1$.
4. Use the extended Euclidean algorithm to compute the unique integer d with, $1 < d < n$, such that $ed \equiv 1 \pmod{\phi(n)}$.
5. A's public-key is (n, e); A's private-key is (n, d).

The RSA Algorithm for public-key encryption can be summarized as follow:

Encryption: In order to make B encrypt a message m for A.
B should do the following:

(a) Obtain A's public-key (n, e).
(b) Represent the message as an integer m in the interval $[0, n-1]$.
(c) Compute $c = m^e \pmod{n}$.
(d) Send the ciphertext c to A.

Decryption. To recover the plaintext m from c and A ; calculate $m = c^d \pmod{n}$ using the private-key (n, d).

Example 1 (William 2003)

1. Select two different prime numbers, $p = 17$ and $q = 11$. (Note that both p and q must be large enough to beat the crackers. However we select them here small as an example).
2. Calculate $n = p \times q = 17 \times 11 = 187$.
3. Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to n (= 187) and less than n; we choose e to be 7.
5. Determine d such that $de \equiv 1 \pmod{160}$. The correct value is $d = 23$, because $23 \times 7 = 161$.

The resulting keys are public-key = $(n, e) = (187,7)$ and private-key are $(n, d) = (187, 23)$. Let the plaintext $m = 88$.
For encryption we need to calculate: c using step (c)

$$c = 88^7 \pmod{187}$$
$$= 40867559636992 \pmod{187} = 11.$$

For decryption we need to calculate m using $m = c^d \pmod{n}$

$$m = 11^{23} \pmod{187}.$$
$$= 895490243255237372246531 \pmod{187} = 88.$$

1. Main Results

We will generalize RSA scheme to a scheme that uses the general linear group (The group of invertible matrices) of square matrices of order k with entries taken from the ring of integers modulo *n* for *n* as a product of two large primes as in the case of RSA.

Integers relatively prime to *n* form a group under multiplication modulo *n* of order $\varphi(n)$.
Invertible square matrices of rank *k* over the ring of integers modulo *n* again form a group the order of this group is unknown in the general case, however, in the case *n* is a product of two primes we can calculate the order of this group as in the following theorem:

Theorem. *Let* $n = pq$ be the product of two prime numbers *p* and *q*, then let *G* be the general linear group of $k \times k$ matrices over Z_n. Then
$|G| = (p^k-1)(p^k-p)\ldots(p^k-p^{k-1})(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})$
Proof: Every matrix $m \in G$ reduced to two matrices m_p and m_q, where m_p and m_q are $k \times k$ matrices over the fields Z_p and Z_q where $m_p = m \pmod p$, $m_q = m \pmod q$. m is non singular iff both m_p and m_q are non singular. In fact the mapping:
$\xi : GL(k, pq) \rightarrow GL(k, p) \otimes GL(k, q)$
is a ring isomorphism of the two rings.
In order to see this, let m and n be two $k \times k$ matrices in GL(k, *pq*) then $\xi(m + n) = ((m + n)_p, (m + n)_q) = (m_p + n_p, m_q + n_q) = (m_p, m_q) + (n_p, n_q) = \xi(m) + \xi(n)$, this is clear since for every matrix entry $a + b \pmod s = a \pmod s + b \pmod s$, for any number s (= *p*, or *q*) therefore, ξ is an additive homomorphism.
$\xi(mn) = ((mn)_p, (mn)_q) = (m_p n_p, m_q n_q) = (m_p, m_q)(n_p, n_q) = \xi(m)\xi(n)$, again, this is clear since for every matrix entry $ab \pmod s = a \pmod s\ b \pmod s$, therefore, ξ is a multiplicative homomorphism.
ξ is one to one, since if $\xi(m) = \xi(n)$ then $(m_p, m_q) = (n_p, n_q)$ then $m_p = n_p$, $m_q = n_q$, it follows by chinese remainder theorem that $m = n$.
ξ is onto is clear. It follows that ξ is an isomorphism of the two rings.
From which it follows that the order of GL(k, *pq*) is the same as the order of the group $GL(k, p) \otimes GL(k, q)$. Since the order of the

groups are $|GL(k, p)| = (p^k - 1)(p^k - p)\ldots(p^k - p^{k-1})$, $GL(k, q) = (q^k - 1)(q^k - q)\ldots (q^k - q^{k-1})$.
Hence $|G| = (p^k-1)(p^k-p)\ldots(p^k-p^{k-1})(q^k-1)(q^k-q)\ldots (q^k-q^{k-1})$

The new scheme (Elatrash scheme)
Suppose that the user B wishs to send the message *m* to A. A should do the following:

1. Generate two large random (and distinct) primes *p* and *q*.
2. Compute $n = pq$ and |G|, G = GL(k, Z_n).
3. Select a random integer *e* such that $gcd(e, |G|) = 1$.
4. Compute the unique integer *d*, such that $ed = 1 \pmod{|G|}$.
5. A publishes his public-key (*n*, *k*, *e*);
6. A keeps his private-key (*n*, *k*, *d*) secret.

Encryption: In order to make B encrypt a message m to A, B should do the following:

(a) Obtain A's public-key (*n*, *k*, *e*).
(b) Represent the message as a non-singular *k* x *k* matrix *m*.
(c) Compute the $k \times k$ matrix $c = m^e \pmod n$.
(d) Send the ciphertext *c* to A.

Decryption: In order to make A recover the plaintext m from c,

A calculate $m = c^d \pmod n$ *using the private-key (n, k, d).*

Example 2
1. Select two prime number, $p = 3$ and $q = 5$.
2. Calculate $n = pq = 15$.
3. Calculate $|GL(2, Z_{15})| = (p^2-1)\ (p^2-p)\ (q^2-1)\ (q^2-q)$
$= 8\times6\times24\times20 = 23040$.
4. Select an integer *e* such that *e* is relatively prime to $|GL(2, Z_n)|$ (i.e., $gcd(e, 23040) = 1$); we choose $e = 7$.
5. Determine *d* such that $ed \equiv 1 \pmod{23040}$, the correct value is $d = 6583$.

The resulting keys are public-key $(n, k, e) = (15, 2, 7)$ and private-key $(n, k, d) = (15, 2, 6583)$, take the plaintext

$$m = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

For encryption, we need to calculate *c* from $c = m^e \pmod n$.

$$c = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}^{7} \pmod{15} \quad = \begin{pmatrix} 10 & 11 \\ 13 & 12 \end{pmatrix}.$$

For decryption, we need to calculate m from $m = c^d \ (mod\ n)$

$$m = \begin{pmatrix} 10 & 11 \\ 13 & 12 \end{pmatrix}^{6583} \pmod{15} \quad = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

Advantages and features of Elatrash scheme

1. One feature of Elatrash scheme is that its key space is large, it can be as large as we can by using matrices of higher ranks. The key space in the RSA is of size φ(n) = (p-1)(q-1), however, in this generalized scheme the key space is of size φ(|G|), for example in the previous example φ(15) = 8, while φ(23040) = 6144.
2. The hardness of the factorization of *n* remains the same.
3. We have used a k × k matrix *m* instead of an integer in the RSA, this is not a disadvantage.In fact, it is an advantage, since the RSA is a block cipher. We take k^2 blocks and set them in a matrix and calculate whatever needed, so it is more complex than one block to one block cipher.
4. Elatrash scheme supports digital signature. And digital signature can be embeded in the matrix as an entry
5. Also it can be composed with Hill cipher to get more complicated ciphertext.
6. It can be used as an RSA scheme where we use integers m and set them in k × k matrix as the left top entry, with 1 in the upper entry of the main diagonal, ones on the rest of the main diogonal and zeros in the remaining places, and still have the feature of having a larger key space than the RSA scheme.
7. For k = 1, it reduces to the RSA scheme.
8. Elatrash scheme can be used with a subgroup not only the full G = GL(k, *pq*). Since (*e*, |G|) = 1, then (*e*, |H|) = 1, for every subgroup H of G.
9. Matrices is more natural to use, since we can use it with a generating matrix for a code.

Aknowledgement I would like to thank my advisor professor Mohammed S. D. Elatrash for suggesting this scheme for me to study. In fact this is why I have named it after him as “Elatrash scheme”.

REFERENCES:

1- Diffie W. and Hellman M. (1976): Multiuser cryptographic techniques, IEEE Transactions on Information Theory.

2- Menezes A. and Vanstore S. (1996): Handbook of applied cryptography, CRC press.

3- Rivest R., Shamir A. and Adleman, L. (1978): A method for obtaining digital signatures and public-key crypto system, Communications of the ACM,.

4- William S. (2003): Gryptography and network security, Person Eduction, Inc.