Journal of the Nigerian Association of Mathematical Physics,
***Volume 8* (*November 2004*).**

An application of the extended RSA congruence

Henry Osaretin Omokaro
Department of Mathematics
University of Benin, Benin City.

Abstract

In [4], ***we proved that the RSA congruence could be extended to a situation where the modulus of the congruence is a simple product of primes. In this work, we discuss the cryptosystem of this extended RSA congruence as an analogue of the RSA cryptosystem, which is hereafter referred to as the Extended RSA Cryptosystem.***

pp 341 - 343

1.0 Introduction

A cryptosystem is a means whereby information is sent in such a way that only the person(s) the message is meant for understands it. To protect the message from being understood by unauthorized persons, some security measures are taken. Such security measure varies from one cryptosystem to another. There are several examples of cryptosystems. One of them is the one developed by Rivest, Shamir and Adleman in [1]. It is often called *RSA cryptosystem* named after the first letters of the developers. Its security is based on the *RSA congruence*. This is possible because of the difficulty involve in factorising larger positive integers as product of prime numbers. These factorised large numbers are then used as the modulus of the congruence.

In a cryptosystem, the *plaintext* is the message being sent. The plaintext has to be put in a form in which only the person it is meant for understands it. This process is called e*nciphering* or *encoding*. The enciphered message is called a *ciphertext* or an *encoded message*. In encoding the message, we make use of the *enciphering key,* S_k. The message is later translated by the receiver to a form that is understandable by everyone. This process is called *deciphering* or *decoding*. In deciphering a message, we make use of a *decoding key*, P_k. In the RSA cryptosystem, the keys S_k and P_k are obtained by solving a congruence modulo Euler-phi function of a product of 2 primes. The encoding and decoding are obtained by raising the numeric equivalent of the message to the power of the key, modulo the product of the two primes from which the keys are obtained as an application of the RSA congruence.

2.0 RSA congruence illustration

As an illustration of the RSA congruence application in the RSA cyptosystem, let us assume that our enciphering and deciphering keys S_k and P_k are given by $S_k = e$ and $P_k = d$ respectively. Let our modulus n be given by $n = pq$ where p and q are prime numbers from which e and d are calculated. Let m be the numerical equivalent of the message. The ciphertext EM is then obtained from the plaintext by applying $E(P) = C = P^e \ mod \ n$ (3). Since $(e, \phi(n)) = 1$ the inverse d of e modulo $\phi(m)$ exist. Therefore the palintext is decoded from the cipher text by applying $D(C) = c^d = (p^e)^d = p^{ed=} p^{k\phi(n)+1} \equiv (p^{\phi(n)})^k p \equiv p$ mode n where $ed = k\phi(n) + 1$ for some integer k because $ed \equiv 1 \bmod \phi(n)$. By Euler theorem, we have $p^{\phi(n)} \equiv 1$ mod n when $(p, n) = 1$, (the probability that p and n are not relatively prime is extremely small the pair (e, n) is a deciphering key [1, 2].

It is interesting to note that once one of the factors p, q of n is known, $\phi(n)$ can be obtained and hence, the private key can be determined and the code broken. In suing the RSA congruence, the keys e and d must satisfy the congruence $ed \equiv$ mod $(p - 1)(q - 1)$ so that knowing p say q can be determined and e can be found, since d, the public key is known. Since in Omokaro [4], it has been proved to be true when n is a simple product of k – primes say $n = P_1 P_2 \ldots P_k$. The extended RSA congruence now gives us a wider class of large numbers n to choose from as the modulus of our congruence, which is expressed as a simple product of 3 or more very large primes.

3.0 The extended RSA cryptosystem

Now we obtain the *extended RSA cryptosystem*. As the name implies in the extended RSA cryptosystem, we obtain our deciphering key, applying the *extended RSA congruence* as follows. In the extended RSA cryptosystem to obtain the plaintext from the ciphertext, we consider

$$D(C)=C^{d}=(p^{e})^{d}=p^{ed}=p^{k\phi(n)+1}\equiv(p^{\phi(n)})^{k}\cdot p=p^{k(p_1-1)(p_2-1)\cdots(p_k-1)}\cdot p=1\cdot p \ mod \ \ p_i \ 1\le i\le r$$

which gives $D(C) = m$ mod $p_1p_2\ldots p_r$ Omokaro [4]

4.0 Example

Le L be the set of English alphabets and symbols in the order in which they are listed below:

$$L=\{a,b,c,d,\ldots,z,+,x,\div,\alpha,\beta,\gamma,\eta,\varphi,\psi,\theta,\phi,\pi,@,/,\#,*,\%,\exists,\sum,\geq,\leq,$$
$$=-,?,\theta_1,\theta_2,\theta_2,\theta_4,\theta_5,\theta_6,\theta_7,\theta_8,\theta_9,\theta_{10},\theta_{11},\theta_{12},\theta_{13},\theta_{14},\theta_{15}\}$$

We assign numbers to the elements of L as follows:

$$a\to 01,b\to 02,\ c\to 3,d\to 04,\ldots,z\to 26,+\to 27,x\to 28,\div\to 29,\alpha\to 30,\beta\to 31,\gamma\to 32,$$
$$\eta\to 33,\ldots,\theta_{12},\to 62,\theta_{13},\to 63,\theta_{14},\to 64,\theta_{15},\to 65.$$

Let us take our modulus n to be 66.

Now $\phi(n)$ is given by

$$\phi(n)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \text{ where } n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$$

is the representation of n as a product of prime numbers [3].

So that $\phi(66)=66\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)=66x\frac{1}{2}x\frac{2}{3}x\frac{10}{11}=20$

Let $e=3, then\ (e,\phi(n))=(3,20)=1$ since d satisfies $ed\equiv 1 \ mod \ \phi(n)$, we have that d satisfies $3x\equiv 1 \ \ mod \ \ 20$ i.e., $3x=20k+1$ for some integer, k. This gives x = 7. So d = 7 satisfies $ed\equiv 1 \ \ mod \ \ \phi(n)$ and is unique. As an illustration, let us code the sentence “Cigarette smoking.” First we consider the numeric equivalents of the alphabets of each word that make up the sentence” Cigarette”.

$$c\to 03,\ i\to 09,g\to 07,a\to 01,r\to 18,e\to 05,t\to 20.$$

We then solve the following congruences for each of the alphabets of cigarette as follows:

- C: $(03)^3$ mod 66 = 27 mod 66 = 27
- i: $(09)^3$ mod 66 = $(09)^2\cdot 09$ mod 66 = 15 x 9 = 3
- g: $(07)^3$ mod 66 = $(07)^2\cdot 07$ mod 66 = 13
- a: $(01)^3$ mod 66 = 01
- r: $(18)^3$ mod 66 = $18^2\cdot 18$ mod 66 = $6\cdot 18$ mod 66 = 42
- e: $(05)^3$ mod 66 = 59 mod 66 = 59
- t: $(20)^3$ mod 66 = $20^2\cdot 20$ mod 66 = $4\cdot 20$ mod 66 = 14

We can then go on and identify the alphabets corresponding to these solutions of the solved moduli:

$$C:27\to +,i:3\to C,g:13\to m,a:1\to a,r:42\to *,e:59\to\theta 9,t:14\to n.$$

We then encipher the word cigarette as $+cma*\theta_9 nn\theta_9$. For “smoking “ we follow similar steps:

$$S\to 19,m\to 13,\ 0\to 15,k\to 11,i\to 09,n\to 14,g\to 07$$

- s: 19^3 mod 66 = $19^2\cdot 19$ mod 66 = $31\cdot 19$ mod 66 = 61
- m: 13^3 mod 66 = $13^2\cdot 13$ mod 66 = $37\cdot 13$ mod 66 = 19
- o: 15^3 mod 66 = $15^2\cdot 15$ mod 66 = $27\cdot 15$ mod 66 = 9
- k: 11^3 mod 66 = $11^2\cdot 11$ mod 66 = 11 mod 66 = 11
- i: 09^3 mod 66 = $09^2\cdot 09$ mod 66 = $15\cdot 9$ mod 66 = 3
- n: 14^3 mod 66 = $14^2\cdot 14$ mod 66 = $64\cdot 14$ mod 66 = 38
- g: 07^3 mod 66 = 13

So that $s:61\to\theta_{11},m:19\to s,\ o:9\to i,k:11\to k,i:3\to c,n:38\to\pi,g:13\to m.$ we can now enclode “smoking as $"\theta_{11}sikc\pi m"$. To decipher we consider”

$$+:\to 27,c\to 03,m\to 13,a\to 01,*\to 44,\theta_9\to 61,n\to 14,\theta_9\to 61$$

So that

1. $+:27^7\ mod\ 66=27^2\cdot 27^2\cdot 27^2\cdot 27\ mod\ 66=3\cdot 3\cdot 3\cdot 27\ mod\ 66=\cdot 27^2\ mod\ \ 66=3\ mod\ 66=3,\ 03\to C$

2. $c:03^7\ mod\ 66=03^2\cdot 03^2\cdot 03^2\cdot 03\ mod\ \ 66=9\cdot 9\cdot 9\cdot 03\ mod\ \ 66=81\cdot 27\ mod\ \ 66=15\cdot 27\ mod\ 66=9$

$mod\ 66 = 9,\ \ 9 \to i$

3. $m : m \to 13\ \ 13^7\ mod\ 66 = 13^2 \cdot 13^2 \cdot 13^2 \cdot 13\ mod\ 66 = 37 \cdot 37 \cdot 37 \cdot 13\ mod\ 66 = \cdot 49 \cdot 19\ mod\ \ 66 = 7,\ 7 \to g$

4. $a \to 1,\ 1^7\ mod\ \ 66 = 1,\ 1 \to a$

5. $* \to 42\ \ 42^7\ mod\ 66 = 42^2 \cdot 42^2 \cdot 42^2 \cdot 42\ mod\ 66 = 48 \cdot 48 \cdot 48 \cdot 42\ mod\ 66 = \cdot 60 \cdot 36\ mod\ \ 66$

$= 50x36\ mod\ 66 = 18,\ 18 \to r$

6. $\theta_9 \to 59,\ \ 59^7\ mod\ 66 = 59^2 \cdot 59^2 \cdot 59^2 \cdot 59\ mod\ 66 = 49 \cdot 49 \cdot 49 \cdot 59 mpd\ 66 = \cdot 25 \cdot 53\ mod\ \ 66 = 5,\ 5 \to e$

7. $n \to 14\ \ 14^7\ mod\ 66 = 14^2 \cdot 14^2 \cdot 14^2 \cdot 14\ mod\ 66 = 64 \cdot 64 \cdot 64 \cdot 14 = 64 \cdot 64 \cdot 38\ mod\ 66$

$= \cdot 4 \cdot 38\ mod\ \ 66 = 20,\ 20 \to t$

We can now decipher $"+cma*\theta_9 nn\theta_9"$ as "Cigarette " which is the word we enciphered at the beginning, which is an example of the use of this congruence as an analogue of the RSA congruence.

5.0 Conclusion

The snag in using the RSA congruence in the RSA cryptosystem is that only positive integers that can be expressed as product of two primes can be used as modulus. But the extended RSA congruence allows us to use any positive integer that can be expressed as a simple product of *k* primes where *k* is any positive integer, thereby given the extended RSA cryptosystem a wider class of integers to be used as modulus and hence improving the security.

References

[1] Rivest, R. L. Shamir, A. Adleman L "A Method for Obtaining Digital Signature and Public Key Cryptosystem ." Communications of ACM Vol. 21 (1978 pp. 120 – 126

[2] Collett, Stacy "Global Term Cracks Crypto Challenge." Computer World Online New, September 28, 1999.

[3] Rosen, K. H. Elementary Number Theory and its Applications, Addison-Wesley Publishing Company. New York (1992).

[4] Omokaro, H. O. A generalization of the RSA congruence Journal Nigeria Association Mathematics Physics Vo. 7, pp 27, 2003