© 2014 IJSRSET | Volume i | Issue i | ISSN: 2394-4099
Themed Section: Engineering and Technology

Variant of RSA – Multi prime RSA

Vaishali Kalaria[1], Bhavesh Kataria[2]
[1]Department of Computer Engineering and Information Technology, RK University, Rajkot
[2]Department of Computer Engineering, LDRP Institute of Technology and Research, Gandhinagar

ABSTRACT

Variant of RSA – Multi prime RSA that is backwards compatible that is a system using multi prime RSA can interoperate with systems using standard RSA and this variant is used to speed up RSA decryption.

Keywords
RSA, Modulo arithmetic, prime numbers, CRT, ECM

I. INTRODUCTION

Multi-prime RSA is a generalization of the standard RSA cryptosystem in which the modulus contains more than two primes. When decryption operations are done modulo each prime and then combined using the Chinese Remainder Theorem, the cost of decryption is reduced with each additional prime added to the modulus (for a fixed modulus size). Thus, multi-prime RSA might be a practical alternative to RSA when decryption costs need to be lowered.

The benefit of multi-prime RSA is lower computational cost for the decryption and signature primitives, provided that the CRT (Chinese Remainder Theorem) is used. Better performance can be achieved on single processor platforms, but to a greater extent on multiprocessor platforms, where the modular exponentiations involved can be done in parallel.

The security of these variants is an open problem. We cannot show that an attack on any of these variants would imply an attack on the standardized version of RSA (as described, e.g., in ANSI X9.31). Therefore, when using these variants, one can only rely on the fact that so far none of them has been shown to be weak. In other words, Use at your own risk.

II. METHODS AND MATERIAL

Fast Variant of RSA

Multi prime RSA: N= pqr. It is referred in PKCS#1v2.0.

Key generation:

The key generation algorithm takes as input a security parameter n and an additional parameter b. It generates an RSA public/private keypair as follows:

Step 1: Generate b distinct primes $p_{1,}\ldots,p_b$ each $\llcorner n/b]$ bits long. Set $N \leftarrow \prod^{b}_{i=1} p_{i.}$ For a 1024 bit modulus, b=3 at most.

Step 2: Pick the same e used in standard RSA public keys. Then compute $d=e^{-1} \bmod \Phi(N)$. e is relatively prime to $\Phi(N)= \prod^{b}_{i=1} (p_i-1)$. The public key is (N,e), the private key is d.

Encryption:

Given a public key (N,e), the encrypter encrypts exactly as in standard RSA.

Decryption:

Decryption is done using the Chinese Remainder Theorem (CRT). Let $r_i=d \bmod p_i-1$. To decrypt a ciphertext C, one first computes $M_i=C^{ri} \bmod p_i$ for each i, i<=i<=b. One then combines the M_i's using the CRT to obtain $M=c^d \bmod N$. The CRT step takes negligible time compared to the b exponentiations.

Performance:

Standard RSA decryption using CRT requires two full exponentiations modulo n/2 bit numbers. In multi prime RSA decryption requires b full exponentiations modulo n/b bit numbers. Using basic algorithms computing x^d mod p takes time $O(\log d \log^2 p)$. When d is on the order of p the running time is $O(\log^3 p)$. Therefore the asymptotic speed up of multi-prime RSA over standard RSA is:

$$2.(n/2)^3 / b.(n/b)^3 = b^2/4$$

For 1024 bit RSA, b=3 at most is used, which gives a theoretical speedup of 2.25 over standard RSA decryption.

Security:

The security of multi factor RSA depends on the difficulty of factoring integers of the form N= $p_1 \dots p_b$ for b>2. The fastest known factoring algorithm (the number field sieve) cannot take advantage of this special structure of N. Prime factors of N should not fall within the range of the Elliptical Curve Method (ECM). Currently, 256 bit prime factors are considered within the bounds of ECM, since the work to find such factors is within range of the work needed for the RSA-512 factoring project. For 1024 bit moduli, more than three factors should not be used.

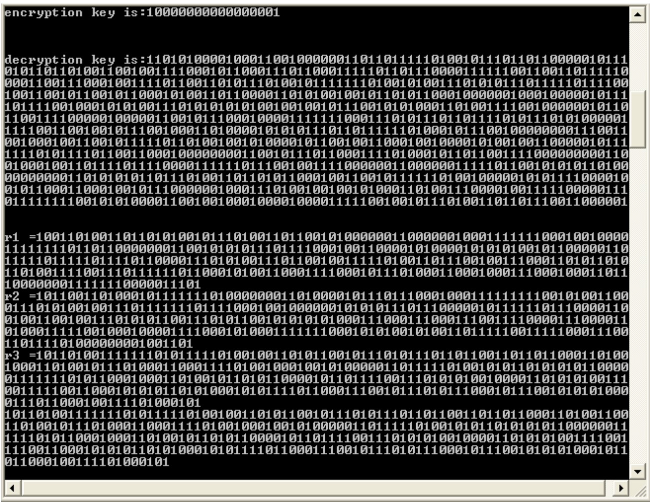
In this paper we survey four simple variants of RSA that are designed to speed up RSA decryption in software. Throughout the paper we focus on a 1024-bit RSA modulus. We emphasize backwards compatibility: A system using one of these variants for fast RSA decryption should be able to interoperate with systems that are built for standard RSA; moreover, existing Certificate Authorities must be able to respond to a certificate request for a variant-RSA public key.

The security of these variants is an open problem. We cannot show that an attack on any of these variants would imply an attack on the standardized version of RSA (as described, e.g., in ANSI X9.31). Therefore, when using these variants, one can only rely on the fact that so far none of them has been shown to be weak. In other words, Use at your own risk.

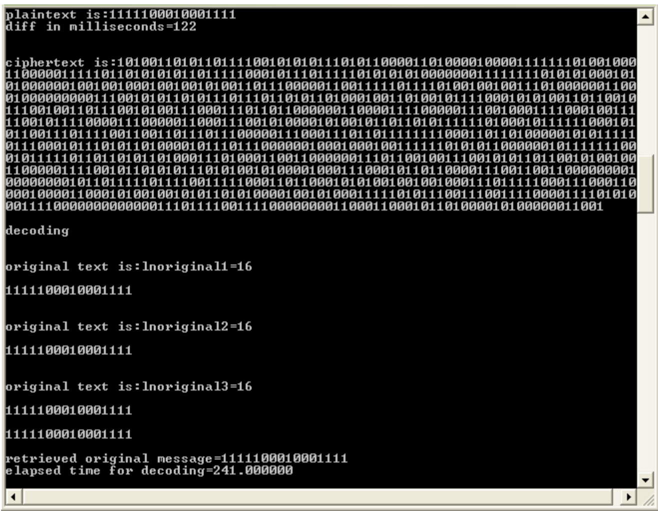
III. RESULT AND DISCUSSION

A. Prime Numbers of Length 341 is generated

B. Decryption key is generated of length equal to the length of prime number



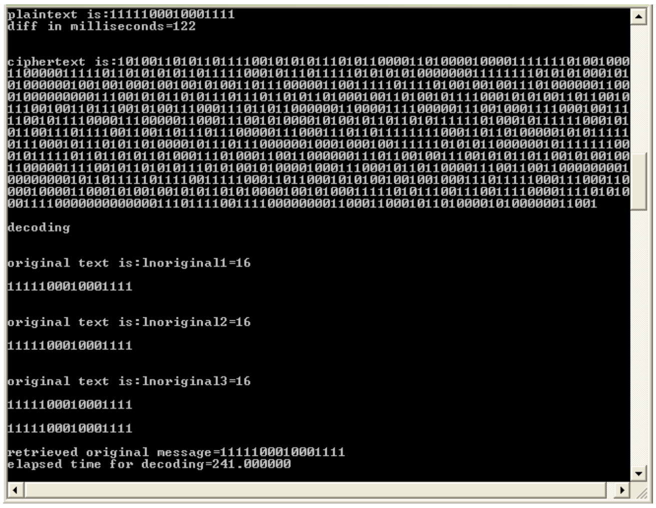
C. Cipher Text Generation



D. Time Analysis Of Basic Rsa And Multi Prime Rsa

1. Basic RSA

2. Multiprime RSA



IV. CONCLUSION

Variant of RSA multi prime RSA gives theoretical speedup of approximately 2.25 over standard RSA decryption. In this implementation slower algorithms are used to implement basic RSA so speed up with multi prime RSA is 3.73 could be achieved over basic RSA

V. REFERENCES

[1] RSA Labs. Public Key Cryptography Standards (PKCS)

[2] 2. Fast Variants of RSA By Dan Boneh and Hovav Shacham

[3] 3. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack By Ranald Cramer and Victor Shoup

[4] 4. Evaluation of Security Level of Cryptography : RSA-OAEP,RSA-PSS, RSA Signature By Alfred Menezes

[5] 5. Network and Internetwork security By William Stallings.

[6] 6. R. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public Key Cryptosystems.”

[7] 7. M. Wiener. “Cryptanalysis of Short RSA Secret Exponents.” IEEE Trans. Information Theory 36(3):553–558. May 1990.Zd

[8] 8. A. Fiat. “Batch RSA.” In G. Brassard, ed., Proceedings of Crypto 1989, vol. 435 of LNCS, pp. 175–185. Springer-Verlag, Aug. 1989.