RSA: The Mathematical Approach

Neeraj Jindal[1] Aditi Sharma[2] Vaishali Agrawal[3]
Assistant Professor ECE Assistant Professor CSE B.Tech(CSE)

Chartered Institute Of Technology, AbuRoad Rajasthan
Email: er.neerajjindal@yahoo.com, aditi1_sharma@yahoo.com, vaishaliagr1790@gmail.com,

***Abstract*—RSA is an important cryptographic technology that is widely used to provide secure transmission of data. It's an application of number theory which uses principles of abstract algebra and modular arithmetic to encrypt and decrypt messages. RSA is named after Rivest, Shamir and Adleman, the individuals who first published the technique. It is very simple to multiply numbers together, especially with computers. But it can be very difficult to factor numbers. RSA was the first algorithm known to be suitable for signing as well as encryption and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. The security of RSA lies under its large keys size because factoring is a hard problem for prime numbers. The security of relies on the fact it is difficult to factor sufficiently large numbers. No polynomial-time method for factoring large integers on a classical computer has been found yet. However, it has not been proven that none exists. As of November 8, 2005, the largest number factored by general purpose methods was 640 bits long (known as the RSA-640 number) which was a 193 digit number. This factorization was done on 80 CPU's working together and took approximately four and a half months, total. The prize that the German BSI team received for factoring this number was $20,000. Because of the different methods of factorization that are being used with the help of linked computers super-computers, the current recommendation for the product of primes, N, is for it to be is at least 2048 bits long. However, if quantum computing reaches a sufficient level, as it is predicted to be no earlier than 2015, it potentially can perform factorization in polynomial time, rendering RSA and related algorithms obsolete.**

I. INTRODUCTION

Number Theory is one of the oldest branches of pure mathematics. Due to its mathematical functionality it's being used in computer security. The sensitive data may be protected by using its applications. In 1970s the most important research of number theory was made in the era of web-based computer security. There must be secure transmission of sensitive data between sender and receiver over network from the unauthorized access. To accomplish this purpose the data is encrypted before sending and while

receiving it the decryption is made at receiver end. Keys had to be distributed over the network for all users for encryption and decryption of sensitive data which requires secure communication channel. Keys had to be protected from the theft. In Public Key Infrastructure the keys for encryption and decryption are different and the decryption key could not feasibly be derived from the encryption key. The decryption key should only be known by authorized parties.
Cryptosystems are made up of three basic parts: the encryption algorithm, the decryption algorithm, and the key(s). The encryption algorithm is the algorithm used to encode an original, or a plaintext message. The decryption algorithm is the reverse process of the encryption algorithm. With the decryption algorithm, the user converts the encoded message back to its original plaintext message. The key system is used during the process of encrypting and decrypting messages. Generally, an encryption key is used to encrypt messages, whereas a decryption key is used decrypt messages.

RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT [1]; the letters **RSA** are the initials of their surnames : - the three cryptographers who invented the first practical commercial public key cryptosystem. RSA provides secure communications over distances between parties that have not previously met, RSA provides the ideal mechanism required for private communications over electronic networks, and forms the basis of almost all of the security products, now in use on the Internet for financial and other private communications, including most organizational level Public Key Infrastructure (PKI) systems.

II. ASPECTS OF NUMBER THEORY USED IN RSA

Three basic approaches in number theory prepare the way for today's RSA public-key cryptosystem.

To find a random prime number of a given size is easy. It means that prime numbers of any size are very common, and it's easy to test whether a number is a prime – even a large prime. Multiplication of two numbers is easy [2]: Given a and b, it's easy to find their product, $n = ab$. Factoring a number is hard: Given such an n, it appears to be quite hard to recover the prime factors a and b. Modular exponentiation is easy: Given n, m, and e, it's easy to compute $c = m^e \bmod$

n[2]. The reverse of modular exponentiation is easy: Given the prime factors: Given *n*, *e*, *c*, and the prime factors *a* and *b*, it's easy to recover the value *m* such that $c = m^e \bmod n$. Its hard to do modular root extraction: Given only *n*, *e*, and *c*, but not the prime factors, it appears to be quite hard to recover the value *m*.

III. The RSA Cryptosystem

A. Algorithm

The key generation of public key/private key of RSA cryptosystem can be shown in the following steps:

1. A pair of large, random primes *a* and *b* must be taken first.
2. Then calculate the modulus *n* as $n = ab$.
3. Choose an odd public exponent *e* between 3 and *n*-1 that is relatively prime to *a*-1 and *b*-1.
4. Calculate the private exponent *d* from *e*, *a* and *b*. The generated output *(n, e)* is used as the public key and *(n, d)* is used as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the e^{th} power modulo *n*:

$c = \text{ENCRYPT}(m) = m^e \bmod n$ [2].

m is the *message* which is input sending to receiver; *c* is the resulting *cipher text* i.e. output which will be received at receiver end .

The decryption operation is exponentiation to the d^{th} power modulo *n*:

$m = \text{DECRYPT}(c) = c^d \bmod n$[2] .

The relationship between the exponents *e* and *d* ensures that encryption and decryption are inverses, so that the decryption operation recovers the original message *m*. Without the private key *(n,d)* (or equivalently the prime factors *a* and *b*), it's difficult to recover *m* from *c*.

B. Key Generation

Choose two large primes randomly:	*a, b*
Calculate the modulus:	$n = a.\ b$
Calculate Eulers Phi function:	$\phi(n) = (a-1).(b-1)$
Randomly choose *d* with:	$\gcd(d, \phi(n)) = 1$
Calculate the inverse *e* of *d*:	$e = [d]^{-1} \bmod \phi(n)$[3]
Public Key:	*(d, n)*
Private Key:	*(e,n)*

C. Encryption-Decryption

Let be *r* the hash value to encrypt:

Encryption:	$c = r^e \bmod n$
Decryption:	$c = r^d \bmod n$

IV. Theorems on which RSA cryptosystem is based

A. Chinese Remainder Theorem:

Let p and q be integers, not necessarily prime, such that they are coprime. If $a \equiv b \pmod{p}$ *and* $a \equiv b \pmod{q}$ *then we have* $a \equiv b \pmod{pq}$.

B. Fermat's Little Theorem:

If p is a prime number and a a natural number, then

$$a^p \equiv a \pmod{p}.$$

Furthermore, if $p \nmid a$ (p does not divide a), then there exists some smallest exponent d such that

$$a^d - 1 \equiv 0 \pmod{p}$$

and d divides $p - 1$. Hence,

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

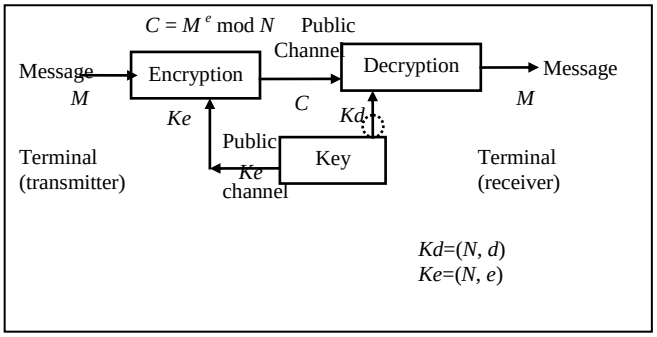
For any integer a and any prime number p, $a^p \equiv a \pmod{p}$. *If a and p are coprime, then* $a^{p-1} \equiv 1 \pmod{p}$, *or, equivalently,* $p \mid (a^{p-1} - 1)$.

C. Fermat-Euler Theorem or Euler's Generalization of Fermat's Little Theorem:

For any number *a* coprime to *n*, we have $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is Euler's phi function

V. RSA Operation

Processing block diagram:-



VI. RSA Digital Signature

The sender signs the document *G* using the private key *(d,m)* as follows:

$S = G^d \bmod m$

The recipient verifies the authenticity of the document *G* using the sender's public key *(e, m)* as follows:

$$G = S^e \bmod m$$

VII. Results And Discussions

A. Modular Arithmetic

RSA uses modular arithmetic. This is similar to conventional arithmetic, but only uses positive integers that are less than a chosen value, called the modulus. The notation used for expressions involving modular arithmetic is:

$$x = y \ (mod\ m)$$

B. Primality and Coprimality

A number is prime if the only numbers that exactly divide it are 1 and itself. A pair of numbers is coprime if the largest number that exactly divides both of them is 1.Its easy to multiply two large prime numbers. But factoring of resultant is too hard. RSA uses the concept of Primality and coprimality.

C. Fermat–Euler theorem or Euler's Totient Theorem

if n and k are coprime positive integers, then

$$k^{\varphi(n)} \equiv 1 (\bmod n)$$

where $\varphi(n)$ is Euler's totient function and "... ≡ ... (mod n)" denotes congruence modulo n. To calculate the value of private key e the concept of Fermat –Euler is used.

VIII. Conclusions

RSA algorithm is very robust and most secure with compare of other cryptographic algorithms due to its computational difficulty of factoring large numbers. The prime numbers ‘a’ and ‘b’ must be taken roughly of same size to prevent elliptic curve factoring. The difference of ‘a’ and ‘b’ should be large enough for preventing them from attack.

RSA provides for message “signing” which entails the sender producing a hash value of the message to be sent, raising that value to the power of d mod N (as done when decrypting), and attaching it as a “signature” to the message. When the receiver gets the signed message, he raises the signature to the power of e mod N (as done when encrypting), and compares the resulting hash value with the message’s actual hash value, making sure they agree, therefore verifying the signature.

RSA can be freely implemented because there are no intellectual property claims any more. RSA algorithm is used in hardware and the signature verification efficiently in compare of other public key cryptography.

RSA encryption is a deterministic encryption algorithm. For transmitting data in a secure way over the internet, RSA is mostly used algorithm for encryption and decryption. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. Today is no known algorithm is developed which can solve the factorization of the no which is created by two large prime numbers of roughly the same size in the reasonable time. In RSA users can easily increase the key size which gives the RSA as protection. Almost all of the security products now in use on the Internet for financial and other private communications, including most organizational level Public Key Infrastructure (PKI) system use the ideal mechanism provided by RSA.

IX. References

[1] R.L. Rivest, A. Shamir,and L. Adleman “A Method For Obtaining Digital Signatures And Public-Key Crypto Systems”

[2] Burt Kaliski, “The Mathematics of the RSA Public-Key Cryptosystem”

[3] Ralf Baier “Internet Security:The use of RSA within ESP and AH” 2004-06-24