A Hybrid Crypto System based on a new Circle-Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications

Rasmi P S
Asst. Professor
Toc H Institute Of Science Technology

Dr. Varghese Paul
Dean CSE/IT/Research
Toc H Institute Of Science and Technology

ABSTRACT
It is widely recognized and accepted that data security will play a crucial and critical role in modern times for businesses will be transacted over the Internet through e-commerce and m-commerce channels. To address these security concerns, various security protocols that are of symmetric-key and asymmetric-key type have been developed. In this paper, we present a hybrid cryptographic system that combines both the symmetric key algorithm, which uses the properties of a circle and asymmetric-key algorithm of RSA with CRT. The circle symmetric key algorithm is based on 2-d geometry using property of circle, and circle-centered angle. It is a block cipher technique but has the advantage of producing fixed size encrypted messages all cases. The asymmetric algorithm is RSA with CRT which improves the performance of the basic RSA algorithm by four.

Keywords: Cryptography, Encryption, Decryption, hybrid cryptography, Symmetric Key Algorithms.

1. INTRODUCTION
The Internet today is a truly global market place, with a wide variety of goods and services available online. Secure communication is an intrinsic requirement for many popular online transactions such as e-commerce, stock trading and e-banking. E-commerce and m-commerce transactions are growing at an explosive rate. The success of these depends on how transactions are carried out in the most secured manner. The prime requirements for any e-commerce and m-commerce transactions are Privacy, Authentication, Integrity maintenance and Non-Repudiation. Cryptography helps us in achieving these prime requirements. Today, various cryptographic algorithms have been developed. These are broadly classified as symmetric key (DES, TDES, Blowfish, CAST, IDEA,RC4, RC6, AES) and asymmetric key (RSA, ECC) algorithms[1]. In this paper, we present a hybrid crypto system based on circle symmetric algorithm and RSA with CRT algorithm for e-commerce application.

Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric key (also called "secret-key") encryption, the same key is used for both encryption and decryption. In asymmetric (also called "public-key") encryption, one key is used for encryption and another for decryption [1]. Hybrid cryptography combines both of these encryption methods. The organization of this paper is as follows. In setion2 we explain the basics of hybrid crypto system. in section 3 we present the circle symmetric key algorithm. In section 4 we present the RSA with RT algorithm. The proposed hybrid system is described in section 5. we concluded the paper saying the advantages of the algorithms.

2. HYBRID CRYPTOGRAPHY
A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to its best advantage. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message [2]. In our paper we present a new circle symmetric algorithm to encrypt the plain text and an asymmetric algorithm RSA with CRT is used to encrypt the symmetric key

Figure 1. Block diagram of Hybrid crypto system

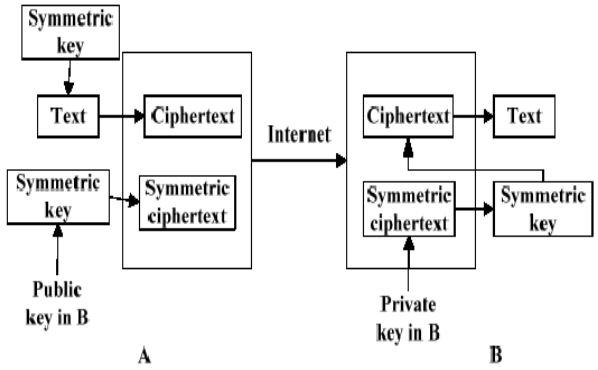


Fig 1 shows the block diagram of a hybrid crypto system which takes the advantages of both shared secret and public key algorithms. That means it combines both the symmetric key algorithm and asymmetric-key algorithm to take the advantage of the higher speed of symmetric ciphers and the ability of asymmetric ciphers to securely exchange keys

3. THE CIRLE SYMMETRIC KEY ALGORITHM
Our cryptographic scheme is inspired by Elliptic Curve Cryptography (ECC) [3]. This has been made computationally efficient by reducing the order of equation from cubic to

quadratic. The idea of ECC evolves around a cubic curve. Here, a circle is the basis of all computation. Also, ECC is based on congruency relation for large prime numbers. Here, planar geometric computation in 2D [4] coordinates is performed and all points on a circle are considered. So, computations are in real value domains rather than integer domains.

This algorithm is a shared Symmetric Key algorithm. The communicating parties may initiate the communication with ECC having their own public and private key. Then they would compute their shared key which will be used as the symmetric key for this algorithm. Thus, finding out the shared symmetric key is a discrete logarithmic problem [5] which means it is as hard as breaking the security of ECC. This algorithm requires a pair of geometric points as the shared symmetric key. The first point is the center O of the circle.

The second point is shared secret point S lying on the perimeter of the circle. It is proposed that both these keys should be exchanged by ECC. It should also be mentioned that, the radius r of the circle is,

$$r^2 = (Sx - Cx)^2 + (Sy - Cy)^2$$

Else, C, SX and r can be transmitted as shared symmetric key. Then, SY will be the unknown quantity of the above equation and can be easily computed.

This algorithm can encrypt/ decrypt as many message symbols as its diameter. If the length of the diameter is the largest integer of n bits (2n) then it can successfully encrypt/decrypt2n distinct message symbols.

First the message point is randomized and the representation of the randomized message point is determined on the circle. Then, the circle-centered angle that is obtained by traversing along the perimeter of the circle from the secret point to the message point in the counter-clockwise direction represents the encrypted value. Note that the encryption process is pretty simple and it can be performed in constant time irrespective of the number of the bits in the message symbol.

The encrypted message is the circle-centered angle and it is transmitted through the network. Note that, this is a floating point value. This value is always less or equal to 2π. So, a custom floating point architecture can be employed for this purpose where more bits can be used after the decimal point for greater precision.

Upon receiving the encrypted message, the receiving entity decrypts the message by traversing along the circle's perimeter from the secret point by an angle equal to the encrypted message.

Encryption:
Input: M, a 64 bit value
Output: E, a 32 bit value
Interpretation: [byte0-1] Circle-centered angle between
Input and Secret Point
[byte2-3] A random value (k); [0<(1/k)<=1]

1. Transpose Y-axis to CX
   $X' = X - CX$
2. Generate a 8 bit random value k
3. Let, MX = M*(1/k)

Find MY1 and M¬Y2, such that (MX, MY1)≡M1 and (MX,MY2) ≡M2 is on the Circle

4. Let, Secret Point, S=(SX,SY)

Find <SCM1=α1 and <SCM2= α2

5. Let α=min(α1, α2)

Output: E= < α, k >
Decryption:
Input: E, a 32 bit value
Output: M, a 64 bit value
Interpretation: [byte0-1] Circle-centered angle between Input and Secret Point
[byte2-3] A random value (k); [0<(1/k)<=1]
1. Let, Secret Point, S≡ (SX, SY)
Find point M′≡(MX′,MY′) such that <SCM′=α.
2. Let, M = MX′*k + CX
3. M=round (M)
4. Output: M

One of the main aspects of this symmetric key cryptographic algorithm is its simplicity in computing the encrypted and decrypted values.

3.1 Security Analysis

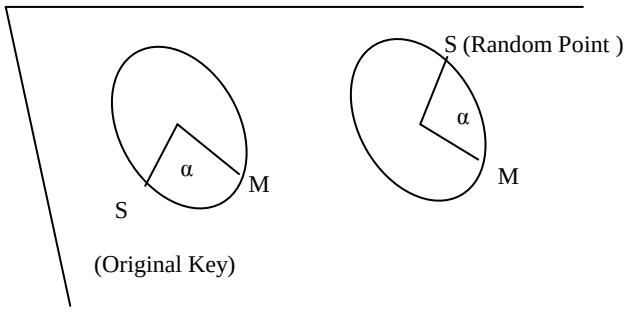
Here the co-ordinates(x and y co-ordinate) of the center are two 32 bit integers, radius is also a 32 bit unsigned integer. Only the x co-ordinate of the secret point is needed here. As radius is known, the y co-ordinate can be computed subsequently. Thus the symmetric key is formed.

To analyze the security and secrecy of the algorithm, different dimensions of attacks which can be attempted to break the secrecy can be considered.

Cipher text-only attack: In this type of attacks, the intruder has only the cipher text (the angle between symmetric key and message point) [6]. For this type of attack, our algorithm depends on the geometric property that same angle can be generated between infinite number of points situated on the circle perimeter see figure). Besides this algorithm is a block cipher protocol instead of stream cipher protocol and randomization is also employed so that statistical analysis of the cipher text does not reveal anything of the actual message

Suppose,
r=radius of the circle, then the perimeter of the circle=$2\pi r$

Figure 2: Invariance of the Secret Key and a Random Point given the Encryption Angle



Now, in practice the no of points on the circle, N= $2\pi r \times P$, where P=a constant depending on the floating point precision used. (For 10 bit floating point precision, P= 210)Now r can be

any of the 232bit quantities Secret
point can be any of the N points and Center point of the circle can be any of the 264 quantities (considering both the x and y co-ordinate.

Message point can also be any of the N points of the circle So, the probability that an intruder (in cipher text only attack) can correctly assume the actual message or Secret Key by intercepting only the encrypted angle is:

$1/(N2 \times 296)$

For even moderate values of the floating point parameter P , this probability tends to zero. So, as per as cipher text only attack this algorithm is fairly unbreakable[8].

Known-plaintext attack: In this type of attacks, the intruder intercepts the cipher text and can guess or know the actual plaintext which was transmitted [7]. So, the intruder has the angle between the secret point and message point as well as the message point. The intruder does not know the circle center and radius of the circle as well as the secret point. So, here r can be any of the 232bit quantities. Secret point can be any of the N points [described previously] and Center point of the circle can be any of the 264quantities (considering both the x and y co-ordinate. So, probability for an intruder in this attack to correctly assume the secret key is same as cipher text-only attack.

3.2 Limitations

The algorithm has several limitations despite the promise it holds. These are described below:

- This algorithm performs several floating point operations which demands sufficient amount of precision from the sender and receiver processor. Reliability of the algorithm thus invariably depends on the precision provided.

- Floating point calculation and round off operation limits the size of the block to encode. In practical simulation it worked perfectly for 32 bit block size. But increasing the block size may subject to round off error.

- This algorithm will be more appropriate for software implementation whereas hardware implementation can be quite tedious and tricky - which contrasts to traditional symmetric key algorithms.

4. RSA WITH CRT ASYMMETRIC ALGORITHM

In 1982 J.J Quisquater and C. Couvreur[9] introduced a new technique to increase the speed of decryption algorithm of RSA crypto system. In this technique two smaller secret keys (dp,dq) are calculated from the original secret key(d),decryption is done with these two keys and the result is combined with the help of Chinese Remainder Theorem(CRT).It improves the performance of the basic RSA decryption algorithm by 4.

4.1 Key Generation of RSA with CRT

It is almost same as in basic RSA

1. Choose two distinct prime numbers p and q. For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2. Compute n = pq. n is used as the modulus for both the public and private keys

3. Compute $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.

4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$ (i.e., e and $\varphi(n)$ are co prime). Determine $d = e^{-1} \pmod{\varphi(n)}$. (i.e., d is the multiplicative inverse of $e \pmod{\varphi(n)}$).

5. Determine $d = e^{-1} \pmod{\varphi(n)}$. (i.e., d is the multiplicative inverse of $e \pmod{\varphi(n)}$).

This is often computed using the extended Euclidean algorithm[10]

4.2 Encryption of RSA with CRT

- Same as in basic RSA
- Sender A does the following:-
- Obtains the recipient B's public key(n,e).
- Represents the plain text message as a positive integer M
- Computes the cipher text = Me mod n
- Send the cipher text to B

4.3 Decryption of RSA with CRT

- Calculate dp=d mod p-1 and dq=d mod q-1
- Mp=Cdp(mod p)
- Mq=Cdq (mod q)
- Calculate M from Mp & Mq using Chinese remainder Theorem

4.4 Chinese Remainder Theorem

For efficiency many popular crypto libraries (like OpenSSL, Java and .NET) use the following optimization for decryption and signing: The following values are pre computed and stored as part of the private key[11]:

- p and q: the primes from the key generation,
- dp= d mod (p-1)
- dq= d mod (q-1) and
- qinv=q-1 mod (p)

. These values allow to compute the exponentiation m= cd mod pq more efficiently computed as follows:

- $Mp = c^{dp} \bmod p$
- $Mq = c^{dq} \bmod q$
- h= qinv * (Mp-Mq) mod p

(if m1 < m2 then some libraries compute h as qinv * (Mp+p-Mq) mod p

M = Mq+hq

This is more efficient than computing M= Cd (mod pq) even though two modular exponentiations have to be computed. The reason is that these two modular exponentiations both use a smaller exponent and a smaller modulus[12]

4.5 Performance of RSA with CRT

Theoretial speed up of this method with relation to the original RSA is

$SRSA= (n^3)/2(n/2)^3 =4$

5. THE PROPOSED HYBRID CRYPTO SYSTEM

The proposed Hybrid System combines both the symmetric key algorithm, which uses the properties of a circle and asymmetric-key algorithm of RSA with CRT. The circle symmetric key algorithm is based on 2-d geometry using properties of circle, and circle-centered angle. The two algorithms are described in the previous section

5.1 The use of proposed system for E-com Application

E-Commerce involves the business between an individual and an organization. The block diagram in fig depicts the total process of an example e-com application. The customer has to visit the website of the travel agency or a broker and get the status of the availability of tickets. If ticket is available he/she will book the ticket and input the credit card details. He/She will be given the details of delivery of ticket[13].

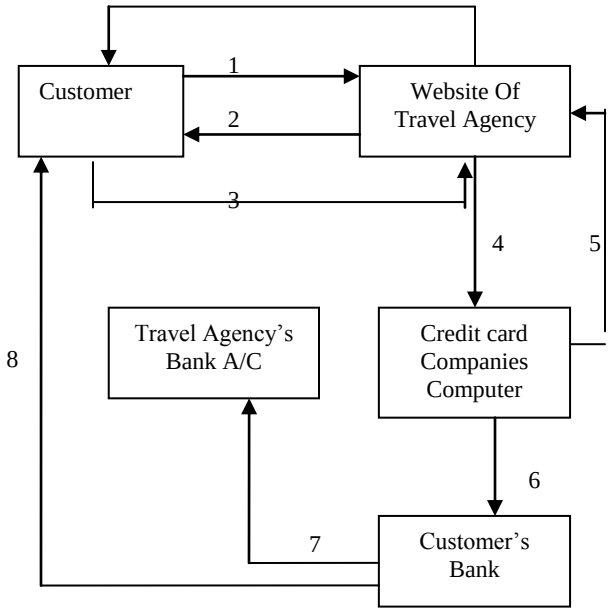


Fig.3 Total process of e-com application

1.Request Service

2.Display Informations on various flights

3.Places order with credit card details

4. Credit card details

5. Credit card OK

6.Debit advice giving credit card Details

7.Credit to travel Agency's A/C

8.Bill to customer

During the transmission of sensitive information like credit card details through the internet, intruders collect and use private information against the person. The intruders generally look for bank account information, credit card details, and other sensitive passwords. The intruders by stealing the information use it to purchase goods and services, while the owner will ignorant of such happenings until the bank or the credit card agency intimates of such crimes. By then it will late and the owner will end up paying a hefty price. So in recent years more and more attention has been directed at the need for increased data security and encryption plays a crucial role in protecting our information, and most notably in securing our on-line purchases from attack. In our system before sending the sensitive information, they are encrypted using the proposed hybrid cryptographic algorithm and in the receiver the encrypted text is decrypted. Fig 4 and fig 5 shows the how the sensitive information is encrypted and decrypted at the sender and the receiver respectively

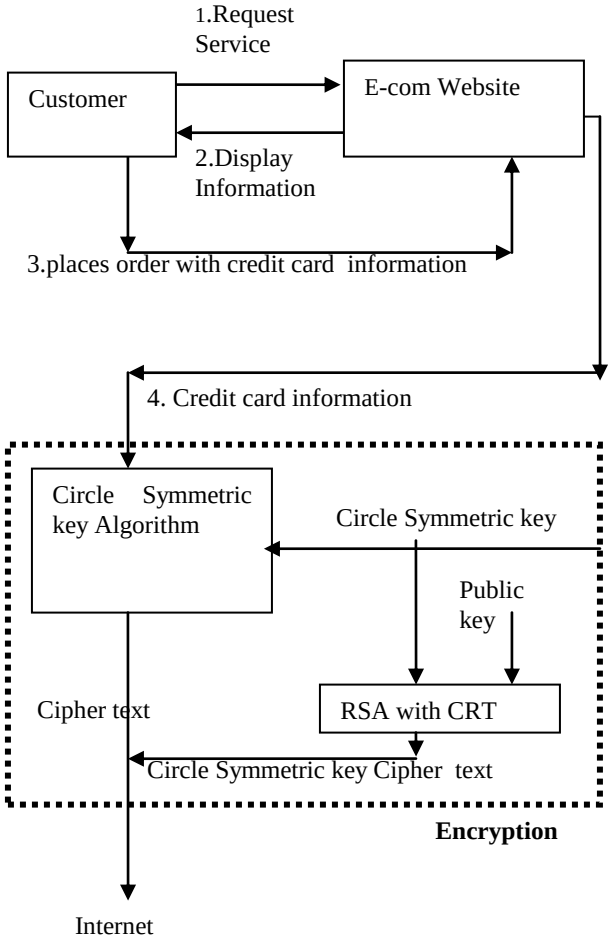


Fig 4 Encryption in sender side

At the sender side the credit card information given by the customer is encrypted using circle symmetric algorithm and the circle symmetric key is encrypted using RSA with CRT algorithm.

This encrypted key is also sent along with cipher text. At the receiving end the circle symmetric key is extracted using RSA with CRT algorithm and with that key and circle symmetric key algorithm the encrypted credit card information is decrypted.

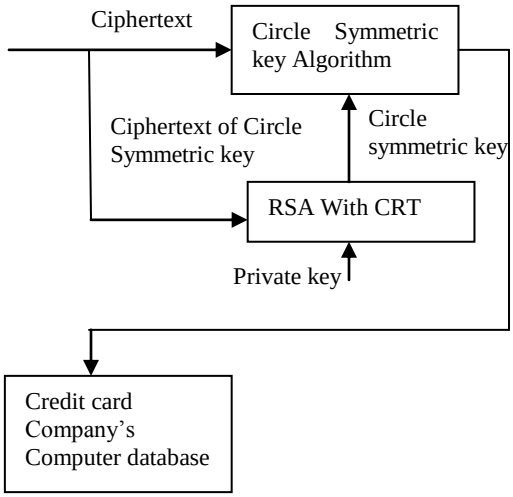


Fig 5 decryption in the receiving end

6. CONCLUSION

The symmetric algorithm used here requires very low computational power and encryption/decryption for input of any length and key size takes constant time. Planar geometric calculations have been used and it has greatly reduced the complexity compare to other symmetric key algorithm. The asymmetric algorithm used here is RSA with RT which enhances the speed of decryption compare to basic RSA algorithm.

7. REFERENCES

[1] William Stallings "Cryptography and Network Security",3rd Edition, Prentice-Hall Inc., 2005.

[2] Janakiraman V S, Ganesan R, Gobi M "Hybrid Cryptographic Algorithm for Robust Network Security" ICGST- CNIR, Volume (7), Issue (I), July 2007

[3] Elliptic curve cryptography http://en.wikipedia.org/wiki/Elliptic Curve Cryptography

[4] Dus and Gupta, Planar geometry (2nd edition)

[5] The Discrete Logarithm Problem (http: //www.cs.toronto.edu/~cvs/dlog/)

[6] Cipher text-Only Attack, http://www.javvin.com/networksecurity/CiphertextOnlyAttack.html)

[7] Known-plaintext attack (http://www.tech- faq.com/known-plaintext-attack.shtml)

[8] "A New Symmetric Key Encryption Algorithm based on 2d geometry"-2009 International Conference on Electronic Computer Technology.

[9] JJ Quisquarter and Couvreur." Fast decipherment Algorithm for RSA public key crypto system", electronic Letters Vol435, 1989

[10] [10] RSA (http://en.wikipedia.org/wiki/chinese RSA.htm)

[11] [11] RSA (http://en.wikipedia.org/wiki/chinese Remainder.htm

[12] Deepak Garg, Seema Verma "Improvement over public Key cryptographic Algorithm" 2009 IEEE International Advance computing conference

[13] Jinbiao Hou "Research on Database Security of E-Commerce Based on Hybrid Encryption" 2009 International Symposium on Web Information Systems and Applications

Biographies

Dr. Varghese Paul has got more than 30 years of professional experience - in industry, utilities and academic institutions. Currently he is working as Dean (CS IT / Research), TIST. Earlier he was Head of Information Technology in CUSAT, SCADA Engineer in Electricity Department in Kingdom of Saudi Arabia, Communication Engineer in KSEB and Industrial Engineer in OEN India Ltd. Kochi. He is a B Tech. degree holder in Electrical Engineering, M Tech. in Electronics and Ph D. in Computer Science. He is a Certified Software Test Manager, Ministry of IT, Govt. of India. His Research area is Fault Tolerant Computing and Data Security. He had developed a special type of coding system, TDMRC Code, which has widespread application in data security. He has many research publications to his credit and presented technical papers in many national and international seminars. He has authored a text book also.

Mrs. Rasmi PS is Asst. Professor, dept of Information Technology in Toc H Institute of Science & Technology. She teaches courses for BTeh in Information Technology. At present she is pursuing her PhD programme in computer Science & engg.