CRT based Secured Encryption Scheme

Subba Rao Y V
Department of CIS
University of Hyderabad
Hyderabad, India
yvsrcs@uohyd.ernet.in

Chakravarthy Bhagvati
Department of CIS
University of Hyderabad
Hyderabad, India
chakcs@uohyd.ernet.in

Abstract: **This paper presents a simple but novel Cryptography system that is based on Chinese remainder theorem. This scheme is the one that uses little or limited computation power for encryption and much lesser requirements for decryption. Also space requirements will not add any more cost as many other systems. Also it is secure for use as good alternate encryption system to deal with multiple secrets and users.**

Keywords: Chinese remainder theorem; Multiple secrets; Secured encryption;

I. INTRODUCTION

All Security and bandwidth are two important parameters of communication. But in any application scenario, these two become a trade of for each other, that is, increase in security needs more bandwidth and any attempt on bandwidth optimization shall not give any security. In this paper we made an attempt to achieve a balance of these two parameters. Cryptography is an ancient art/science of sending information secretly, such that only intended recipient can gain access to it. Starting from age old classical systems such as shift cipher system, hill cipher system etc., it had grown to modern secured systems such as RSA, AES, ElGammel, ECC etc.. In this evolution process various useful techniques such as secret sharing schemes, zero knowledge proofs, digital signature schemes etc. where introduced and used by people who work with cryptography or security. Among many mathematical topics which are very crucial in all these schemes and techniques, Chinese remainder theorem (CRT) is an important topic. One simple application of CRT in cryptography is to reduce the high exponentiation cost in RSA decryption process [1]. Later CRT was used by many for implementing/improving efficiency of various algorithms mainly by splitting or sharing encrypted information into smaller units and thus increase the security of those algorithms. [7] gives details about usage of CRT in computing, coding and cryptography. [8] explains about the security of the threshold scheme based on the Chinese Remainder Theorem. But, later many new results were presented using CRT. For instance [6] proposed a verifiable secret sharing scheme and later [5] proposed a verifiable threshold secret sharing scheme to decrease the size of shares without compromising on the security. But then [2] demonstrated that schemes in [6] and [5] can by attacked to have inconsistent shares and proposed a scheme to deal with consistent shares.[3] first gives robust threshold function sharing scheme for the RSA cryptosystem and then applies the ideas to the ElGamal and Paillier decryption functions.

In all these and many other applications, CRT plays a good supporting role to provide/enhance security/efficiency. In this paper we made an attempt to use it as an encryption tool. Section 2 here presents a brief explanation of CRT, section 3 explains the proposed scheme and section 4 gives security analysis of the proposed scheme along with some possible lines of improvement as future work.

II. CHINESE REMAINDER THEOREM

Chinese remainder theorem assures existence of solution for system of congruence relations (unique modulo some M). For a given system of congruencies as

$$x = a_1 \, Mod(m_1)$$

$$x = a_2 \, Mod(m_2)$$

$$\vdots$$

$$x = a_k \, Mod(m_k).$$

for some positive integer k, with only condition that this m_i 's are pair wise co-prime.. Then from the proof of CRT, as given in many Number theory/Cryptography books such as [1], we can define some variables as

$$M = m_1 * m_2 * \ldots\ldots m_k \quad (1)$$

$$M_i = M/M_i \quad (2)$$

$$y_i = M^{-1}{}_i \, Mod(m_i). \quad (3)$$

Now the unique solution mod (M) is

$$x = (\sum^{k}{}_{i=1} a_i * M_i * y_i) Mod(M). \quad (4)$$

This construction gives a unique x (Modulo M) that can satisfy the given system of congruencies.

1) Example

Consider the System of congruencies as

$$x = 1 Mod(97)$$

$$x = 2 Mod(99)$$

$$x = 1 Mod(101).$$

978-1-4577-0697-4/12/$26.00 ©2012 IEEE

Here we have

$$a_1 = 1,\ a_2 = 2,\ a_3 = 1$$

and

$$m_1 = 97,\ m_2 = 99,\ m_3 = 101.$$

Now from CRT we can see the following values

$$M = m_1 * m_2 * m_3 = 97 * 99 * 101 = 969903$$

and

$$M_1 = M/m_1 = 9999$$

$$M_2 = M/m_2 = 9797$$

$$M_3 = M/m_3 = 9603$$

Now we can compute the inverses as

$$y_1 = 9999^{-1} = 85 Mod(97)$$

$$y_2 = 9797^{-1} = 74 Mod(99)$$

$$y_3 = 9603^{-1} = 38 Mod(101)$$

From the expression

$$x = a_1 * M_1 * y_1 + a_2 * M_2 * y_2 + a_3 * M_3 * y_3,$$

we have

$$x = 849915 + 1449956 + 364914 = 2664785.$$

Considering $Mod(M)$, we have $x = 724979$. For this value of x, we can easily see that

$$x = 1 Mod(97) = 2 Mod(99) = 1 Mod(101).$$

III. CRT CRYTOSCHEME

A. Phase I:

This is set-up phase. Consider the environment for the proposed scheme with a single dealer/administrator D and a set of n users $U_1, U_2, \ldots, U_n$. Let D choose n pair wise co-prime numbers (positive integers) $m_1, m_2, \ldots, m_n$. Each m_i is privately communicated to user U_i (this can be done with help of public key systems such as RSA or ElGammel or ECC etc). At the end of this, each user U_i will be having m_i, which the user can use as a key for decrypting the cipher received from dealer D.

B. Phase II:

This is encryption phase, where the dealer D, possesses data $a_1, a_2, \ldots, a_n$, with each a_i is from the ring Z_{mi} .Here, for $i = 1, 2, \ldots n$, each a_i is intended to be sent only for user U_i, but not for others. Dealer shall first compute x using CRT, such that x satisfies set of congruencies $x = a_i Mod(m_i)$, for $i = 1, 2, \ldots n$. From CRT we know that, this x is unique upto $Mod(M)$, where M is the product of all m_i's. Then this x is communicated to all users.

C. Phase III:

This is decryption phase, where each user U_i after receiving x, using his key m_i, shall compute a_i as $xMod(m_i)$. For others who have no knowledge of m_i will not be able to know, what the a_i is, as shown in next section.

1) Example

Here dealer first chooses 3 pair wise co-prime number as 97, 99, 101 (we are using same values as in last example), then secretly communicates $m_1 = 97$ to U_1, $m_2 = 99$ to U_2 and $m_3 = 101$ to U_3 in set-up phase. Assume that secrets for U_1, U_2 and U_3 are $a_1 = 1$, $a_2 = 2$ and $a_3 = 1$ respectively, then dealer will have same system of congruence (as in our earlier example)

$$x = 1\ Mod(97)$$

$$x = 2\ Mod(99)$$

$$x = 1\ Mod(101)$$

Thus dealer can use CRT to solve for x and hence will have $x = 724979$, which he shall just broadcast to all. Now user U_1, with his knowledge of $m_1 = 97$ can compute

$a_1 = 1 = 724979 Mod(97)$

Similarly, U_2 and U_3 can also read their respective secrets.

	Dealer – D	Users U1, U2, … Un
Set-up	Choose m1, m2, … mn such that they are pairwise co-prime. Send each mi to user Ui secretly	 Ui receves mi
Encryption	Let secret for Ui be ai from the space Zi. Consider the system of congruences as x=aiMod(mi) for i= 1,2, … n Broadcast x	 Users can receive x
Decryption		Each Ui can read his secret as ai=xMod(mi)

Figure 1. Proposed Architecture

IV. Analysis of the Scheme

Security of this scheme can be proved by showing that even with the knowledge of $n-1$ pairs of (a_i,m_i), for $i = 1, 2, \ldots n-1$ and the cipher x, it is not possible to guess what the a_n is, without the knowledge of m_n. For this, we shall show that for many choices of a_n, m_n can be computed to satisfy the requirement $x = a_n \; Mod(m_n)$. Let us start with some arbitrary value for a_n say α, then consider the variables defined as,

$$y = x - \alpha$$

$$M_1^{\,n} = m_1 * m_2 * \ldots * m_{n-1}$$

$$d = gcd(y, M_1^{\,n})$$

$$\beta = (y/d).$$

From this computation, if β> α, we can consider β as m_n and this will serve our requirement as seen from the above equations. If $\beta \leq \alpha$, we can start again with a new choice of a_n. This proves the randomness of a_n, as desired. Apart from security, we are also interested in economic use of space for efficient communication. In our scheme each a_i is from space Z_{mi} and needs $log_2(m_i)$ bits of space and the encrypted message x is from space Z_M which is approximately sum of all $log_2(m_i)$s. Thus there is no real increase in size as in many other encryption systems.

Computation requirements are also quite limited as seen from scheme and for decryption it just computes a mod operation.

In spite of all these positive aspects there are few limitations to this scheme. First and important one is, if the values of m_i's are very small (say 8 bits to handle ASCII) and if the same m_i's are used to encrypt a sequence of characters, then in the event of having knowledge of $n-1$ m_i's, can lead to an attack where one can try with all possible m_n's, until one sees a meaningful decryption of characters. To overcome this limitation we recommend use of m_i's of minimum 100 bits in size, so that above brute force type of attack becomes infeasible.

The second limitation is, if the same secret is to be transmitted to all, this encryption scheme will not mask the secret. This is demonstrated in the example bellow.

1) Example

Here we continue with same m_i's, that is 97, 99, 101 for U_1, U_2 and U_3 respectively.

Assume that secrets for U_1, U_2 and U_3 is same and it is

$$a_1 = a_2 = a_3 = 2,$$

then dealer will have new system of congruencies

$$x = 2 Mod(97)$$

$$x = 2 Mod(99)$$

$$x = 2 Mod(101)$$

From the expression

$$x = a_1 * M_1 * y_1 + a_2 * M_2 * y_2 + a_3 * M_3 * y_3,$$

we now have

$$x = 1699830 + 1449956 + 729828 = 3879614.$$

Considering $Mod(M)$, we have $x = 2$. We need not be surprised of this, as this is only unique value modulo 969903 to satisfy our system, we stated working with, in this example. This is always true whenever the secret is same for all users.

Few simple tricks can save us in such nasty situation. First alternate is to send 969905 that is $M + 2$. Second alternate is to add some kind of padding for at least one user. Third alternate is to add a dummy user with a different secret and some new m_{n+1} as key parameter.

V. Conclusions

The above given scheme is a simple but secured and efficient scheme as proved in analysis section. Future work can look on lines of obtaining some compression of data to make a real and very useful scheme.

Acknowledgment

The authors would like to thank Ms Rukma Rekha, Ms Anupama and Dr, S Durga Bhavani for their support and help.

References

[1] D. R. Stinson, Cryptography Theory and Practice, 3rd ed. Chapman and Hall/CRC, 2006.

[2] Kamer Kaya and Ali Aydin Selcuk, A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem, INDOCRYPT 2008, LNCS 5365, pp. 414-425, 2008.

[3] Kamer Kaya and Ali Aydin Selcuk, Robust Threshold Schemes Based on the Chinese Remainder Theorem, AFRICACRYPT 2008, LNCS, pp. 94-108, 2008.

[4] Ron Steinfeld, Josef Pieprzyk and Huaxiong Wang, Lattice- Based Threshold Changeability for Standard Shamir Secret- Sharing Schemes, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 53, NO. 7, pp.2542-2559, JULY 2007.

[5] Iftene S, Secret sharing schemes with applications in security protocols, Technical report, University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science (2007).

[6] Qiong L, Zhifang W, Xiamu N and Shenghe S, A noninteractive modular veriable secret sharing scheme, ICCCAS 2005: International Conference on Communications, Circuits and Systems, pp. 8487. IEEE, Los Alamitos (2005).

[7] Ding C, Pei D and Salomaa A, Chinese Remainder Theorem: Applications in Computing,Coding, Cryptography, World Scientific, Singapore (1996).

[8] E Quisquater M, Preneel B and Vandewalle J, On the security of the threshold scheme based on the Chinese Remainder Theorem, PKC 2002. LNCS, vol. 2274, pp. 199210. Springer, Heidelberg (2002).