Hybrid cryptosystem RSA – CRT optimization and VMPC

R Rahmadani¹, H Mawengkang² and Sutarman²

¹Master Program (S2) of Informatics Engineering, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia.
²Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Sumatera Utara, Medan, Indonesia.

¹reni_rahmadani@students.usu.ac.id, ²hmawengkang@yahoo.com, ³sutarman@usu.ac.id

Abstract. Hybrid cryptosystem combines symmetric algorithms and asymmetric algorithms. This combination utilizes speeds on encryption/decryption processes of symmetric algorithms and asymmetric algorithms to secure symmetric keys. In this paper we propose hybrid cryptosystem that combine symmetric algorithms VMPC and asymmetric algorithms RSA – CRT optimization. RSA – CRT optimization speeds up the decryption process by obtaining plaintext with $d_p$ and $p$ key only, so there is no need to perform CRT processes. The VMPC algorithm is more efficient in software implementation and reduces known weaknesses in RC4 key generation. The results show hybrid cryptosystem RSA – CRT optimization and VMPC is faster than hybrid cryptosystem RSA – VMPC and hybrid cryptosystem RSA – CRT – VMPC.

Keyword : Cryptography, RSA, RSA – CRT, VMPC, Hybrid Cryptosystem.

1. Introduction
Hybrid cryptosystem is a combination of symmetric and asymmetric key cryptography [1]. Ramaraj et al. [1] formed a security protocol using hybrid encryption on online transactions. This protocol is made using symmetric cipher (AESRijndael) and asymmetric cipher (RSA) with hash function. They have successfully fulfilled three cryptography objectives: integrity, confidentiality and authentication. Rasmi and Paul [2] combine circle symmetric key algorithm and RSA – CRT for e-commerce applications. The symmetric circle symmetric algorithm is based on 2-d geometry using the circle's nature and the center corner of the circle. This algorithm is a block cipher that has advantages in producing cipher text with fixed size. This symmetric algorithm does not require large computations. The time for the encryption / decryption process is not based on the key size. Kuppuswamy and Al-Khalidi [3] conducted research by creating a system that has two different cryptography algorithms. The public key cryptography algorithm used is based on linear block cipher and secret key algorithm based on simple symmetric algorithm. This algorithm fulfills the cryptography objectives of integrity and confidentiality.

VMPC (Variably Modified Permutation Composition) [4] is one of the symmetric cryptography algorithms included in the stream cipher found by Bartosz Zoltak. This algorithm is the modified version of RC4 algorithm. The author claims that the cipher text was designed to be efficient in software implementations and to resist attacks against the cipher's Key Scheduling Algorithm (KSA). As a symmetric cryptographic algorithm that uses the same key for encryption and decryption, it requires the sender to find a secure way to deliver the keys to the receiver [1].
RSA is a public key cryptography algorithm found by Rivest et al. in 1978 [5]. Although it is quite old, RSA still used for securing web traffic, email, and some wireless devices [6]. This is because RSA is a secure cryptographic algorithm for using a large encryption and decryption keys. Therefore, the process in RSA takes a considerable time. Many improvements have been made to speed up the process without reducing the level of security. One of them is RSA - CRT from Quisquater and Couvreur [7]. In this modification, the decryption process is based on the CRT (Chinese Remainder Theorem) method and improvisation on the modulus multiplication. So the whole process is accelerated by reducing the time for the decryption process using smaller exponents and moduli than the RSA algorithm [8].

In this paper we concentrated on RSA – CRT how to make it faster. In doing so, we reduced the decryption time by optimizing RSA – CRT to speed up the overall processing time and perform hybrid cryptosystems on RSA – CRT optimization with VMPC to produce faster algorithms.

2. Study Of Literature

2.1. Hybrid Cryptosystem

One of the approaches of hybrid cryptosystem is to generate a secret key from symmetric cryptography algorithm then encrypt the key with asymmetric cryptography algorithm using receiver public key, and then encrypt the message using the private key of symmetric cryptography algorithm [2].

Hybrid cryptosystem scheme combines the convenience of an asymmetric cryptography algorithm scheme with the effectiveness of symmetric cryptography algorithm scheme. This scheme added security of the delivery process enhancing overall system performance [3].

2.2. RSA

RSA stands for Rivest, Shamir, and Adleman is a cryptography system which security rested on the difficulties of factoring large numbers [5].

RSA Key Generation

- Generate two large prime numbers \( p \neq q \)
- Find \( n = pq \) and \( \phi(n) = (p-1)(q-1) \), integer \( n \) is called modulus (RSA)
- Find \( e \in \mathbb{N} \) where \( e < 1 < n \) and GCD \( (e, \phi(n)) = 1 \)
- Find \( d \in \mathbb{N} \) and \( d < 1 < n \) where \( ed = 1 \mod \phi(n) \)
- Publish \( (n, e) \) and \( (d, p, q, \phi(n)) \) remain private.

RSA encryption process

- Public key \( (n, e) \) received
- Perform encryption process with the formula Encryption \( C \equiv M^e \mod n \)
- Cipher text \( C \) is sent to the owner of the public key

RSA Decryption Process

After the cipher text is received, decrypt the cipher text to get the message \( M \) with formula

Decryption \( M \equiv C^d \mod n \)

\( \phi(n) \) is read totient n is an Euler function where \( n \geq 1 \) and denotes the number of positive integers \( < n \) relatively prime with \( n \).

2.3. RSA – CRT

Using the standard double and square method for modular exponentiation, the cost of RSA process is almost identical to the bit length \( e \) (public key) and \( d \) (private key) [9].

Research conducted by Quisquater and Couvreur [7] aims to reduce the length of decryption process in RSA. They use CRT (Chinese Remainder Theorem) to reduce the large size of modulus on decryption. In their research the decryption process is accelerated by decreasing the value of \( d \) hence
the calculation to get the plaintext becomes smaller. Additional savings in memory space are also possible due to reduced modulus size [8].

In this research the generation of keys and encryption process is the same as RSA, the difference is in the decryption process such as [7].

- Calculate $d_p = d \mod p - 1$ and $d_q = d \mod q - 1$
- Calculate $M_p = C^{d_p} \mod p$ and $M_q = C^{d_q} \mod q$.
- Calculate $M$ from $M_p$ and $M_q$ using CRT.

### 2.4. VMPC (Variably Modified Permutation Combination)

VMPC is a combination of basic operations on permutations and integers. The function in this algorithm can be calculated by three basic operations on permutations per byte. The resulting cipher text is designed to be more efficient in software implementation and reduce known weaknesses in RC4 key generation without reducing its speed and simplicity [4].

In VMPC algorithm there are two processes viz, key scheduling algorithm (KSA) and VMPC stream cipher [4]. VMPC stream cipher performs XOR process on cipher text and cryptography keys derived from KSA. VMPC stream cipher

$n = 0$

Repeat step 3 – 6 $L$ times

- $s = P[(s + P[n]) \mod 256]$
- Output $\oplus (P[(P[P[s]] + 1) \mod 256])$
- Swap $(P[n], P[s])$
- $n = (n + 1) \mod 256$

where: $P = 256$-byte permutation table initialize on KSA VMPC

- $s = 8$-bit variable initialize KSA VMPC
- $n = 8$-bit variable
- $L =$ keystream length in bytes

KSA VMPC converts the cryptographic key into 256 permutation elements $P$ and initializes the variable $s$.

$s = 0$

for $n$ from 0 to 255: $P[n] = n$

for $m$ from 0 to 767: execute step 4-6

- $n = m \mod 256$
- $s = P[(s + P[n] + K[m \mod c]) \mod 256]$
- Swap $(P[n]$ and $P[s])$

where : $c =$ length of cryptographic keys in bytes, $16 \leq c \leq 64$

- $K =$ table storing of $c$ – elements from cryptographic keys
- $m =$ 16 bit variable

### 3. Findings And Discussions

#### 3.1. RSA – CRT Optimization

The proposed scheme to speed up the decryption process at RSA is by optimizing the RSA – CRT (ORSA – CRT). In the proposed scheme the encryption process is the same as RSA, while the decryption process:

- Calculate $d_p = d \mod p - 1$
- Calculate $M = C^{d_p} \mod p$
The optimization performed on RSA - CRT is by eliminating the process to find the value of \( M_p \), so the message is obtained only by calculating the cipher text with \( d_p \) and \( p \) that the CRT process is not necessary. In this scheme the \( p \) and \( q \) keys must be greater than 2 digit number.

3.2. Hybrid Cryptosystem RSA – CRT Optimization and VMPC

In this study we propose a hybrid algorithm by utilizing the symmetric VMPC and RSA – CRT optimization algorithms to produce an efficient and secure cryptography algorithms. The proposed algorithm scheme can be seen in figure 1

![Figure 1. Encryption and Decryption Process](image)

Encrypt the plaintext with VMPC stream cipher using \( P \) and \( s \) keys derived from KSA VMPC. \( P \) and \( s \) are encrypted with RSA – CRT optimization algorithms using previously generated public keys. Cipher text and cipher key are used as input on the decryption process. Then decrypt the cipher key using RSA – CRT optimization private key and obtained \( P, s \). Decrypt cipher text with VMPC stream cipher using \( P \) and \( s \) keys to get the plaintext.

3.3. Result of Decryption Process

Differences of RSA, RSA - CRT, and RSA - CRT optimization algorithms are in the decryption process. In the RSA - CRT optimization algorithm \( p \) and \( q \) value must be greater than 2 digit number to obtain the correct plaintext.

| \( p \)   | \( q \)   | \( e \)   | \( d \)   | Decryption Result |
|--------|--------|--------|--------|------------------|
| 71     | 59     | 53     | 3677   | RSA Experiment   |
| 337    | 509    | 881    | 44561  | RSA - CRT Experiment |
| 7901   | 2531   | 6651   | 18135851 | RSA – CRT Optimization Experiment |
| 85717  | 13829  | 62959  | 989130319 | RSA – CRT Optimization Experiment |
| 59393447 | 31229371 | 73990999 | 1846979500600279 | RSA – CRT Optimization Experiment |
| 612087229 | 260888650 | 7812862283 | 315964251945534483 | RSA – CRT Optimization Experiment |
| 3      | 7      | 5      | RSA Attribute certificate | RSA – CRT Optimization Attribute certificate |
| 779658128 | 397625195 | 930989909 | 171991145629106972 | RSA – CRT Optimization Attribute certificate |
Referring from table 1 RSA – CRT optimization algorithms obtain the correct plaintext as long as the \( p \) and \( q \) keys are larger than 2 digit number.

### 3.4. Results of Hybrid Cryptosystem

Encryption and decryption process of all hybrid algorithms compared to see which hybrid algorithm is faster in processing. In table 2 we can see the difference in execution time of each hybrid algorithm with different key sizes \( n \) and \( e \). The size of \( n \) and \( e \) keys are in bytes.

#### Table 2. Execution Time with Different Keys

| \( n \) length | \( e \) length | RSA – VMPC | RSA – CRT – VMPC | RSA – CRT Optimization and VMPC |
|---------------|---------------|------------|------------------|----------------------------------|
| 256           | 128           | 26.275 sec | 14.841 sec       | 11.653 sec                       |
| 512           | 256           | 176.1 sec  | 88.44 sec        | 70.08 sec                        |
| 1024          | 512           | 1260.78 sec| 620.04 sec       | 491.82 sec                       |
| 2048          | 1024          | 9335.4 sec | 4501.92 sec      | 3599.1 sec                       |

#### Table 3. Data Execution Time

| Char. Length | RSA – VMPC | RSA – CRT – VMPC | RSA – CRT Optimization and VMPC |
|--------------|------------|------------------|----------------------------------|
| 1151         | 23.609 sec | 13.249 sec       | 10.531 sec                       |
| 4563         | 24.013 sec | 13.59 sec        | 10.826 sec                       |
| 8283         | 24.267 sec | 13.925 sec       | 11.146 sec                       |
| 15788        | 25.118 sec | 14.602 sec       | 11.811 sec                       |
| 30656        | 26.274 sec | 15.709 sec       | 13.104 sec                       |

Table 3 shows the execution time of each hybrid algorithm with different message length. The length of \( n \) used is 248 bytes.
Figure 2. Comparison of Data Execution Time

Based on figure 2, hybrid cryptosystem RSA – CRT optimization and VMPC are faster than other hybrid cryptosystems. Hybrid cryptosystem RSA – CRT optimization and VMPC completed the process 53.49% faster than RSA – VMPC and 19.3% faster than RSA – CRT – VMPC.

4. Conclusion

Based on the findings and discussions described in the previous section, it can be concluded that

- RSA – CRT optimization speed up the process by calculating the cipher text only with dp and p that the CRT process is not necessary.
- RSA – CRT optimization can obtain plaintext with p and q key larger than 2 digit number.
- Hybrid RSA – CRT optimization and VMPC are 53.49% faster than RSA – VMPC and 19.3% faster than RSA – CRT – VMPC.

References

[1] Ramaraj E, Karthikeyan S and Hemalatha M 2009 A Design of Security Protocol using Hybrid Encryp. Tech AES- Rijndael and RSA 17 7886.
[2] Rasmi P S and Paul V 2011 A Hybrid Crypto System based on a new Circle – Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Application Proc. of Int. Conf. on VLSI, Comm. & Inst (ICVCI) pp 14–18
[3] Kuppuswamy P and Al-Khalidi S Q Y 2014 Hybrid Encryp./Decryp Tech. Using New Public Key and Symm. Key Algo 19 0113
[4] Zoltak B 2004 VMPC One-Way Function and Stream Cipher Proc. of Fast Soft. Encryp pp 210 –255.
[5] Rivest R, Shamir A and Adleman L 1978 A Method for Obt. Digital Sign. and Public-Key Crypto 21 126.
[6] Boneh D and Shachan H 2002 Fast Var. of RSA 5 52431
[7] Quisquater J. and Couvreur C 1982 Fast Decipher. Algo. for RSA Public-Key Crypto 18 90507
[8] Seungkwang L, Dooho C. and Yongje C 2014 Improved Shamir’s CRT-RSA Algo.: Rev. with the Mod. Chain. Method 36 46978.
[9] Verma, Seema, Garg and Deepak 2015 Improvement in Rebalanced CRT RSA 12 52431