Hybrid cryptosystem multi-power RSA with $N=P^mQ$ and VMPC

U Erdiansyah[1], MKM Nasution[2] and Sawaluddin[3]

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

[1]umrierdiansyah13@gmail.com, [2] mahyuddin@usu.ac.id, [3]sawal@usu.ac.id

Abstract. In digital world, data and information is very valuable and much targeted by unauthorized parties. One way to secure messages is cryptography. Cryptography itself is a branch of science in concealing messages. In further development a hybrid cryptosystem was formed which combines symmetrical and asymmetric cryptography, which in this paper uses VMPC and Multi-Power.. The RSA Multi-Power algorithm is an asymmetric algorithm that is excellent at message encryption but requires a long process time because it uses very complicated calculations. While VMPC has advantages in the process with fast time and relatively small size of ciphertext. Here we have analyzed the performance of various variants of RSA that have been hybridized with VMPC and given the results.

1. INTRODUCTION

Cryptography is a system that can be used to change messages in order to make the message not understood by someone other than the recipient [1]. The combination of symmetrical and asymmetric cryptographic systems is called Hybrid Cryptosystem [2]. One method that is commonly done is to generate a secret key on a symmetrical cryptographic system and then the message is encrypted with that key, then the secret key is encrypted with an asymmetric cryptographic system using the recipient's public key [3]. The hybrid cryptosystem scheme combines the effectiveness of symmetric encryption and the accuracy of asymmetric encryption. So that both of these add to the security of the shipping process along with the increase in results in the entire system [4].

Rivest-Shamir-Adleman (RSA) uses separate public and private keys for each encryption and decryption [5]. The security of the RSA algorithm lies in the complexity of factoring large numbers into prime factors. Factoring is done to obtain a private key. As long as factoring on large numbers becomes prime factors has not been found, the security of the RSA algorithm is guaranteed [6]. With the size of the encryption key used, the size of the ciphertext produced became large. Over time, many people have tried modifying RSA to maximize processing time in RSA without reducing its security. One of them is RSA with Chinese Remainder Theorem (CRT). In this modification, the whole process is accelerated by reducing the time for the decryption process by using exponents and modulus that are smaller than the RSA algorithm [7]. In further development Multi-Power RSA-CRT cryptosystems were developed with $N = Pm \times Q$ [8].

BartoszZoltak [9] developed a Variably Modified Permutation Composition (VMPC) algorithm from the RC4 algorithm. VMPC itself is one of the symmetric cryptographic algorithms that are included in the stream cipher. In this algorithm the message is encrypted

using a secret key obtained from the Key Scheduling Algorithm (KSA). The advantages of VMPC are generates ciphertext efficiently in software implementation and resistant to attacks, such as distinguish attacks (differentiating keystream from random sources) and attacks on KSA keystream. As a symmetric cryptographic algorithm that uses the same key for encryption and decryption, the sender must find a safe way to distribute the key to the recipient [2]. But the resulting ciphertext is the same as the message size because the key used is 8 bits.

2. STUDY OF LITERATURE

2.1 Hybrid Cryptosystem

Many modern cryptographic protocols currently combine symmetric algorithms with asymmetric algorithms to obtain advantages in each algorithm [6]. The common hybrid cryptosystem technique used is to generate secret keys from symmetric cryptographic algorithms and then encrypt keys with asymmetric cryptographic algorithms using the recipient's public key, finally encrypting messages using the private key of cryptographic symmetrical cryptographic algorithms [3].

2.2 RSA

RSA was found by R. Rhivest, A. Shamir, and L. Adleman in 1978. In their writings they describe public key cryptographic systems whose security is based on the difficulty of integer factoring into the primary factors [5]

RSA Key Generation

1. Find two large prime numbers $p \neq q$
2. Determine $n = p*q$ and $\phi(n) = (p-1)*(q-1)$, integer n is called modulus (RSA)
3. Determine $e \in N$where $e< 1 <n$ and GCD $(e, \phi (n)) = 1$
4. Determine $d \in N$and $d< 1 <n$ where $ed \equiv 1 \pmod{\phi (n)}$
5. Values (n, e) are issued but $(d, p, q, \phi (n))$ remain confidential

RSA encryption process

1. Public key (n, e) received
2. Then do the encryption process with the formula
   Encryption $C \equiv M^e \pmod{n}$
3. Cipher text C is sent to the owner of the public key

RSA Decryption Process

When the ciphertext has been received, do the decryption process using the formula

Decryption $M \equiv C^d \pmod{n}$

$\phi(n)$ is read totien 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

Quisquater J. and Couvreur C [10] conducted a study on RSA using CRT to reduce the magnitude of appointment on decryption. In his research the decryption process was accelerated by reducing the d value. The d value is modulated with p and q to get the values dp and dq, then squared it to get the plaintext smaller. Additional savings in memory space are also possible because of reduced modulus size [7].

The generation of keys and encryption process are the same as RSA, but in this research the difference is in the decryption process such as [10].

1. Calculate dp = d mod p – 1 and dq = d mod q – 1

2. Calculate Mp= Cdp mod p and Mq= Cdq mod q.
3. Calculate M from Mp and Mq using CRT.

2.4 Multi-Power RSA

One way to speed up the decryption process from RSA is to use modulo from the formula N = pmq. In this research, we use CRT to gain results much faster than modular exponentiation [8]

The encryption process are the same as RSA, but the key generation and decryption process are different which can be seen as follows [10].

Multi-Power RSA Key Generation

1. Select two prime numbers, p and q
2. Calculate N = pm x q
3. Select an integer e where GCD ((n), e) = 1 and 1 < e < (n)
4. Calculate d = e-1 mod (p - 1)(q - 1)
5. Calculate dp = d mod (p - 1) and dq = d mod (p - 1)
6. The public key is (e, N) and the private key (p, q, dp, dq)

Multi-Power RSA Decryption Process

1. Calculate $M_p = C^{dp}$ mod $p$dan$M_q = C^{dq}$ mod q
2. Calculate from $M$from$M = (Mpq\ (q - 1 \bmod p) + Mq\ (p - 1 \bmod q)) \bmod (pq)$ using CRT

2.5 VMPC (Variably Modified Permutation Combination)

VMPC algorithm is one of the symmetrical algorithms that modifies the RC4 algorithm. The inventor of this cryptographic system is BartoszZoltak, published in 2004 [9]. VMPC Stream Cipher uses KSA to change cryptographic keys and vector initialization (optional) to 256-bit permutations. The VMPC Stream Cipher cryptographic system works by generating VMPC KSA first, then implementing a Pseudo-Random Generator Algorithm (PRGA) that will generate keystream. After that, the XOR operation is performed on the plaintext and keystream to produce the ciphertext.

$n = 0$
Repeat step 3 – 6 L times
  $s = P[(s + P[n]) \bmod 256]$
  Output ^= $(P[(P[P[s]] + 1) \bmod 256])$
  Swap($P[n], P[s]$)
  $n = (n + 1) \bmod 256$
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
$n = m \bmod 256$
$s = P[(s + P[n] + K[m \bmod c]) \bmod 256]$
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 bitvariable

3. FINDINGS AND DISCUSSIONS

3.1 Hybrid Cryptosystem RSA – CRT Optimization and VMPC

In this study we propose a hybrid algorithm by utilizing the symmetric VMPC and Multi-Power RSA algorithms to make an efficient and secure cryptography algorithms. The proposed algorithm scheme can be seen in figure 1

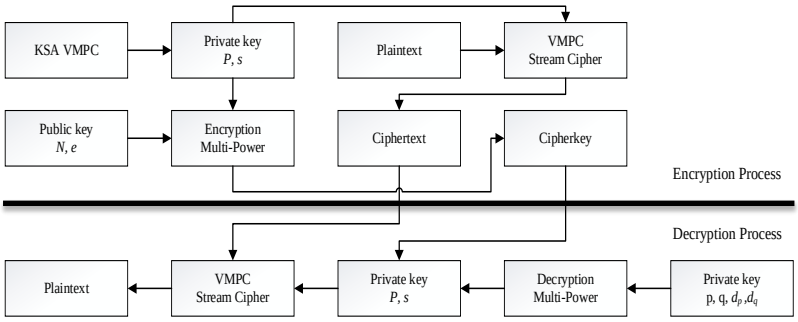

Figure 1. Encryption and Decryption Process

Encrypt the plaintext with VMPC stream cipher using P and s keys derived from KSA VMPC. P and s are encrypted with Multi-Power 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 Multi-Power private key and obtained P, s. Decrypt cipher text with VMPC stream cipher using P and s keys to get the plaintext.

3.2 Result of Decryption Process

RSA – VMPC, RSA-CRT – VMPC, and Multi-Power – VMPC are implemented in Python. These algorithms are tested and calculate the Key Generation, Encryption And Decryption times. Each algorithm is executed for 10 times and mean average time of Key Generation, Encryption and Decryption are tabulated as follows

Key Generation	
Algorithm	Average Time (sec)
RSA – VMPC	12,828
RSA-CRT – VMPC	7,875
Multi-Power – VMPC	4,657

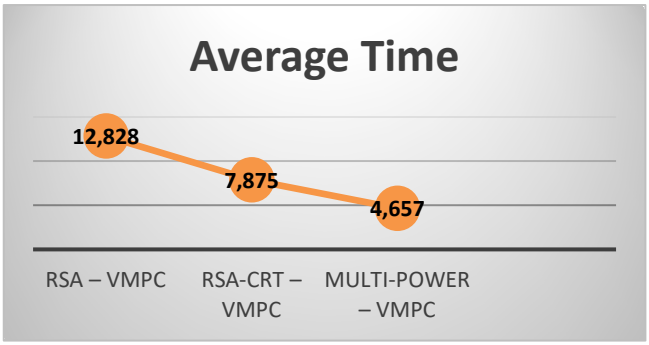

Figure 2. Average mean time taken for Key generation Process

The above Figure 2 shows average time taken in Key Generation process for RSA – VMPC, RSA-CRT – VMPC, and Multi-Power – VMPC. Multi-Power – VMPC is taking less key generation average mean time when compared to other RSA variants.

Encryption	
Algorithm	Average Time (sec)
RSA – VMPC	5,234
RSA-CRT – VMPC	5,143
Multi-Power – VMPC	8,097

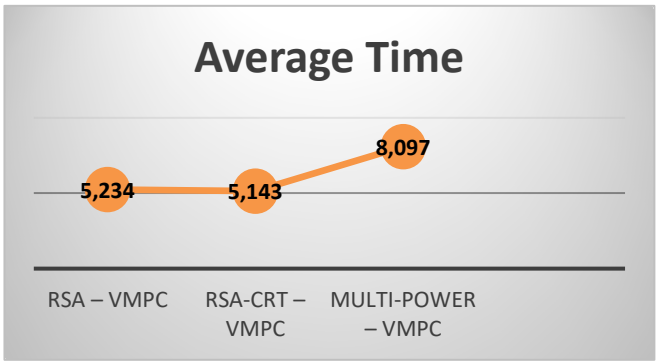

Figure 3. Average mean time taken for Encryption Process

The above Figure 3 shows average time taken in Encryption process for RSA – VMPC, RSA-CRT – VMPC, and Multi-Power – VMPC. RSA-CRT – VMPC is slightly faster than Multi-Power – VMPC.

Decryption	
Algorithm	Average Time (sec)
RSA – VMPC	5,222
RSA-CRT – VMPC	3,985
Multi-Power – VMPC	4,081

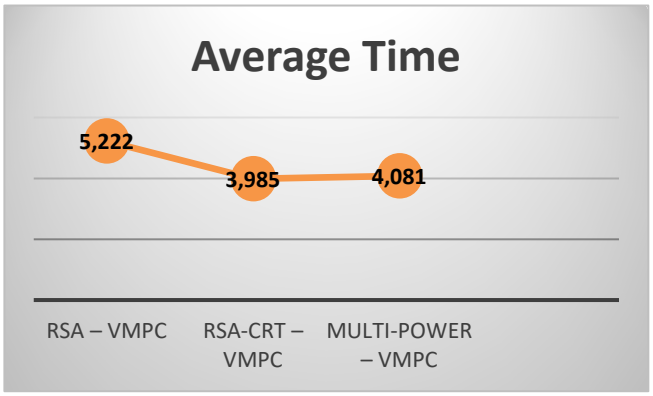

Figure 4. Average mean time taken for Decryption Process

The above Figure 4 shows average time taken in Decryption process for RSA – VMPC, RSA-CRT – VMPC, and Multi-Power – VMPC. RSA-CRT – VMPC is slightly faster than Multi-Power – VMPC.

Finally we are calculating the total time taken for executing the RSA – VMPC, RSA-CRT – VMPC, and Multi-Power – VMPC. Analysis has been made and shown in below Tabel1.

Table 1. Total time taken to execute different algorithms of RSA

Algorithm	Average Key Generation Time	Encryption Time	Decryption Time	Total Time
RSA – VMPC	12,828	5,234	5,222	23,284
RSA-CRT – VMPC	7,875	5,143	3,985	17,003
Multi-Power – VMPC	4,657	8,097	4,081	16,835

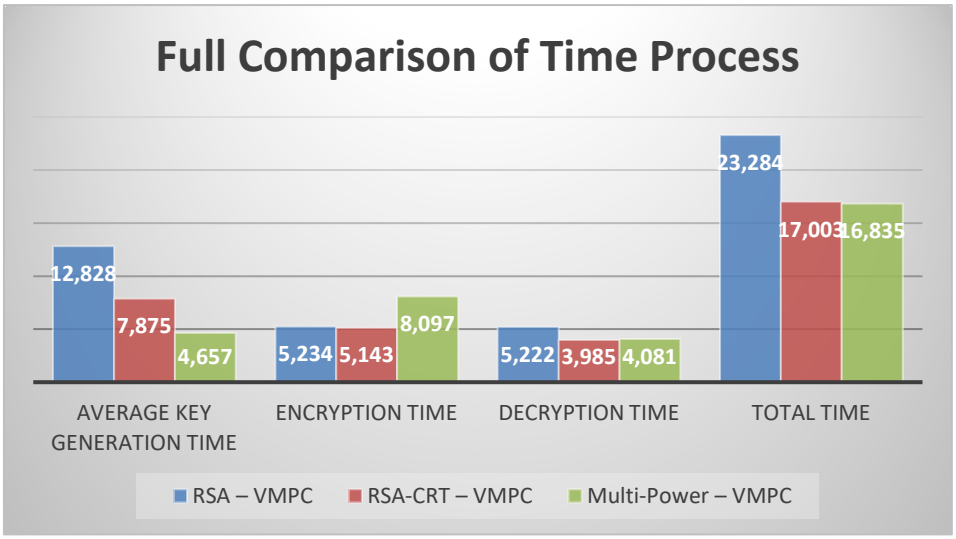

Figure 5. Column chart showing total time taken for existing and proposed algorithms

Figure 5 shows the average time cost in seconds of different variants of hybrid RSA. We have calculated the cost time of Key Generation, Encryption And Decryption Process. When comparing with other hybrid variants of RSA, Multi-Power – VMPC is taking less execution time, giving more performance and more security when compared to other methods. It is decreasing decryption time and giving more security for the data.

4. CONCLUSION

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

1. That Hybrid Multi-Power RSA - VMPC Algorithm requires less time for Key Generation and Decryption processes, which results in shorter overall processing time.
2. Although there is only slightly different from with RSA-CRT - VMPC on processing time, but Multi-Power RSA - VMPC provides more protection with the keys produced more safely.
3. Hybrid Multi-Power RSA - VMPC is 27.70% faster than RSA - VMPC and only 0.99% different from RSA-CRT - VMPC.

5. REFERENCES

[1] Churchhouse R. F. 2002. *Code and Ciphers: Julius Caesar, the enigma and the Internet,* Cambridge University Press

[2] Ramaraj E, Karthikeyan S and Hemalatha M 2009 *A Design of Security Protocol using Hybrid Encryp. Tech.* (AES- Rijndael and RSA). **17** 7886.

[3] 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.

[4] Kuppuswamy P and Al-Khalidi S Q Y 2014 *Hybrid Encryp./Decryp Tech. Using New Public Key and Symm. Key Algo*. **19** 0113

[5] Menezes A J and van Oorschot P C, and Vanstone S A., *Handbook of Applied Cryptography*, CRC Press 1997

[6] Schneier, Bruce. 1996. *Applied Cryptography- Protocols, Algorithms, and Source Code in C*. 2nd Edition. John Wiley & Sons, Inc: New Jersey

[7] Seungkwang L, Dooho C. and Yongje C 2014 *Improved Shamir's CRT-RSA Algo.: Rev. with the Mod. Chain. Method***36** 46978

[8] Sreedevi, E & Padmavathamma, M. 2017. *Design & Implementation of Multi Power RSA– CRT Cryptosystem with N=P^{m}Q. International Journal of InnovativeResearch in Computerand Communication Engineering***5**(3): 5466 – 5472

[9] Zoltak Bartosz 2004 *VMPC One-Way Function and Stream Cipher* Proc. of Fast Soft. Encryp. pp. 210 – 255.

[10] Quisquater J. and Couvreur C 1982 *Fast Decipher. Algo. for RSA Public-Key Crypto*. **18** 90507