Data security system using hybrid cryptosystem RC4A-RSA algorithm

R Rahmadani*, T T A Putri, S Sriadhi, R D Sari, and H D Hutahaean
PTIK-FT, Universitas Negeri Medan, Indonesia

*renirahmadani@unimed.ac.id

Abstract. Data confidentiality is an important aspect of information systems. In case of that we need an application to maintain data confidentiality. This study aims to compare two methods of data security systems, namely using the RC4A algorithm which is a symmetric key cryptographic algorithm and the RSA algorithm which is an asymmetric algorithm with a hybrid process on the RC4A and RSA algorithms to secure the secret key of RC4A and speed up the encryption process of RSA. The study uses a comparative test on two algorithm methods, according to data security system parameters. Data is encrypted with the RC4A algorithm and the RC4A key obtained from KSA RC4A will be encrypted with RSA before sending to the receiver. The test results get Hybrid cryptosystem RC4A-RSA faster in completing the encryption process than RSA. Furthermore, the RC4A key can be secured by being encrypted using the RSA algorithm.

1. Introduction
Data confidentiality is the most important key to data security. Cryptography is one way that can be applied to secure data. There are two key divisions in the cryptographic algorithm namely symmetric keys (private) and asymmetric keys (public). In symmetric keys, the keys used on encryption and decryption have the same value [1]. Symmetric key algorithms are robust against common attacks on data, but weak against brute force attacks on the secret key. This characteristic is the biggest weakness in all cryptographic systems that use a symmetric key algorithm because of the distribution of secret keys between sender and receiver [2]. The RC4A algorithm is a symmetric algorithm so key secrecy must be maintained.

Asymmetric algorithm uses two different keys, namely private key and public key [3]. The key used in encryption process called public key and for decryption called private key. Public key encryption is based on computationally intensive mathematical functions [4]. RSA is a public or asymmetric key algorithm, the keys used in this algorithm are different for encryption and decryption. However, the key to this algorithm uses large numbers so that the encryption and decryption process takes a long time [5]. Hybrid cryptosystem can solve problems that occur in symmetric key and asymmetric key algorithms by combining the strengths of both algorithms [6]. The asymmetric algorithm used to secure the keys of symmetric algorithm and the symmetric algorithm is used to encrypt the information to be sent [7]. In this paper we purpose a hybrid cryptosystem by combining RC4A algorithm and RSA to cover the weakness of RC4A in keys security thereby increasing the overall system result.
2. Method

2.1. Hybrid cryptosystem
Hybrid cryptosystem is a combination of symmetric and asymmetric key algorithms. One approach to hybrid cryptosystem is to generate a secret key from the symmetric algorithm then encrypt the key with an asymmetric algorithm using the recipient's public key, and encrypt the message using the secret key from the symmetric key algorithm [8-10]. Hybrid cryptosystem is the best cryptographic system method available today. This system is called hybrid because it is a combination of symmetric and asymmetric key algorithms. This integration utilizes the security and speed of symmetric algorithms and security forces in key distribution, and authentication from asymmetric algorithms [3].

2.2. RSA
R. Rivest, A. Shamir, and L. Adleman cryptographic systems whose safety rests on the difficulty of factoring large numbers [5]. RSA is a cipher block that each message is mapped into an integer [11].

RSA Key Generation [5].
- Generate two large prime number \( p \) and \( q \), where \( p \neq q \)
- Calculate \( n = pq \) and euler number \( n \phi(n) = (p-1)(q-1) \)
- Let \( e \in \mathbb{N} \) where \( e < 1 < n \) and GCD \( (e, \phi(n)) = 1 \)
- Let \( d \in \mathbb{N} \) and \( d < 1 < n \) satisfying \( ed \equiv 1 \) (mod \( \phi(n) \))
- Publish \((n, e)\) keys while \((d, p, q, \phi(n))\) stay private.

RSA Encryption Process.
- Received public keys \((n, e)\).
- Perform the encryption process with the formula
  \[ C \equiv M^e \pmod{n} \]
- Sent Ciphertext \( C \) to the public keys owner.
- RSA Decryption Process
After the ciphertext is received carry out the decryption process to get the \( M \) message with the formula
  \[ M \equiv C^d \pmod{n} \].

2.3. RC4A
RC4A algorithm is a modification of the stream cipher RC4 cryptographic algorithm which has better security than RC4. The principle of RC4A is to reduce the correlation between output bytes and internal variables by making output bytes more dependent on random variables [12]. RC4A is considered to be stronger in dealing with weaknesses in RC4, especially in the distribution of output in the first two bytes [13]. The ability of RC4A can be improved by extracting hidden step equations in the algorithm [14].

\[ \text{KSA (K)} \]
\[ \text{RC4\_KSA(K, S1)} \]
\[ \text{For } i = 0 \ldots l - 1 \]
\[ WK[i] = \text{RC4\_PRGA(S1)} \]
\[ \text{RC4\_KSA(WK, S2)} \]

\[ \text{PRGA (S1, S2)} \]
\[ \text{Initialization:} \]
\[ i = 0 \]
\[ j1 = j2 = 0 \]
\[ \text{Generation loop:} \]
i = i + 1  
\[ j_1 = j_1 + S_1[i] \]
Swap(S1[i], S1[j1])
Output z1 = S2[S1[i] + S1[j1]]
\[ j_2 = j_2 + S_2[i] \]
Swap(S2[i], S2[j2])
Output z2 = S1[S2[i] + S2[j2]]

3. Result and discussions

3.1. Hybrid cryptosystem RC4A - RSA
In this paper a hybrid process is carried out on the RC4A and RSA algorithms to secure the secret key to RC4A and speed up the encryption and decryption process at RSA. The message will be encrypted with the RC4A algorithm using the RC4A secret key obtained from KSA. Then the RC4A secret key is encrypted with the RSA algorithm using the public key obtained from the receiver before being sent to the recipient. After the ciphertext and the cipherkey are received, the recipient decrypts the cipherkey with the public and private keys that have been generated previously. Then encrypt ciphertext using the decrypted RC4A secret key.

![Encryption and decryption process.](image)

**Figure 1.** Encryption and decryption process.

3.2. Result
To find out the results of the RC4A-RSA hybrid cryptosystem, we performed the encryption process by using different key lengths for each process.
Table 1. Execution time with a different key.

| n length | e length | Time   |
|----------|----------|--------|
| 64       | 32       | 0.585 sec |
| 128      | 64       | 0.94 sec |
| 256      | 128      | 2.697 sec |
| 512      | 256      | 16.363 sec |
| 1024     | 512      | 112.62 sec |
| 2048     | 1024     | 876 sec |

Table 2. Execution time with different character lengths.

| Char. length | RSA    | Hybrid RC4A-RSA |
|-------------|--------|-----------------|
| 26372       | 18.964 | 1.178           |
| 21657       | 16.604 | 1.103           |
| 16719       | 13.183 | 0.986           |
| 10171       | 8.705  | 0.906           |
| 4041        | 3.457  | 0.878           |

The results in table 2 show the difference between the encryption and decryption processing time in the RSA and Hybrid RC4A-RSA algorithms with a key length of 128 bytes.

Figure 2. Comparison of RSA and Hybrid RC4A-RSA execution times.

From Figure 2 it can be seen that the encryption and decryption process is 88.77% faster with the Hybrid RC4A-RSA algorithm. Hybrid RC4A-RSA algorithm is faster than RSA because the messages that must be encrypted by RSA are only RC4A keys which is smaller than most messages.

The execution time of RSA and Hybrid RC4A-RSA algorithm is directly proportional to the size of the key used. The size of the encrypted message greatly affects the execution time of the RSA while on the Hybrid RC4A-RSA algorithm the message size is not very big because the message is encrypted using the RC4A algorithm which produces a ciphertext with a size almost the same as the size of the message.
4. Conclusion
Based on the results described previously, it can be concluded that the Hybrid RC4A-RSA algorithm can improve security in the distribution of RC4A keys by encrypting keys before sending it to the receiver. Hybrid RC4A-RSA algorithm is 88.77% faster than RSA in decryption encryption process.

References
[1] Kester Q A 2013 A Hybrid Cryptosystem Based on Vigenère Cipher and Columnar Transposition Cipher 3 141-7
[2] Preetha M and Nithya M 2013 A Study and Performance Analysis of RSA Algorithm 2 126-39
[3] Torkaman M R N, Kazazi N S and Rouddini A 2012 Innovative Approach to Improve Hybrid Cryptography by Using DNA Steganography 2 225-36
[4] Mahajan P and Sachdeva A 2013 A Study of Encryption Algorithms AES, DES and RSA for Security 13 14-22
[5] Rivest R, Shamir A and Adleman L 1978 A Method for Obt. Digital Sign. and Public-Key Crypto 21 126
[6] Gutub A A A and Khan F A A 2012 Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems pp 116-21
[7] Nadjia A and Mohamed A 2015 AES IP for Hybrid Cryptosystem RSA-AES 1-6
[8] Rahmadani R, Mawengkang H and Sutarman 2017 Hybrid cryptosystem RSA – CRT optimization and VMPC 978 1-6
[9] Ramaraj E, Karthikeyan S and Hemalatha M 2009 A Design of Security Protocol using Hybrid Encrypt. Technology AES- Rijndael and RSA 17 78-86
[10] 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
[11] Kalpana P and Singaraju S 2012 Data Security in Cloud Computing using RSA Algorithm 1 143-46
[12] Budiman M, Rachmawati D and Parlindungan M 2017 An Implementation of Super-Encryption using RC4A and MDTM Cipher Algorithms for Securing PDF Files on Android 978 1-4
[13] Hammood M M, Yoshigoe K and Sagheer A M 2015 Enhancing Security and Speed of RC4 3 37-48
[14] Paul S and Preneel B 2004 A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher pp 245-259