Toward a New Safer Cybersecurity Posture using RC6 & RSA as Hybrid Crypto-Algorithms with VC Cipher

Jenan.S Alkhonaini[1] Shuruq.A Alduraywish[1] Dr. Maria Altaib Badawi[2]

[1] Department of Computer Science and Information, College of Science, Majmaah University, Riyadh city, Saudi Arabia
[2]Department of Computer Science and Information, College of Science, Majmaah University

ABSTRACT
As our community has become increasingly dependent on technology, security has become a bigger concern, which makes it more important and challenging than ever. security can be enhanced with encryption as described in this paper by combining RC6 symmetric cryptographic algorithms with RSA asymmetric algorithms, as well as the Vigenère cipher, to help manage weaknesses of RC6 algorithms by utilizing the speed, security, and effectiveness of asymmetric algorithms with the effectiveness of symmetric algorithm items as well as introducing classical algorithms, which add additional confusion to the decryption process. An analysis of the proposed encryption speed and throughput has been conducted in comparison to a variety of well-known algorithms to demonstrate the effectiveness of each algorithm.

Keywords
Cybersecurity, Cryptographic, Encryption algorithms, hybrid algorithms, Encryption, Decryption, RSA, RC6, Vigenère cipher.

1. INTRODUCTION

The internet's proliferation and technological advancements have created a world where all of your sensitive personal information, as well as all businesses, are exchanged online, stored, and accessed. As a consequence, we hear about Dozens, and occasionally hundreds, of electronic attacks channeled at information systems and computers that destabilize the security of data and aim to unjustly violate rights and hack and tamper with systems. Hence, the need to defend against these attacks emerged, through an important specialty known as cyber security, which focuses on guarding sensitive data and monitoring those who want to cross-systems and deter them, reducing malicious attacks in a unique way. However, cryptography considers which is the most significant measure of cybersecurity and one of its pillars that aims to increase information security It ensures that an institution's private data is safe even if attackers get beyond the firewall through the use of unique codes and algorithms. So, cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher messages in a cryptographic system. To put it in simple terms, the principle of cryptography is to describe the message as a text to be sent is identified as - plaintext-, then is encrypted using an encryption algorithm, turning it into an unreadable -ciphertext- to protect data by generating a secure environment in the presence of malevolent third parties. Thus, this paper is an attempt to improve the security and the performance of encryption algorithms to enhance the security of information to be an ideal process for those who also want to increase security, accurately, and efficiently by combining hybrid crypto algorithms with classical ones. Due to the Hybrid cryptosystems can provide a greater level of security.[1]

2. THEORETICAL BACKGROUND

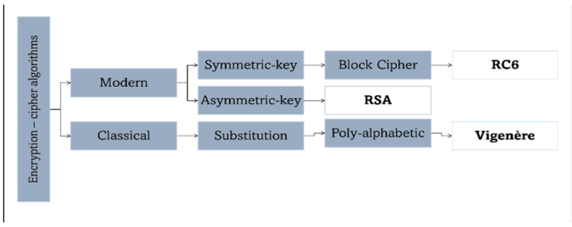
Computer technology has developed into multi-user systems where data may be shared in a computer network or on a larger network, such as the internet, with other users. but there is certain data that should be protected against irresponsible users, counterfeiting, theft, and illegal data conversion.[2] Therefore, it is essential to understand what Cyber Security really is since cyber security is a broad issue that is getting increasingly relevant as the world becomes more linked as a field that is rapidly evolving, and it can be confusing at times. The following definitions apply more to our paper "Cyber Security involves reducing the risk of a malicious attack on software, computers, and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on.".[15]
"The state of being protected against the criminal or unauthorized use of electronic data, or the measures are taken to achieve this.". [16]

That's what motivated us to examine cryptography closely, a crucial component of cyber security, and we will go deeper into its "Cryptocurrency" is derived from "crypto," which is Greek for "secret" - a hint as to what entails the study of cryptography implying that cryptography is the science of writing secret code.[3]
With cryptography, information and communications are

Manuscript received January 5, 2023
Manuscript revised January 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.1.21

safe, since only those who need to see and process them can do so. To put it another way, cryptography is generating secure communication in the presence of malevolent third parties to encrypt and decrypt data. And the basic cryptographic principle is described as a text to be sent is identified as plaintext, then encrypted using an encryption algorithm, this process is known as encryption.[4] The term Encryption algorithm, in cryptography, is a technique for converting plaintext into ciphertext from data as a means of protecting data by combining one or more mathematical procedures with a "key" that may be used to decode the data. The main feature of the encryption/decryption program implementation is the generation of the encryption key.[17]

3. ENCRYPTIONALGORITHMS



Cryptography algorithms

There are two types of encryption algorithms: classical and modern. symmetric and asymmetric encryption are examples of modern encryption. In cryptography, the term "classical" refers to the method of encryption algorithms, often also known as a classical cipher, which is a form of encryption that has been used historically and can be calculated and solved by hand in most cases. it focuses on the computational difficulties of factoring a big number and is based on mathematics. The tremendous complexity of the mathematical issue for instance factorization of a large integer underpins the security of classical cryptography however, modern encryption algorithms are more powerful than classical encryption techniques because they construct ciphertext using operations on binary bit sequence. As we mentioned before, this stream of cryptography is entirely dependent on mathematical principles such as number theory and computational complexity theory, as well as probability notions so the modern encryption algorithm's aim is to provide information security as data privacy, data integrity, and authentication.so, all types of algorithms have come up with powerful encryption mechanisms incorporated into them. All mentioned types of encryption algorithms are used in this paper, starting with the classical Vigenère cipher and then two modern algorithms defined as a hybrid, which is using an asymmetric algorithm to encrypt the key to a symmetric algorithm.

3.1 Vigenère - Classical Cipher

The VC (Vigenère cipher) is a polyalphabetic cipher in which each plaintext letter has multiple corresponding ciphertext letters, which makes cryptanalysis harder with more alphabets to guess and flatter frequency distribution.[7] The choice of the Vigenère Cipher is based on the fact that the Vigenère Cipher is the best example of a compound-alphabet cipher.[8]

The following equations depict the encryption and decryption process:

The plaintext (P) and Key (k) are added modulo 26.

encryption process:

$$Ci = E(Pi + Ki)\ mod\ 26$$

decryption process:

$$Pi = D(Ci - Ki)\ mod\ 26$$

Where C is the ciphertext generated from the Encryption E process by adding the alphabetic index of Plaintext P with a Key K modulated with 26, and vice versa Plaintext P is generated from the Decryption D process by subtracting the Ciphertext C alphabet index with key K and also modulated with 26.[9]

3.2 RSA - Asymmetric Key

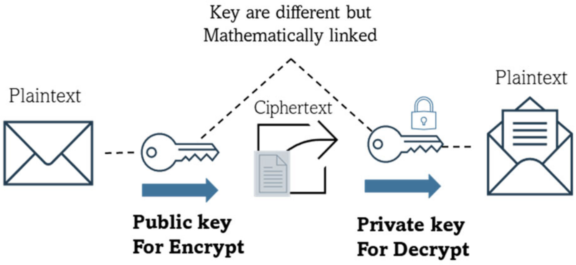
The RSA (Rivest–Shamir–Adleman) is an Asymmetric key cryptography algorithm. The term "Asymmetric" refers to the use of two separate keys: a Public Key and a Private Key.

RSA is commonly used for developing secure communication channels and for digital signatures. [10]

RSA security concept is based on the practical difficulties of factoring the product of two large prime numbers and how to maintain them strong. The public key is formed as a result of multiplying two large prime numbers.

The same two prime numbers are also used to derive the private key.

As a result, the private key is compromised if a huge number can be factorized. Therefore, encryption strength is entirely dependent on the key size, and as key size is doubled or tripled, encryption strength grows exponentially with typical key sizes of 1024 or 2048 bits.



RSA algorithm

3.3 RC6 - Symmetric Key

The RC6 (Rivest Cipher 6) is a symmetric key fast block cipher; it is a well-known modern algorithm but has a fairly good security standard and becomes the nearest rival of the Rijndael algorithm which is the winner of the Advanced Encryption Standard (AES) a competition to gain new standards in the cryptographic fields organized by the National Institute of Standards and Technology (NIST) in 1997.[18]

RC6 is very similar to RC5 in structure, using data-dependent rotations.[12]

Where it uses four running registers instead of two running registers, in addition to integer multiplication.[13]

IT used Data-dependent rotations, XOR operations, and modular addition.

Furthermore, to guarantee that the rotation is dependent on all bits in a word, not just the least significant ones, it also employs an extra integer multiplication operation.

Where it considerably enhances the diffusion accomplished every round, allowing for more security, and higher throughput, in fewer rounds.

The RC6 features are having four registers [A, B, C, D] with a total length of 32 bits that aid in rotation. The first byte of plaintext is placed in the least significant byte of A. The last byte of plaintext is placed into the most significant byte of D. [20]

As it has more registers, the rc6 performs the jobs better and more quickly. And the proper block size of RC6 is 128 bits, while the key sizes are 128, 192, and 256 bits up to 2040 bits.

4. PROPOSED WORK - RESEARCH METHODOLOGY

In a hybrid cryptosystem, a file is secured by using the symmetric algorithm, and a symmetric key is secured by using an asymmetric algorithm.[19]

So combing RSA and RC6 as a hybrid with Vigenère will blend the speed and security forces in authentication and key distribution from the RSA algorithm with the effectiveness and security of the RC6 algorithm while incorporating the Vigenère cipher as double, hackers will be discouraged from decrypting data, which will make it more difficult.

To sum up, hybrid cryptosystems can solve problems that occur in symmetric key and asymmetric key algorithms by combining the strengths of both algorithms.[14]. Based on this approach, we generate the RC6 private key in order to encrypt it with the RSA an asymmetric algorithm, and then encrypt the entire message (including the already encrypted private key as well as the plaintext) with Vigenère Cipher, then re-encrypt by the RC6 which is the original symmetric key. The ciphertext will only be decoded by those who have access to the private key that we generated.

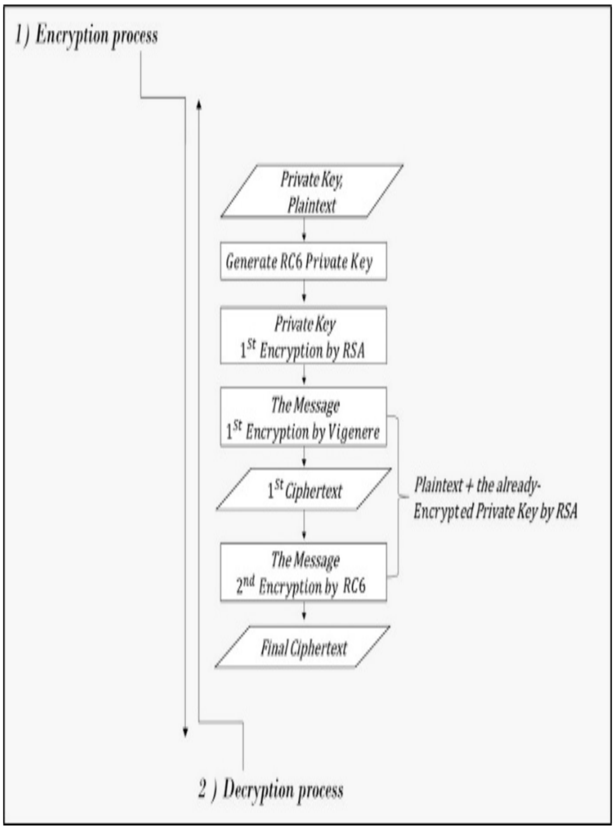

1) Encryption process
Private Key, Plaintext
Generate RC6 Private Key
Private Key 1St Encryption by RSA
The Message 1St Encryption by Vigenere
1St Ciphertext
Plaintext + the already-Encrypted Private Key by RSA
The Message 2nd Encryption by RC6
Final Ciphertext
2) Decryption process

Figure 1. Encryption and decryption process for proposed Algorithm

Fig 3 demonstrates the Encryption and decryption process for the proposed Algorithm. Since we are in the cyber security industry, the security of our chosen algorithms is something we think about and anticipate. As a result, the RC6 algorithm and Vigenère cipher have been cloned from an open-source GitHub repository, since the RC6 technique was originally designed for Python 2, therefore necessary changes have been done to make it more suitable for our sequence, and we use several helper functions to enhance our work, such as the RSA function to produce a random public and private key.

4.1 PROPOSED METRICS

This study compares our proposed algorithm to the results of other algorithms and previous studies in order to measure its performance and effectiveness in computing **throughput MBytes/Sec** and **execution time KBytes/Sec.** An algorithm's encryption time is the time taken to generate an encrypted text (cipher text) from plaintext; its decryption time is the time taken to regenerate plain text from the ciphertext. By dividing the total encrypted plaintext by the encryption time, you can calculate throughput, therefore a higher throughput is considered high performance. The last factor is the execution time, which is used to estimate the throughput of any encryption process, which is calculated by dividing the total encrypted plaintext by the encryption time.

5. RESULTS AND DISCUSSIONS

5.1 Hardware used:

Device name: DESKTOP-2H1RCE5. Processor: 11th Gen Intel(R) Core (TM) i7-11390H @ 3.40GHz 2.92 GHz. Installed RAM: 8.00 GB (7.74 GB usable). System type: 64-bit operating system, x64-based processor.

5.2 Software used:

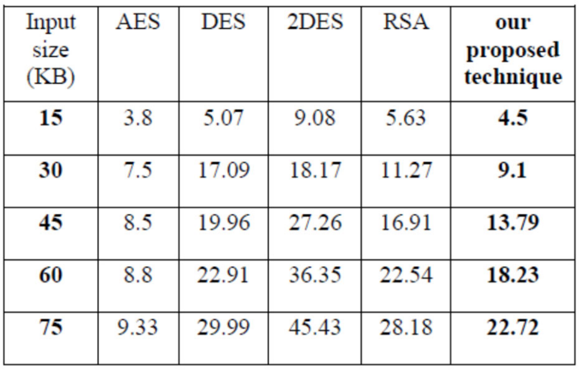
With the aid of Visual Studio, we developed our program using the Python programming language.

5.3 Analysis based on Execution Time

The results shown in Table 1 compare the execution times of our proposed technique to those of the following symmetric block ciphers:

AES (Advanced Encryption Standard), DES (Data Encryption Standard), 2DES (Double DES), and RSA as an Asymmetric key the data used for this analysis were fixed text file sizes. The simulation outcomes at this point are shown in Table 1, during the execution time of the encryption stage, our proposed technique have three types of encryptions have been combined in order to exploit the advantages of each one to build a high security system and yet we achieve excellent results when compared to AES and outperform every other algorithm we have compared with. Additionally, we have an edge over DES and 2DES because their security mechanisms are known to contain wormholes.

Table 1. Execution Time

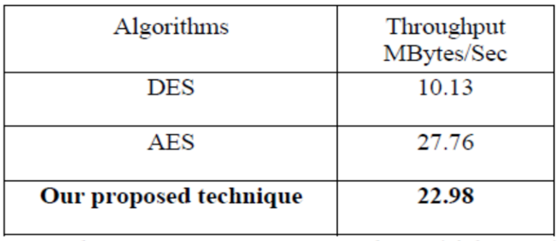


Input size (KB)	AES	DES	2DES	RSA	**our proposed technique**
15	3.8	5.07	9.08	5.63	**4.5**
30	7.5	17.09	18.17	11.27	**9.1**
45	8.5	19.96	27.26	16.91	**13.79**
60	8.8	22.91	36.35	22.54	**18.23**
75	9.33	29.99	45.43	28.18	**22.72**

5.4 Analysis based on Throughput

Table 2 represents the throughput MBytes/Sec metric as well as indicates the speed at which encryption is performed and tells us the degree of diffusion of information. As is shown that the encryption speed of our proposed technique is high compared to the DES algorithm and it performs well compared to AES.

Table 2. Throughput Time



Algorithms	Throughput MBytes/Sec
DES	10.13
AES	27.76
Our proposed technique	**22.98**

The power consumption of AES is reduced since the throughput value has increased. Due to the fact that our algorithm uses both hybrid and double encryption, it is considered a high throughput algorithm and it is more efficient or equally efficient than all the other algorithms considered. furthermore, the experiments being run several times to ensure the results are consistent and valid for comparing different algorithms, there were also some changes made during implementation to measure performance properly.

6. CONCLUSION

In this paper, Enhancements to the security and performance of classical and modern encryption algorithms through a fit-for-purpose combination where each algorithm can perform effectively and

performance factors for our proposed hybrid crypto-algorithms were measured, included throughput, which measures speed, power consumption, and execution time by using fixed text file sizes, to our proposed hybrid crypto-algorithms as well as to other algorithms that were also compared. Our assessment of the simulation results indicates that our primary focus on maintaining the confidentiality of text data was successful, and that overall data privacy and security was improved.

7. REFERENCES

[1] Ruziq, F., Sihombing, P., & Author, C. (2020). Combination Analysis of Data Encryption Standard (DES) Algorithm and LUC Algorithm on File Security. International Journal of Research and Review, 7(2).

[2] Erna,K,N. and Analisis,K,M. (2008) Algoritma Vigenère Cipher Dengan Mode Operasi Cipher Block Chaining (CBC).

[3] Naik, P. G., & Naik, G. R. (2014). Asymmetric key encryption using genetic algorithm. International Journal of Latest Trends in Engineering and Technology (IJLTET), 3(3), 118-128.

[4] Hoobi, M. M., Sulaiman, S. S., & AbdulMunem, I. A. (2020, November). Enhanced Multistage RSA Encryption Model. In IOP Conference Series: Materials Science and Engineering (Vol. 928, No. 3, p. 032068). IOP Publishing.

[5] Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security, 16, 1-11.

[6] Shorman, A., & Qatawneh, M. (2018). Performance improvement of double data encryption standard algorithm using parallel computation. International Journal of Computer Applications, 179, 25.

[7] Bhateja, A. K., Bhateja, A., Chaudhury, S., & Saxena, P. K. (2015). Cryptanalysis of Vigenere cipher using Cuckoo Search. Applied Soft Computing, 26, 315–324

[8] Jamaludin, J., & Romindo, R. (2020). Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security. IJISTECH (International Journal of Information System and Technology), 4(1), 471-481.

[9] Agu, E. O., Ogar Michael, O., & Okwori Anthony, O. (2019). Formation of an improved RC6 (IRC6) cryptographic algorithm. International Journal of Advanced Research in Computer Science, 10(4).

[10] Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. Engineering, Technology & Applied Science Research, 7(4), 1781-1785.

[11] Paje, R. E. J., Sison, A. M., & Medina, R. P. (2019, January). Multidimensional key RC6 algorithm. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (pp. 33-38).

[12] Gunasundari, T., & Elangovan, K. (2014). A comparative survey on symmetric key encryption algorithms. International Journal of Computer Science and Mobile Applications, 2(2), 78-.

[13] A. Sallam, E. EL-Rabaie , O. S. Faragallah. (2012) "HEVC selective encryption using RC6 block cipher technique".

[14] Rahmadani, R., Putri, T. T. A., Sriadhi, S., Sari, R. D., & Hutahaean, H. D. (2020, April). Data security system using hybrid cryptosystem RC4A-RSA algorithm. In IOP Conference Series: Materials Science and Engineering (Vol. 830, No. 3, p. 032008). IOP Publishing.

[15] Amoroso, E. (2006) Cyber Security. New Jersey: Silicon Press).

[16] Oxford University Press. (2014) Oxford Online Dictionary. Oxford: Oxford University Press. October http://www.oxforddictionaries.com/definition/english/Cybersecurity).

[17] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[18] Paar C and Pelzl J 2010 Understanding Cryptography Springer Verlag Berlin Heidelberg

[19] N. Smart, (1999) Cryptography: An Introduction, 3rd Ed

[20] Agu, E. O., Ogar Michael, O., & Okwori Anthony, O. (2019). Formation of an improved RC6 (IRC6) cryptographic algorithm. International Journal of Advanced Research in Computer Science, 10(4).