SW40103 SCIENTIFIC PROJECT II

EFFICIENCY ENHANCEMENT OF RSA CRYPTOSYSTEM USING MODIFIED CFEA LOSSLESS COMPRESSION TECHNIQUE

RAUDATUL ATIQAH RAMDAN & DR. ARIF BIN MANDANGAN
tiqah_datul@yahoo.com & arif.lecture2020@gmail.com
Fakulti Sains dan Sumber Alam, Universiti Malaysia Sabah, 88400, Kota Kinabalu Sabah

Abstract

The rising of data exchange among people is a wake-up call for the urgency of security. In conjunction to people's urgency of data security, cryptography is introduced as cryptography conceal private messages and keep it secure from unauthorized access by using mathematical calculation. The root of this study would be based on Rivest-Shamir-Adleman (RSA) cryptosystem, one of the asymmetric cryptosystems. Because the size of and rose as the number of original plaintexts increased, this study attempted to enhance the efficiency of the RSA cryptosystem's encryption and decryption algorithms by employing a modified CFEA compression approach.The study was carried out in this dissertation by using different numbers of plaintext to fixed size and comparing the results between RSA cryptosystem and modified RSA cryptosystem by using Maple 2021 software as measuring tools. The results indicate that the modified CFEA compression approach is able to reduce the two plaintexts yet not reducing the execution time for the encryption and decryption procedures.

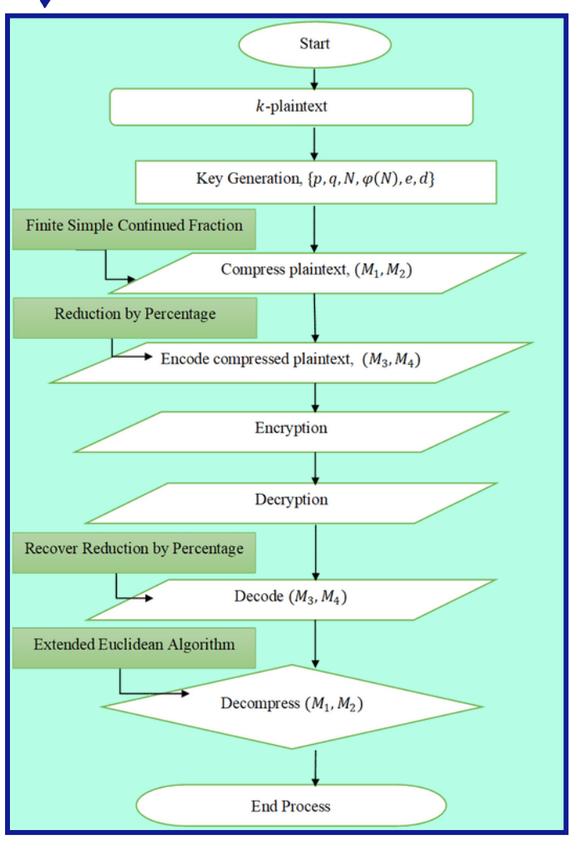
Introduction

Cryptography is a field of study about technique of concealing and hiding private messages and keeping it secure from unauthorized access by using mathematical calculation. cryptography can be classified into asymmetric cryptography and symmetric cryptography. Asymmetric cryptography uses different key for encryption of plaintext and decryption of ciphertext while symmetric cryptography uses same key for both encryption and decryption Rivest-Shamir-Adleman cryptosystem (RSA) is one example of cryptosystem that uses asymmetric key for the system's encryption and decryption process. Continuous Fraction Euclidean Algorithm (CFEA) -Compression is a new way to improve the efficiency of asymmetric cryptosystems.

Objective

- To modify the CFEA compression technique for reducing the size of the compressed plaintext .
- To implement the modified CFEA compression technique in the encryption and decryption algorithm of the RSA cryptosystem.
- To compare the efficiency of the original RSA with the improved RSA cryptosystem.

Methodology

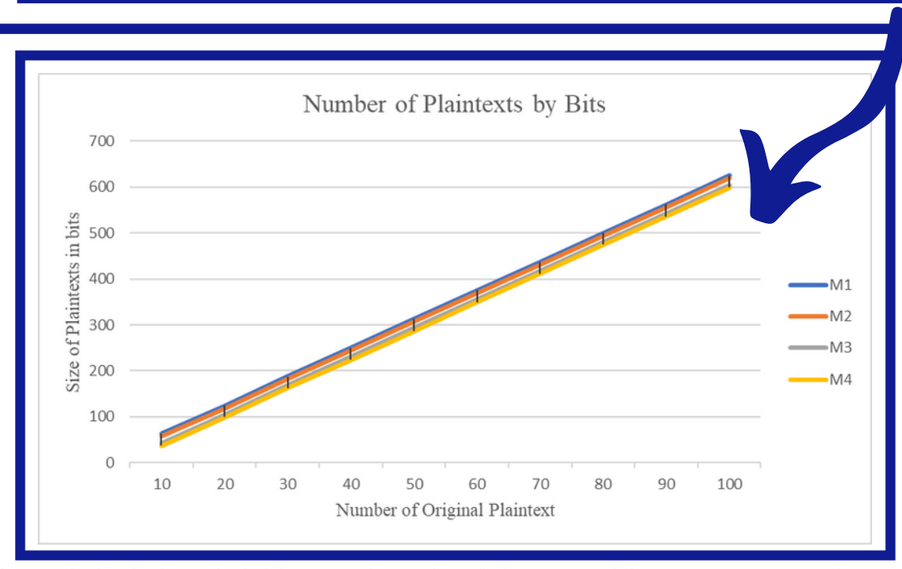


Results

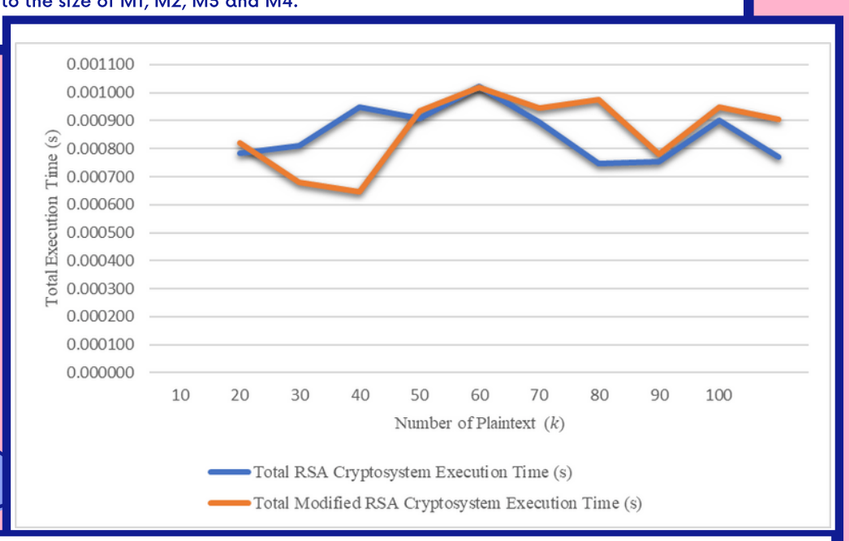
The result of this study showed that the RdB method has significantly reduced the size of plaintext for encryption and decryption as compared to the original RSA cryptosystem. The improved CFEA compression algorithm, on the other hand, required more time to execute for encryption and decryption than the original RSA cryptosystem. The improved CFEA compression technique increase the security level of original RSA cryptosystem.

Discussion

The first figure below has been demonstrated that the modified RSA cryptosystem which implement modified CFEA compression may minimize the size of plaintext (M1, M2) regardless of the number of plaintexts. The second graph below shows the total execution time for both cryptosystems, both were almost similar and has no big differences. However, most of the total execution time for modified RSA cryptosystem has greater total execution time compared to original RSA cryptosystem. From the table comparion Big O notation of original RSA and Modified RSA shows that the worse-case for both cryptosystems is O(N) meaning that both cryptosystems provide the same amount of tempory complexity and this means that the effectiveness of both algorithms is identical and neither is more efficient than the other.



The graph clearly shows the link between the number of plaintexts and the sizes M1, M2, M3 and M4 . When the number of plaintexts rises, so does the size of M1, M2, M3 and M4 . As a result, the number of plaintexts is proportional to the size of M1, M2, M3 and M4.



References

- Daud, M. A., Mahad, Z., Rafley, M., Rasit, A., & Asbullah, M. A. (2020). Use of the CFEA Lossless Data Compression Method in Transmitting Encrypted Modified Baptista Symmetric Chaotic Cryptosystem Data. ASM Science Journal, 26.
- Hung, C. E., & Mandangan, A. (2013, April). Compression-RSA: New approach of encryption and decryption method. In AIP Conference Proceedings
- Siriboonpipattana, W., Soomlek, C., & Seresangtakul, P. (2020, March). Increasing the input data length of RSA cryptosystem by applying a hybrid lossless data compression algorithm. In Journal of Physics: Conference Series

Acknowlegement

I would like to express my deepest appreciation to my supervisor for all the guidance and support provided. I also like to deliver my gratitude towards my examiner, Dr. Suzelawati Zenian for pointed out the weaknesses and given so many useful comments. Also, I'm thankful for my family members and beloved friends that supported me along the way in completing this study. Lastly, of course for those who I might left out, I am pretty assure that all of your assistance would not be overlook.

Conclusion

RdB method has significantly reduced the size of plaintext for encryption and decryption as compared to the original RSA cryptosystem. The modified CFEA compression method also enables us to get back the original plaintext eventhough went through two times of compression on the original plaintext. The improved CFEA compression algorithm, on the other hand, required more time to execute for encryption and decryption than the original RSA cryptosystem. This is because the encryption-decryption process is dependent on the length of the plaintext M3 and M4. The compressed plaintext M3 and M4 would not be show any pattern on how long is the original values repeated when original message is repeated. This definitely reduce the possibility for the unauthorized party to obtain the original plaintext M1 and M2 after encryption is done over the compressed plaintext M3 and M4 and this shows that the security level of modified RSA was improved in this study.

Step	Procedure	Big O Notation
1	Key Generation: i. Choose two distinct, large primes p and q. ii. Compute $N = pq$. iii. Compute $\varphi(N) = (p-1)(q-1)$. iv. Choose a random encryption key, e such that $\gcd(e, \varphi(N)) = 1$, where $1 < e < \varphi(N)$. v. Compute the decryption key d such that $ed \equiv 1 (\mathrm{mod} \varphi(N))$. The public key is $\{N, e\}$ and private key is $\{p, q, d\}$.	O(1)
2	Compress plaintext by finite simple continued fraction	O(N)
3	Encryption: $C_1 = M_1^e (mod\ N)$ $C_2 = M_2^e (mod\ N)$	O(N)
4	Decryption: $M_1 = C_1^d (mod\ N)$ $M_2 = C_2^d (mod\ N)$	O(N)
5	Recover original plaintext by Euclidean algorithm	O(N)

Step	Procedure	Big O Notation
1	Key Generation: i. Choose two distinct, large primes p and q. ii. Compute $N = pq$. iii. Compute $\varphi(N) = (p-1)(e-1)$. iv. Choose a random encryption key, e such that $\gcd(e, \varphi(N)) = 1$, where $1 < e < \varphi(N)$. v. Compute the decryption key d such that $ed \equiv 1 (\mathrm{mod} \varphi(N))$. The public key is $\{N, e\}$ and private key is $\{p, q, d\}$.	O(1)
2	Compress plaintext by finite simple continued fraction	O(N)
3	Reduce original plaintext (M_1, M_2) with Reduction-by-Percentage method	O(N)
4	Encryption: $C_1 = M_1^e (mod\ N)$ $C_2 = M_2^e (mod\ N)$	O(N)
5	Decryption: $M_3 = C_1^d (mod\ N)$ $M_4 = C_2^d (mod\ N)$	O(N)
6	Recover original plaintext (M_3, M_4) with Reduction-by-Percentage method	O(N)
7	Recover original plaintext by Euclidean algorithm	O(N)

Comparing Big O notation for original RSA cryptosystem and modified RSA cryptosystem