Int. J. Appl. Math. Comput. Sci., 2022, Vol. 32, No. 1, 139–146
DOI: 10.34768/amcs-2022-0011

HYBRID CRYPTOGRAPHY WITH A ONE–TIME STAMP TO SECURE CONTACT TRACING FOR COVID–19 INFECTION

AHMED ABDEL-RAHIM EL-DOUH[a,c], SONG FENG LU[a,b,*], ABDELATIF A. ELKOUNY[c], A.S. AMEIN[c]

[a] School of Cyber Science and Engineering
Huazhong University of Science and Technology
1037, Hongshan, Wuhan 430074, China
e-mail: {I201922057,lusongfeng}@hust.edu.cn

[b] Shenzhen Huazhong University of Science and Technology Research Institute
A216, Nanshan, Shenzhen 518057, China

[c] Faculty of Information Systems and Computer Science
October 6 University
Al Mehwar Al Markazi, Giza 12572, Egypt
e-mail: {aelkouny.csis,ahmed.saleh.csis}@o6u.edu.eg

The COVID-19 pandemic changed the lives of millions of citizens worldwide in the manner they live and work to the so-called new norm in social standards. In addition to the extraordinary effects on society, the pandemic created a range of unique circumstances associated with cybercrime that also affected society and business. The anxiety due to the pandemic increased the probability of successful cyberattacks and as well as their number and range. For public health officials and communities, location tracking is an essential component in the efforts to combat the disease. The governments provide a lot of mobile apps to help health officials to trace the infected persons and contact them to aid and follow up on the health status, which requires an exchange of data in different forms. This paper presents the one-time stamp model as a new cryptography technique to secure different contact forms and protect the privacy of the infected person. The one-time stamp hybrid model consists of a combination of symmetric, asymmetric, and hashing cryptography in an entirely new way that is different from conventional and similar existing algorithms. Several experiments have been carried out to analyze and examine the proposed technique. Also, a comparison study has been made between our proposed technique and other state-of-the-art alternatives. Results show that the proposed one-time stamp model provides a high level of security for the encryption of sensitive data relative to other similar techniques with no extra computational cost besides faster processing time.

Keywords: hybrid cryptography, digital signature, hash, RSA, AES, asymmetric cryptography, symmetric cryptography, cybersecurity, COVID-19.

1. Introduction

The COVID-19 pandemic has created a range of unique circumstances associated with cybercrime that have affected society and business. The anxiety due to the pandemic increased the probability of successful cyberattacks, which repreented an increase in cyberattacks and their number and range. The hybrid cryptography technique offer is an advanced encryption algorithm (traditional means of encrypting data are not sufficient for today's information security) (Lallie *et al.*, 2020). Securing information is becoming a big problem in this digital world. It is a good idea for any business owner or person to find the best way to keep their data secure.

One way to protect this information is to encrypt and/or sign them before their distribution process to guarantee this security, i.e., data integrity, authenticity, nonrepudiation, and confidentiality (Papaioannou *et al.*, 2020; Devidas *et al.*, 2021). Users can transmit any kind of files such as text files, audio files, pictures, etc. The system requires a file to be submitted as input

*Corresponding author

which is then encrypted and stored in a remote location. Using shared encrypted files, users may download the file and decrypt it on their computer by using the metadata information shared with them by the owner. There are two different groups of users for the system: the owner of the files and the person who has access to other people's files. The system utilizes asymmetric techniques, symmetric techniques, and hashing algorithms to ensure the integrity and authenticity of a message. In this section, we will present the principles of encryption methods and digital signatures and algorithms for cryptography. Since communication and data transmission across networks has increased exponentially over the last few years, there is a need for protection in the transfer of such data.

The use of cryptography algorithms is one of the solutions to safe communication. To achieve these aims, there is a symmetrical cryptography algorithm and an asymmetric cryptography algorithm (Shetty *et al.*,2020).

1.1. Symmetric cryptography. Symmetric encryption is a well-known and widespread technique. This is a method of encrypting and decrypting electronic data using only one key (a hidden key). Symmetric encryption is faster than asymmetric encryption but the problem of sharing the secret key belongs to symmetrical encryption. Commonly, symmetric encryption has many algorithms such as Blowfish, AES, 3DES, and RC6 (Adeshina, 2020).

1.2. Asymmetric cryptography. In the current sense of the security of all communication networks, the asymmetric key cryptosystem plays an important role (Shetty *et al.*, 2020). The asymmetric key consists of two keys, the first one used in data encrypting and the second used in data decrypting. The current cryptanalytic attacks encourage researchers to call for new approaches to digital signatures to cope with the wide-ranging increase in security attacks. Public-key encryption gains its popularity by developing two pioneering concepts, firstly, solving the key distribution problem of symmetric key cryptography, and secondly, providing a digital signature scheme. There are some algorithms used in asymmetric cryptography such as RSA, DSS, and Elgamal (Sasi *et al.*, 2014).

1.2.1. Digital signature. The most important development from the work on public-key cryptography is the digital signature (Zhan and Ye, 2020). The digital signature is one of the strongest authentication mechanisms for the digital message and offers a range of security features like integrity, authentication, and nonrepudiation that would be difficult to achieve in another way. Suppose the sender would like to send the received data or message. As a safeguard, the recipient must be able to check the validity of the recorded message. When the message is binary and is also presumed to be of the same kind, a full list of its contents can be given. For digital signing, we recommend the use of this classical four-step approach as follows: you set up the signer architecture, prepare the signed message, receive the signed message and then you use the hash function to make the verification. More reliable and convenient technology for safe data is offered by the proposed hybrid technique, using the asymmetric and symmetric keys. The hashing function and digital signature add importance to data authentication.

1.2.2. Hashing. Hashing is the process of taking a string and converting it into a fixed-length value. Hashing is quicker to search for and retrieve because a hash represents the original value as a short unique string. Key asymmetry is used in many encryption techniques. A hash function is a function that performs hashing and therefore, does not need to convert back to its original value. Hash functions include MD2, MD4, and MD5, and there is a standard algorithm known as SHA that produces longer 60-bit message digests (Pittalia,2019).

The remainder of this paper is organized as follows: Section 2 contains clear algorithms on which the proposed model is based. Section 3 discusses the recent works that focus on hybrid cryptography techniques that aim to enhance robustness. Section 4 represents the proposed model. Section 5 discusses the results and performance analysis of the proposed model. A brief conclusion is presented in Section 6.

2. Existing methods

2.1. Advanced encryption standard (AES). The AES algorithm has its structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world (Khachatrian and Abrahamyan, 2019). It is essential for government computer security, cybersecurity, and electronic data protection. The AES algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm that takes the plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard (Zhou *et al.*, 2021).

There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition, and mixing of the input plain text to transform it into the final output of ciphertext. Each round in the algorithm consists of four steps. The first one is the substitution of the bytes; the bytes of the block text are substituted based on rules dictated by predefined S-boxes (the abbreviation for substitution boxes). Next

come the shifting rows (the permutation step). In this step, all rows except the first are shifted left by one bit. The third step is called mixing the columns; this step has two parts. The first part explains which parts of the state are multiplied against which parts of the matrix. The second one explains how this multiplication is implemented over what is called a Galois field. The final step is adding the round key; the message is XORed with the respective round key. When done repeatedly, these steps ensure that the final ciphertext is secure. In this proposed technique we use AES as the symmetric algorithm to encrypt and decrypt the original message.

2.2. Rivest–Shamir–Adleman (RSA). RSA is the most used public-key cryptosystem in the world. It is a public-key encryption algorithm, which is used for both encryption and digital signatures (Shetty *et al.*, 2020). One of the benefits of RSA is that it is easy to incorporate and use. It allows us to detect data tampering. Additionally, fewer resources are needed to sustain it. RSA employs modulus as the dominant element. The RSA algorithm is used in this paper to obtain a signature and secures the key of SHA.

2.3. Secure hash algorithm (SHA). Secure hash algorithms, also known as SHAs, are a family of cryptographic functions designed to keep data secured. An SHA works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed-size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they are transformed into their respective hash values, it is virtually impossible to transform them back into the original data. For this paper, we use SHA-256 because of its speed and security as recommended by FIPS2 180-4 (Zhan *et al.*, 2020). SHA-2 consists of 6 hash functions with 224, 256, 384, or 512 bit digesters. SHA-256 is a computer math function. The measured hash value to check the integrity of the data is compared with the predicted hash value (Sklavos and Koufopavlou, 2003).

3. Related work

The research papers have been scrutinized to understand which method is beneficial in securing the data based on different techniques. A comparative analysis has been made to compare various main algorithms such as AES, DES, 3DES, Blowfish, and RSA. It turns out that AES and Blowfish are the best and most powerful algorithms among the symmetric encryption algorithms. These algorithms are quicker than the others in speed and power consumption. RSA is stable and can, due to the good speed and protection of asymmetric encryption algorithms, be used in wireless networks (Vanitha and Manayarkarasi, 2016).

The AES algorithm for encrypting and decrypting image and text is provided by Rani *et al.* (2019). It uses a 128-bit encryption key that secures and speeds AES more than DES. Since the key is bigger, most attacks such as the assault by brute force and man in the middle of the attack can be overcome. The key concept of this work is the creation and implementation of a safe web. The implementation process of a security system is achieved by using the MRC6 algorithm for the encryption of data and hashed values are used to generate a digital signature using the private key which is followed by the digital Elliptic curve signature algorithm (Lu *et al.*, 2017).

Patil and Bansode (2020) explained how to encrypt and decrypt text with AES. The algorithm has high security than the other standards. There is no indication that AES has any weakness that can be attacked other than exhaustive search, that is brute force. This provides complete security of multiple accounts and multiple files that are confidential. This new method encrypts the images and applies the digital signature to the frame. A digital signature is a tool used to achieve integrity and authenticity of records, digital documents, and applications. The picture is well-known for covering objects which is also an encryption method in steganography. Java is here to support the efficiency of the proposed model under various key lengths, encrypted text lengths, message lengths, times for encryption, and time for decryption (Sharma and Kapoor, 2017). An analysis of different cryptographic hash algorithms and the essential reasoning behind them is given by Kale and Dhamdhere (2018).

The hash value is preserved by various hash algorithms to determine whether or not the message has been changed in different circumstances. It addresses which algorithm is more suited for the specific message. In contrast, the RSA algorithm, which is relatively slow, is considered more reliable in process time than the El-Gamal algorithm, especially for the generation of the signature. In this research, public and private-key El-Gamal and RSA cryptosystems were proposed, simulated, and tested using a sample text file, as a means of creating digital signatures (Papaioannou *et al.*, 2020). They proposed that electronic medical records could become a more secure alternative to electronic medical records by encrypting all patient information using the AES-256 encryption algorithm as one of the best symmetric algorithms and a digital signature that uses RSA key pair to prove the validity of the encrypted data (Mukti and Setiawan, 2020). The El-Gamal encryption scheme is seen as a form of the key-agreement scheme. It is different because it selects multiple random factors for

the same message.

The ICARFAD evaluation mechanism was proposed by Jain *et al.* (2015) to react promptly and improve the identification of the security environment. The security mechanisms proposed by Kumar *et al.* (2020) introduced a new approach for the storage of data using hybrid cryptography through RSA and DES algorithms for cloud storage. The proposed method can make encryption and decryption faster than usual.

4. Proposed technique

4.1. Contact tracing model. Contact tracing can be viewed as an issue of safe communication between pairs of physical users. You can show the contact history of every person to the service provider how you communicate, who sends messages to whom. This concept is recognized as a computer security privacy leakage. Patient contact tracking is about identifying unreported infected individuals that may have contracted the disease in a confirmed case by tracking them back and then secure their information. Some countries such as China, Singapore, and Malaysia have systems (Cho *et al.*, 2020) built to achieve that. A health official (HO) can use the data points of infected patients (and the associated time-stamps) to initiate sessions with everyone who wants to trace themselves and create a report. The report from the patient's perspective may be a text if additional information is required, images such as medical X-rays, or a PDF file containing medical tests, or it may be a voice if the patient is unable to write the text. This is described in Fig. 1. The HO creates a circuit to be sent to all interested individuals. During the evaluation, everyone must perform oblivious communication with the HO. The different format of this information is encrypted through the proposed technique. Also, our system takes advantage of the existence of HO collecting location histories of infected users, as done in many countries hit by the epidemic. We also assume that a vast majority of individuals use location-based services that store their history locally. This research aims to develop a more privacy-preserving approach to centralized communication tracking using GPS data.

4.2. Encryption schema. AES and RSA are the most common encryption algorithms. Both have strengths and weaknesses that make them vulnerable. The AES is a symmetrical algorithm. The sender of data must be able to find the main way to transmit the secret key. The risk that an attacker will find the hidden key is higher. More secure symmetric encryption algorithms rely on the key value and size. AES does not provide signatures of sending to the data transmitted, to ensure authentication and nonrepudiation. Therefore, symmetrical encryption tried to solve the problem of keys sharing. RSA is

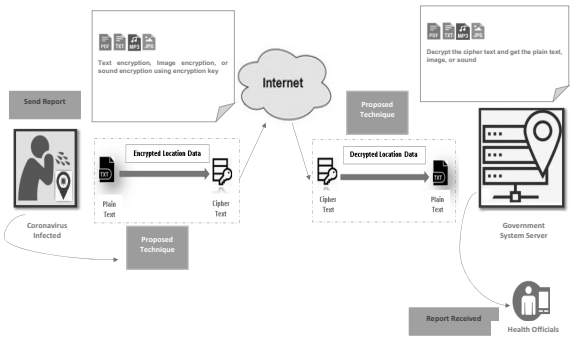


Fig. 1. General architecture scenario of the contact tracing model.

an asymmetrical algorithm with different encryption and decryption keys. Two separate keys and a digital signature are the main benefits of asymmetric cryptography. On the other hand, The RSA algorithm was not used to encrypt messages but to encrypt the symmetric key with the message receiver's public key. This is because the work of the RSA algorithm is slower than symmetric cryptography such as RC or AES. Hashing is a way to obtain a small output from enormous data. Hashing, unlike cryptography, is an irreversible process. The hash value can be produced from the data, but the original data cannot be retrieved from the hash value. Hash functions are designed in such a way that the same hash cannot produce two or more different data items. A calculated hash is compared with an expected hash value through SHA-256 as a method to verify the integrity of the data.

The one-time stamp model uses asymmetric hashing, and symmetric algorithms. They are combined and used to improve the level of data immunity.

- The RSA algorithm is an asymmetric algorithm used to create a digital signature and to encrypt the symmetric key.
- The SHA-256 algorithm is used for producing the hash and as a generator of a one-time stamp symmetric cipher key.
- The AES-128 algorithm is a symmetric algorithm used to encrypt/decrypt the message.

4.3. Proposed one-time stamp model. The 256-bit hash produced from SHA-256 is divided into two halves 128 bits each. The first half is used in the generation of the digital signature. The second half is used as a one-time stamp key for encrypting the message using AES-128. To produce a different hash every time, a time stamp is added to the message before producing its hash. Thus, producing a unique hash as described in Fig. 2. Furthermore, the level of security has increased since the key generated by

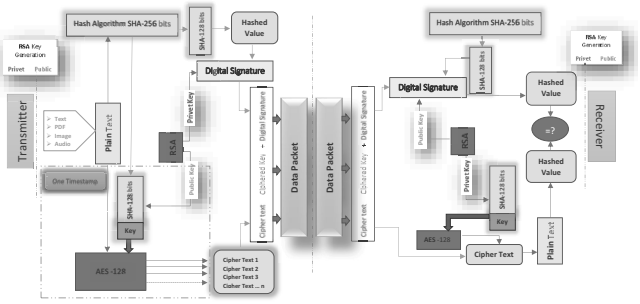


Fig. 2. one-time stamp hybrid cryptography model.

the hash is not even known to the transmitter. In contrast to the normal case, the sender places the initial key and is aware of it.

The encryption and decryption processes are developed as follows, cf. Fig. 2:

1. Encryption:
   - Generate an RSA public key and a private key for encryption.
   - Generate an RSA private key and a public key for signature.
   - Get the data to be encrypted.
   - Divide 256 SHA-bits into two halves.
   - The first 128 bits are used as a key for AES-128 to encrypt data.
   - Encrypt the SHA-128 key using the RSA public key.
   - Create a digital signature using the RSA private key and the other 128 bits of SHA-256.
   - The obtained data packet contains the the ciphertext, cipher key, and the digital signature.
2. Decryption:
   - Verify the signature using the RSA public key.
   - Decrypt the SHA key using the RSA private key.
   - If the key is obtained, use it to decrypt data with AES-128.
   - Integrate for the hashed values from the two halves used in (Key & Signature).
   - Compare the two hashed values.
   - Finally, check the data integrity.

The components of the one-time stamp hybrid cryptography, shown in Fig. 2, are as follows:

Plain text or message: It is the original message, which is required to secure, in consequence, file formats via which the message is formed as input to the system.

Hashing: Converting a string into a fixed-length value is called hashing. Once the information has been converted, it is almost impossible to turn it back into the original data. The SHA-256 algorithm is used for producing the hash and as a generator of a one-time stamp symmetric cipher key. Also, we use SHA-256 because of its speed and security as recommended by FIPS2 180-4 (Zhan and Ye, 2020).

Digital signature: The message digest is encrypted with the sender's private key and embedded into a digital signature. The RSA algorithm is an asymmetric algorithm used to create a digital signature and to encrypt the symmetric key.

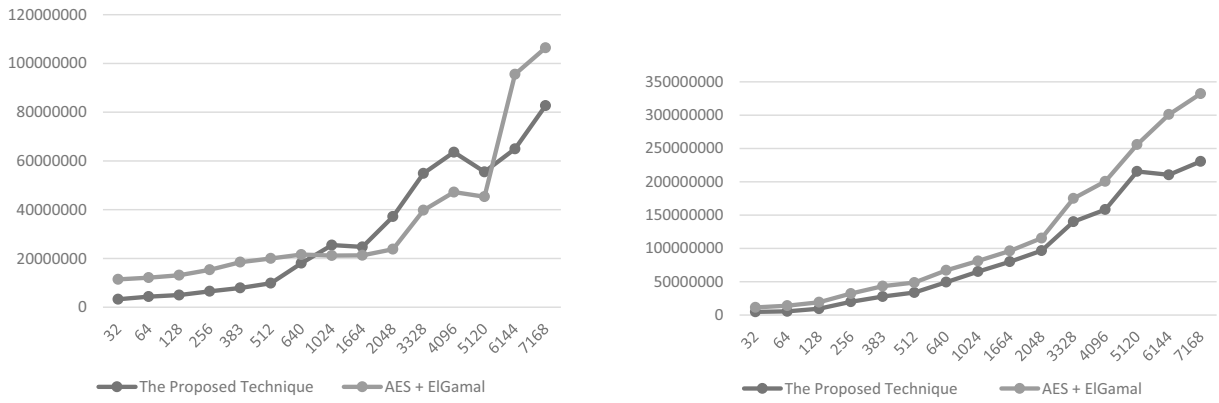
Ciphertext: It is the produced ciphertext after applying the AES algorithm.

5. Results and a discussion

The one-time stamp hybrid cryptography is an innovative and new encryption process to guarantee data protection based on asymmetric, hashing, and symmetric cryptography strengths.

5.1. Materials and methods. The experiments are conducted on a computer device with the various hardware and software requirements is shown in Table 1. The Java security packages are used to implement the digital signature that guarantees data integrity, confidentiality, and nonrepudiation. Also, the AES algorithm is implemented to encrypt and decrypt plain text. We used the development tools known as Inelj JetBrains. Inelj JetBrains enables the users to perform computationally encryption and decryption per specific document. A Java program is written to combine different features required by AES and RSA algorithms to build the enhanced hybrid model. The Chilkat library was used to call encryption algorithms as it is very relevant in cryptography systems. The data used in the following experiments are a set of real data for medical multimedia data related to Covid-19 collected from O6U University's hospital in Egypt. We have tested the proposed model with different input file sizes, Sample text files of sizes 32Kb, 64Kb, 128Kb, 256Kb, 383Kb, 512Kb, 640Kb, 1024Kb,1664Kb, 2048Kb, 3328Kb, 4096Kb, 5120Kb, 6144Kb, 7168Kb were used to evaluate the one-time stamp hybrid cryptography model.

5.2. Performance analysis. The research results describe the output encryption and decryption times with respect of the proposed hybrid algorithm for the complete



(a) (b)

Fig. 3. Encryption (a) and decryption (b) times.

Table 1. Hardware and software details.

Processor	Intel i7 5500U
SSD	512 Crucial GB
RAM	8 GB
Operating system	Linux Mint 19.3 Cinnamon
Programming language	Java JDK 8
IDE	Inelj JetBrains

work. Experiments regarding time efficiency were done using the one-time stamp hybrid cryptography. Different sizes of plain text were used. The execution times for the one-time stamp hybrid cryptography are measured in nanoseconds; Fig. 3(a) shows the encryption times on different file sizes. It is clear from the figure that the encryption time of the proposed hybrid model overcomes the comparable method. The time it takes to retrieve original cipher data is known as the time of decryption.

The proposed one-time stamp model and the AES and ElGamal model (Iavich *et al.*, 2018) yielded performance shown in Fig. 3(b) The decryption time of the proposed hybrid model is efficient compared with the AES and ElGamal models. The results show that in contrast to the AES and ElGamal models, the one-time stamp hybrid cryptography consumes less time. The amount of time depends on file sizes. For comparative value approximation, the average performance of the algorithms is given in Fig. 4. In comparison with the AES and ElGamal models, the one-time stamp hybrid cryptography consumes less time according to the average time in all phases. The memory consumption of the one-time stamp hybrid cryptography and the AES and ElGamal is demonstrated in Fig. 6 to show the advantage of the proposed algorithm. The mean space complexity is computed and reported in Fig. 5. The diagram shows memory consumption in kilobytes. The performance of the proposed model is efficient compared with the AES and ElGamal. A comparison of the plain text size and the encrypted file size was made during tests for the proposed hybrid algorithm (kilobytes). They of the proposed algorithms are shown in Fig. 6. The results show that, compared with the AES and ElGamal methods, the new hybrid model produces better results.

6. Conclusions

This paper presents a new hybrid cryptographic model called the one-time stamp hybrid model. This model uses a combination of asymmetric, hashing, and symmetric algorithms in an entirely new way, different from conventional and similar existing algorithms. Several experiments have been conducted to analyze and evaluate the proposed model. Its performance is based on plain text and ciphertext sizes, memory consumption, and computational times for encryption and decryption. A comparison study has been made with other state-of-the-art models. Our results show that the proposed one-time stamp hybrid model provides a higher level of security for the encryption of sensitive data relative to other similar models with no extra computational cost besides faster processing time.

Acknowledgment

This work is supported by the Hubei Provincial Science and Technology Major Project of China under the grant no. 2020AEA011 and by the Key Research & Development Plan of the Hubei Province of China under the grant no. 2020BAB100, as well as the project of Science, Technology and Innovation Commission of the Shenzhen Municipality of China under the grant no. JCYJ20210324120002006.

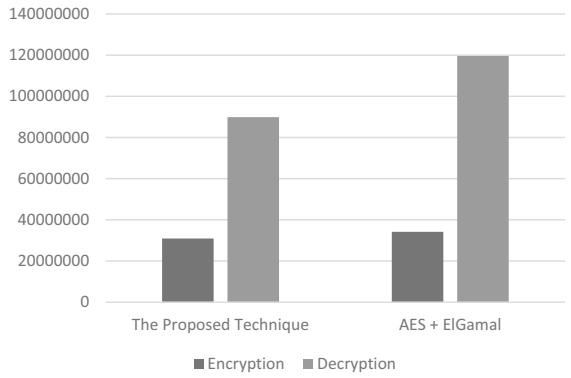


Fig. 4. Average times.

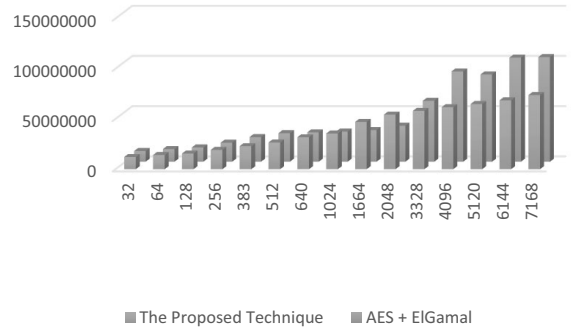


Fig. 5. Memory consumption.

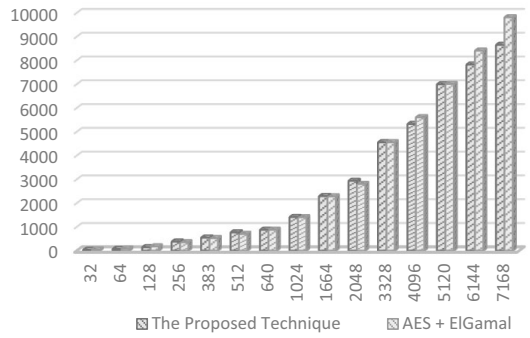


Fig. 6. Encrypted file size.

References

Adeshina, A.M. (2020). Evaluation of elliptic curve El-Gamal and RSA public-key cryptosystems for digital signature, *Information Science, Systems and Technology* **4**(1): 36–49.

Cho, H., Ippolito, D. and Yu, Y. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs, *arXiv* 2003.11511.

Devidas, S., Rao Y.V., S. and Rekha, N.R. (2021). A decentralized group signature scheme for privacy protection in a blockchain, *International Journal of Applied Mathematics and Computer Science* **31**(2): 353–364, DOI: 10.34768/amcs-2021-0024.

Iavich, M., Gnatyuk, S., Jintcharadze, E., Polishchuk, Y. and Odarchenko, R. (2018). Hybrid encryption model of AES and ElGamal cryptosystems for flight control systems, *IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, Kiev, Ukraine*, pp. 127–131, DOI:10.1109/MSNMC.2018.8576289.

Jain, A. and Kapoor, V. (2015). Secure communication using RSA algorithm for network environment, *International Journal of Computer Applications* **118**(7): 6–9.

Kale, M.A. and Dhamdhere, S. (2018). Survey paper on different type of hashing algorithm, *International Journal of Advanced Scientific Research and Engineering Trends* **3**(2): 14–16.

Khachatrian, G. and Abrahamyan, S. (2019). Towards secure and efficient "white-box" encryption, *Journal of Universal Computer Science* **25**(8): 868–886.

Kumar, A., Jain, V. and Yadav, A. (2020). A new approach for security in cloud data storage for IoT applications using hybrid cryptography technique, *International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control, PARC 2020, Mathura, India*, pp. 514–517, DOI: 10.1109/PARC49193.2020.236666.

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *arXiv* 2006.11929.

Lu, S., Ali, H. and Farooq, O. (2017). Proposed approach of digital signature technology for building a web security system based on SHA-2, MRC6 and ECDSA, *2017 2nd International Conference on Information Technology and Industrial Automation (ICITIA 2017), Guangzuhou, China*, pp. 254–261.

Mukti, G.W.W. and Setiawan , H. (2020). Designing and building secure electronic medical record application by applying AES-256 and RSA digital signature, *IOP Conference Series: Materials Science and Engineering* **852**(1): 12148.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V. Essop, I. Rodriguez, J. and Lymberopoulos, D. (2020). A survey on security threats and countermeasures in Internet of medical things, *Transactions on Emerging Telecommunications Technologies* **2020**: 1–15, Paper ID: e4049.

Patil, P. and Bansode, R. (2020). Performance evaluation of hybrid cryptography algorithm for secure sharing of text & images, *International Research Journal of Engineering and Technology* **7**(9): 3773–3778.

Pittalia, P.P. (2019). A comparative study of hash algorithms in cryptography, *International Journal of Computer Science and Mobile Computing* **8**(6): 147–152.

Rani, N.S., Juliet, A.N. and Devi, K.R. (2019). An image encryption and decryption and comparison with text—AES algorithm, *International Journal of Scientific and Technology Research* **8**(7): 668–673.

Sasi, B.S., Dixon, D. and Wilson, J. (2014). A general comparison of symmetric and asymmetric cryptosystems

for WSNs and an overview of location based encryption technique for improving security, *IOSR Journal of Engineering* **4**(3): 01–04.

Sharma, S. and Kapoor, V. (2017). A novel approach for improving security by digital signature and image steganography, *International Journal of Computer Applications* **171**(8): 7–11.

Shetty, V.S., Anusha, R., Dileep, K. and Hegde, P. (2020). A survey on performance analysis of block cipher algorithms, *2020 International Conference on Inventive Computation Technologies, Coimbatore, India*, DOI:10.1109/ICICT48043.2020.9112491.

Sklavos, N. and Koufopavlou, O. (2003). On the hardware implementations of the SHA-2(256, 384, 512) hash algorithms, *2003 International Symposium on Circuits and Systems, Bangkok, Thailand*, pp. 153–156.

Vanitha, M. and Mangayarkarasi, R.(2016). Comparative study of different cryptographic algorithms, *International Journal of Pharmacy and Technology* **8**(4): 26433–26438.

Zhan, W. and Ye, X. (2020). Research on dynamic identity authentication mechanism based on digital signature, *Journal of Physics: Conference Series* **1693**(1): 12009.

Zhou, Y., Tang, G., Yang, J., Yu, P. and Peng, C. (2021). Logic Design and Simulation of a 128-bit AES encryption accelerator based on rapid single flux quantum circuits, *IEEE Transactions on Applied Superconductivity* **31**(6):1302911, DOI: 10.1109/TASC.2021.3075604.

Ahmed Abdel-Rahim El-Douh is currently an assistant lecturer at October 6 University, Egypt. He received his BS in information systems from October 6 University, and his MS degree in big data from Cairo University, Egypt, in 2018. He is currently pursuing his PhD degree in cyber science and engineering at the Huazhong University of Science and Technology, China. His research interests include information security, big data, and the Internet of things.

Song Feng Lu received his PhD degree from the Huazhong University of Science and Technology, Wuhan, China, in 2001. He is currently a professor at the School of Cyber Science and Engineering at that university. He has authored more than 120 articles published in related international conference proceedings and journals, and holds more than 20 patents. His current research interests include information security, quantum computing, and artificial intelligence.

Abdelatif A. Elkouny received his PhD degree in electronic engineering from Kent University, UK, in 2003. From 2004 to 2009 he was a part-time professor at Cairo University, Institute of Statistical Studies & Research. From 2009 to 2012 he was a visiting researcher at Korolev Rocket & Space Cop. Energia. He is currently a lecturer at several universities. He has authored more than 25 articles published in journals and international conferences. His current research interest includes information security and wireless communications.

A.S. Amein received his BSc and MSc degrees in electrical engineering from Military Technical College (MTC), Cairo, Egypt, in 1994 and 2000, respectively, and his PhD degree in electrical engineering from the University of Strathclyde, UK, in 2006. He joined MTC in 1994, where he is now a full professor. His research interests include systems engineering, advanced DSP algorithms, high-resolution SAR imaging algorithms, remote sensing, pattern recognition, modern radar systems design and analysis, millimeter and submillimeter radars, small-target tracking, IoT, and software engineering.

Received: 13 June 2021
Revised: 8 August 2021
Accepted: 18 October 2021