



Testing data security using a vigenere cipher based on the QR code

Eko Hari Rachmawanto^{*1}, Rizky Syah Gumelar¹, Qotrunnada Nabila¹, Christy Atika Sari¹, Rabei Raad Ali²

University of Dian Nuswantoro, Indonesia¹
Northern Technical University, Iraq²

Article Info

Keywords:

Crypto, Decryption, QR Code, Vigenere Cipher, Encryption

Article history:

Received: May 24, 2023

Accepted: September 02, 2023

Published: November 30, 2023

Cite:

E. H. Rachmawanto, R. S. Gumelar, Q. Nabila, C. A. Sari, and R. R. Ali, "Testing Data Security Using a Vigenere Cipher Based on the QR Code", *KINETIK*, vol. 8, no. 4, Nov. 2023.
<https://doi.org/10.22219/kinetik.v8i4.1734>

*Corresponding author.

Eko Hari Rachmawanto

E-mail address:

eko.hari@dsn.dinus.ac.id

Abstract

Data, especially personal data, is sensitive and if misused, it can become a source of threats and crimes for ourselves or for others. Therefore, data security is very important. Cryptography is a way to secure data that aims to safeguard the information that contained in data, so the information contained is not known by unauthorized parties. Vigenere Cipher is a cryptographic method used to hide data with steganography. In the process, the Vigenere cipher converts information called plain text into ciphertext or text that has been steganographed. In this research, process of encryption was carried out on the text based on the given key. The results of the text encryption were stored in the form of a QR-Code which can later be decrypted from the QR-Code using the key, so that the text contained in the QR-Code can be identified.

1. Introduction

Security and privacy are very important things to do in this technological era [1]. Data security is something that aims to protect against crime and data theft [2] and is important to do in order to prevent misuse of information from data [3]. This is because data is sensitive and important to maintain [4]. Especially in the era of technology like now, there might be information sharing that intersect with our privacy [5]. Sharing such information in the application domain is a concern for some people [6]. In some cases, due to the lack of regulation and the high demand for applications, it has an impact on the lack of security and privacy of the products developed [7]. Not only in applications, data privacy is also had an important role in vehicle automatic control systems [8]. In the automatic control system, data security and privacy play an important role in protecting user ID from third parties so that there is no misuse of data [9]. From the explanation given, it can be concluded that data security is important to secure information so that it is not manipulated and used without considering morals and laws [10].

The process of securing data effectively to protect important information is a very necessary thing [11]. The best technology to secure data is using cryptography [12]. Cryptography is an important and widely used part of mathematics [13] to secure privacy and data [14]. Cryptography converts text into a code so that hackers who find the information, cannot see the message directly [15]. In cryptography, it is possible to convert plain text into secret data using keys [16]. Because of this, cryptography is also referred to as a technique for providing confidential communication [17] and to achieve the confidentiality and integrity of data by using user authentication [18] through key that used in the message encryption [19], where that key is only to be known by the sender and receiver [20].

Vigenere cipher is an algorithm in cryptography that is used to prevent hackers from knowing the information provided [21]. This can happen because the process uses key characters that are used to encrypt the text [22]. Which in the process, the key is repeated continuously until it has same length according to the given text [23]. The key is used for the encryption and the decryption of message [24]. In the process of encryption or decryption, vigenere cipher also uses tabula recta table [25]. It contains the letters of the alphabet presented in a 26 x 26 table [26]. Vigenere Cipher is the implementation of symmetric algorithm in cryptography [27] because it uses the same key for encryption process and the decryption. Mittal et. al [28] suggested the implementation of vigenere cipher that inspired by Caesar cipher algorithm which combines two or more alphabet tables. Besides using the alphabet, the Vigenere cipher technique can also use numbers, where the process is the same, namely by shifting to the next area to encrypt [29]. Because it is a simple algorithm, the vigenere cipher can work efficiently with a short computation time [30]. In cryptography, encryption and decryption of data can be done [31]. Encryption is a form of securing data [32]. During the process, encryption converts text into a ciphertext where algorithms and keys are needed to make changes to the text [33]. Decryption is

the process of converting ciphertext into text so that it can be understood by ordinary people [34]. Ahamed et. al [35] suggested that decryption process is the inverse process from encryption process.

QR code is a barcode that is 2-dimensional and can hold up to 4000 or more characters in it [36]. QR codes usually store information, such as personal data and background of a person [37]. QR code has a visualization in the form of a collection of black squares scattered on a white background so that it can be identified [38]. Because of the ease, access and usefulness offered to store information, QR codes are widely used in the process of data verification, payment and others [39]. Ali et. al [40] explained that the storage offered by the QR Code is relatively large and can store a lot of information in the form of characters, alphabet, numbers and others. In this research, an encryption process was carried out by using vigenere cipher algorithm where the information represented in the form of a QR Code. The purpose of this research was to send messages in secret and generate QR codes from the messages. The vigenere cipher algorithm is used because this algorithm is quite easy and efficient to implement, considering that it only aims to encrypt and decrypt messages from the resulting QR Code.

Another research conducted by Putra et al [41] in 2020 discusses the implementation of base64 to encrypt with QR Code media. The purpose of this research is to secure information using the base64 encryption technique for QR codes which were used as an online presence. This research built a system that can prevent the falsification of attendance data and the results of attendance can be properly stored in the database. Furthermore, a research conducted by Ichsan et. al [42] implemented an encryption process with vigenere cipher and QR Code for employee attendance. This research aimed to build a system that can encrypt data using vigenere cipher and show it in the form of a QR code so that the QR code can vanish. The results obtained from this study are that using the QR code-based vigenere cipher algorithm can run well according to the specified process flow.

2. Research Method

2.1 Vigenere Cipher

Vigenere cipher is an algorithm in cryptography to secure data using key characters to encrypt text [22]. Which in the process, this key is repeated continuously until it has a length according to the given text [23]. The key is used for the encryption and the decryption of the message [24]. In the process for encrypting or decrypting, vigenere cipher also uses tabula recta table [25] that contains the letters of the alphabet presented in 26 x 26 table [26]. Apart from using the alphabet, the Vigenere cipher process can also use numbers where the process is almost the same as using the concept of substitution, namely replacing letters with numbers [29]. Because by using letters and numbers, the characters used either as text or keys have limitations, so there is another method of modification from vigenere cipher to perform encryption and decryption, namely by modulo 256.

In the modification process using the 256 method, the characters used are the characters from American Standard Code for Information Interchange or ASCII. By using this 256 modification method, it can use a variety of characters in ASCII as many as 256 characters [43]. In the process of using modulo 256, ASCII characters are used as text which will later be converted into ciphertext [44] by Vigenere cipher. ASCII is a form of character coding where each character is represented by an integer ranging from 0 to 255. During the encryption and decryption process using modulo 256, the text and key will be converted into ciphertext with each text character representing an ASCII value, the encryption and decryption process mathematically can be seen in Equation 1 and Equation 2.

$$N[y] = (H[y] + J[y \bmod c]) \bmod 256 \quad (1)$$

$$M[y] = (N[y] + J[y \bmod c] + 256) \bmod 256 \quad (2)$$

2.2 QR Code

QR code is a barcode that has a 2-dimensional shape and can accommodate and store up to 4000 or more characters in it [36]. QR codes are usually used to store information, such as personal data and medical background of a person [37]. QR codes have a visualization in the form of a collection of black squares scattered on a white background so that they can be identified [38]. Because of the ease, access and usefulness offered to store information, QR codes are widely used in the process of data verification, payment and others [39]. This research uses QR Code because QR Code can withstand attacks and has the ability to overcome errors up to 30%.

Figure 1 shows the visualization of a QR code. Each block or box contained in the QR Code symbolizes something so that it can be read by a computer. In Figure 1, it can be seen that there is a position pattern which usually consists of 3 large boxes at the end of the QR code which functions to help in code recognition. Then, there is a Timing pattern that helps in the data decoding process so that it is possible to calculate the code reading time. Furthermore, there is a quiet zone section that does not contain any modules, which is useful as a border for QR Code. The Data and Error Correction Keys section is used to perform error corrections with the ECI method or can be referred to as Error Correction Keys, so that the QR Code reconstruction results become accurate. And there is an alignment pattern area

which functions to help determine the rotation angle in reading the QR Code pattern and to make corrections to the distortion during the code scanning process.

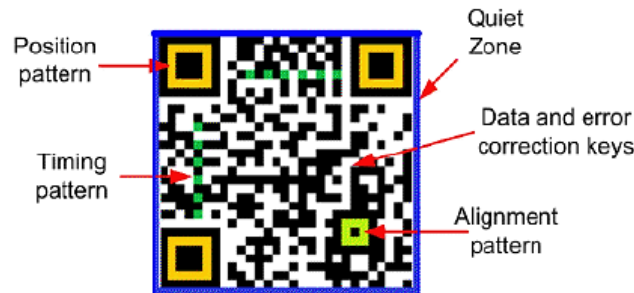


Figure 1. QR Code Component

2.3 Encryption with Vigenere Cipher Modulo 256 and QR Code Transformation

In this research, the encryption and decryption process used Vigenere cipher modulo 256. Encryption process had been carried to make changes to the text into ciphertext using the given key, and the decryption process is used to convert the ciphertext into text using the given key. After obtaining the ciphertext, the transformation process from ciphertext to QR Code is carried out again. So that after the process of converting into a QR Code, the decryption process can then be carried out from the QR Code to text. From this process, the message contained in the QR Code is obtained. For the flow of the process of encrypting text into ciphertext, transforming ciphertext to QR Code and the decryption process of QR Code is given in Figure 2.

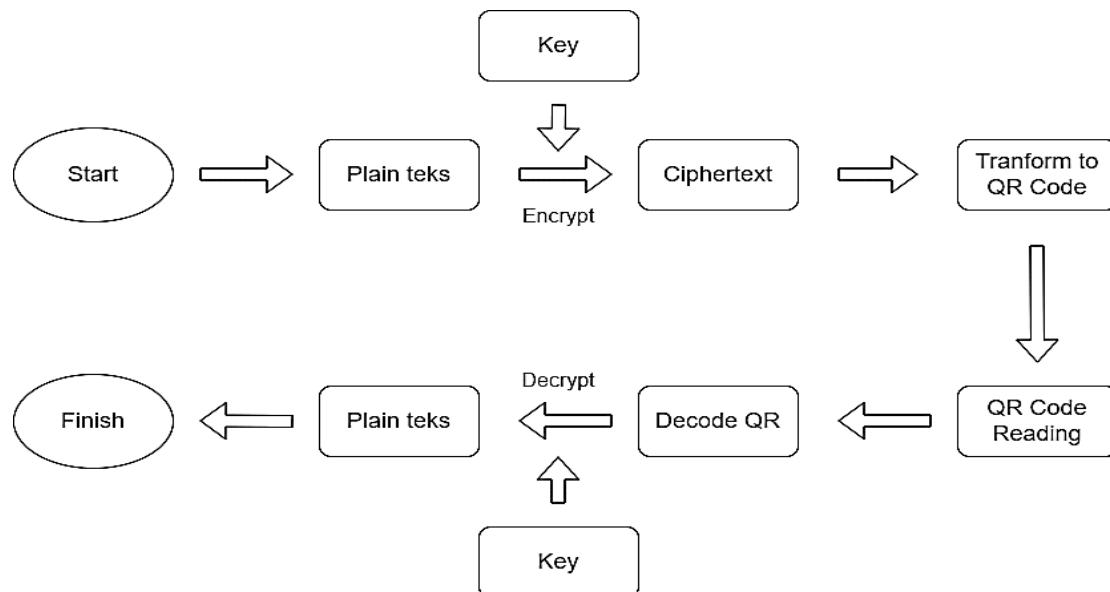


Figure 2. Workflow Process

Figure 2 shows the process flow in performing encryption, transformation of ciphertext into QR and decryption process. During the process of encrypting and decrypting data, the same algorithm, namely Vigenere Cipher, was used. Therefore, the keys were used in these 2 processes, both encryption and decryption processes are the same. For an explanation of the process flow that is done, it is explained below.

1. The first thing to do for the user is to input the text containing the information or message and the key that would be used for encryption and decryption process.
2. After obtaining the text containing information or message, the text is encrypted using the key inputted by the user using the Vigenere Cipher modulo 256.
3. Then after the encryption process is carried out using the information text or message and the key or key using the Vigenere Cipher algorithm, it will produce a ciphertext containing characters that match the given key and have a length according to the inputted information text or message.
4. After obtaining the ciphertext, the transformation process of the ciphertext is changed into a QR Code or can also be referred to as the QR Code encode process. In this process, first the cipher data analysis will be inputted. Then,



encode the data and correct the errors in the data using the Reed-Salomon error correction method, so that the data can be transformed properly without any errors. After the data is checked and transformed, the data will be placed on the block or module of the QR Code. When the placement process is completed, masking will be carried out to protect the data that has been transformed to protect it from the QR Code. After masking, the QR Code has been formed and given version and format information from the generated QR.

5. Then, after getting a QR code that has been generated in accordance with the given ciphertext, the QR reading process of the previous process is carried out again so that the information contained or stored in the QR Code could be read.
6. The next step after reading the QR Code, the QR decode process will be carried out, where in this process, the QR Code pattern will be read and information that is stored inside QR Code will be identified.
7. The next process is the QR Code decode process where the inputted QR Code image will be converted into grayscale form. After becoming a grayscale form, the image is converted again into binary form. When the preprocessing is done, the process of reading the information in the data will be carried out by prioritizing the modules with low level of complexity first. Then, formatting the information found and performing a masking process to reduce the similarity of patterns so that the modules can read the data more accurately. After the masking process, the recovery process is carried out or the recovery of the data contained in the QR and the error checking process is performed. When the data is recovered, it will produce data in the form of ciphertext.
8. After obtaining the ciphertext, the decryption process for ciphertext that had been obtained is carried out by using the same key or key as the encryption process. This process will also use the Vigenere Cipher algorithm to perform decryption based on the decoded ciphertext and the key used.
9. The result obtained after the decryption process is a text which can be read by the user so that the user knows what information or message is contained in the QR Code.

3. Results and Discussion

In this research, the testing process was carried out by inputting text containing information or messages and the keys used. The text and key used characters in the ASCII table so that it is not limited into numbers or alphabets. After the information and key input process, encryption process was carried out using the Vigenere Cipher algorithm which produced a ciphertext after the process. The ciphertext that has been obtained was then transformed into a QR Code. The test results of encryption and QR code transformation are presented in Table 1.

Table 1. Result from Encryption and Transform QR

Information Text	Key	Ciphertext	Generated QR Code
halloTest 123	test123]G`a!fxhZs&CE	
There appeared to be some presence within the tree. Its nature was elusive when viewed from the ground, yet Rachael managed to discern motion. She narrowed her eyes and focused in the motion's direction, aiming to interpret her observation accurately. However, the longer she gazed, the more she entertained the idea that it could be a product of her mind's invention. Every time she shifted her attention away from the tree, it seemed that nothing stirred. But just as she started to divert her gaze, she would catch a glimpse of movement	TheKeyInser t_)QK>Ky+_dKTgE9hZ;eVngU`Z_E[K?Kh-Ts]iH>We@N_lcfKX#_}]YKT[>dfKriAHhK8[m3eYej]ECh5Kq/SsLedMT]N1ea<^iTW!_NNZK8[- WUK_tM6WG3K^lccceW^S8NX:eg9c]Ua#_(QKKT[<ac]XY_=NXKks/bsGaY_;XIA Y_.n]TriH:hS;Zc9]zYrYIGNI@Oi8zsG\blCPe@Uy3]hKeeR:]e4KII^VYXgV6]O;Ty+RW[eVT:U_YeB9fY\XgkT]N1ef9][KetS=Ne3Gt/S eg]ETVU>Ky=WYeXcT:[Z-Oh/SsZ[Z_>MK-en2PheI_8X[8Jy,TsGreRDM[/Zy9UsNXg_BRT0ImIXb\XcT>XTYe?@Tf_rilBNe?N_lb\OYiE9hN1Xy+chKaiDW-e]i_HNK9K^lc\GgtND]N5TalbhOegE9ve[nlYiYgtAHhY4Ky=cUXgZDT]UKJc@TfZr]EGhM-`_UngNXtWD^R0e]+cWNrV_<UO9Vm/nclRbOKNS1TnlXbe[ZRTYK>Oj2TfG_tV>	

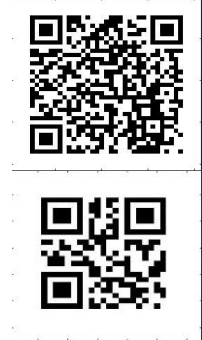
in her peripheral vision, prompting her to resume her intense scrutiny.

\O;T&I_fU`eT>WMKN_<nhUrgEH^S1eb/
asOaiEC\KKY]<dhOanm

This is the key with char and number 123456789_*(!)@^

TheUsedKey1234_

)QOIsOXKZbv2~yYT`OJ\eH4GI1s"x_C^
S8YXd\w-EGIKwmHo]]f%*



Just Test

Key1234

u[m&2gy?Z

Table 1 shows the results from vigenere cipher encryption process and the QR Code obtained from the ciphertext transformation results obtained. It can be seen from the table, testing to encrypt information and transform it into a QR Code can be conducted well, so that the ciphertext can be converted into a QR Code. It also can be seen in the information column given the message to be sent and in the Ciphertext column given the encryption results using the Vigenere cipher modulo 256. Therefore, it can be concluded that the text provided can be properly encrypted by vigenere cipher so that it is not easy for the hackers to directly read the information.

In the next test, the process of reading information from the QR Code that has been generated were carried out to be able to see information that was contained in QR Code. In this test, the QR Code reading, QR Code decoding and decryption process of the QR Code decoded ciphertext were carried out using the key that was used during the encryption. The test results for decoding and decrypting text are given in Table 2.

Table 2. Result from decode QR and Decrypt Ciphertext


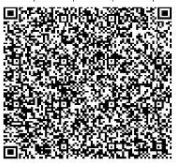


QR Code	Key	Decode QR	Plain Text
	test123	halloTest 123	halloTest 123
	TheKeyInsert_	<p>JQK>Ky+ dKTgE9hZevngU`Z_E[K?Kh-Ts]iH+We@N_lcrKX#_]]YKT>dfKrlAHhk8j m3eYej]ECh5Kq/SsLedMT]NTea<hTWI_NNZk8[-WUJK_tM6WG3K^lceW^S8NX:e g9c]Ua#_[QKKT]<ac]XY_ =NXXks/bsGaY_XIAY_ n]TrH:hS.Zc9]zYYIGNI@Oi8zs GibCPe@Uy3]hKeeR.je4KI^VYXgV6jO_Ty+RW[eVT:U_YeB9YXgkT]N1ef9]]KetS =Ne3Gt/S eg]ETVU>Ky=WYeXCTJZ_OhSsZIZ_>MK-en2 PheU_8X]8jy.TsGreRDM[Z]9JstUqg_BRT0lmXbXct>XYe?@Tf riBNe^N_l]b]OYIE9hN1Yy+chKaiDWVe-][CnZbb_IQKZl/T eU_HNk9K^clGgtND]N5TalbhOegEsvem[n]YIGtAHhY4Ky=cUXgZDT]U KJc@TtZIEGHM^* UofoKtWD^R0eI+cWNNv <UO9Vm/nclRbOKNS1TrN]baf</p>	<p>There appeared to be some presence within the tree. Its nature was elusive when viewed from the ground, yet Rachael managed to discern motion. She narrowed her eyes and focused in the motion's direction, aiming to interpret her observation accurately. However, the longer she gazed, the more she entertained the idea that it could be a product of her mind's invention. Every time she shifted her attention away from the tree, it seemed that nothing stirred. But just as she started to divert her gaze, she would catch a glimpse of movement in her peripheral vision, prompting her to resume her intense scrutiny.</p>
	TheUsedKey1234_)QOIsOXKZbv2~yYT`OJ\eH4GI1s"x_C^S8YXd\w-EGIKwmHo]]f%*	This is the key with char and number 123456789_*(!)@^
	Key1234	u[m&2gy?Z	Just Test

Table 2 shows the results from decoding and decrypting the ciphertext using the Vigenere cipher and the key used during encryption. Had been seen in Table 2, the decode process to get the ciphertext contained in the QR Code runs well. This is indicated by after the decryption process, the message or information contained in the QR Code matches the original message used to generate the QR Code.

In the next test, an attack was carried out on the QR Code containing the text or information sent. The attack carried out is the image inverse process, blur using gaussian blur, darkening the image by 60%, vertical flip, salt and pepper noise of 0.6, 45 degrees rotation and 90 degrees rotation. In this test, an attack was carried out on QR Code 3,

with the message "This is the key with char and number 123456789_*(!@^" and the key "TheUsedKey1234_". This attack process aimed to see the durability of encryption and QR Code in storing information or messages after QR is given an attack. In this process it will be seen if the image is given an attack whether the text or information contained can still be recognized or not. For testing the attack QR Code is given in Figure 3.

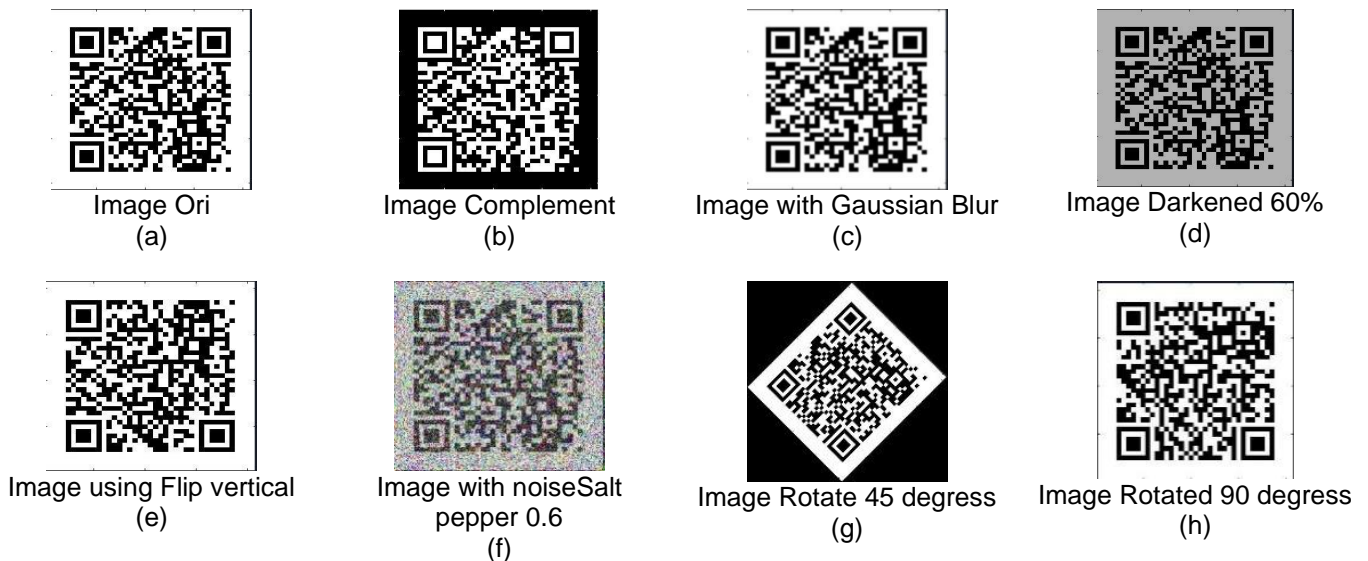


Figure 3. Attacking Process In QR Code

Figure 3 shows the results of the attacks given to the QR Code. After the attack process is carried out on the QR Code, the process is carried out again to decode the QR and decrypt the message using Vigenere Cipher and key that used during the encryption process. The results obtained are that when the QR Code is attacked in the form of salt and pepper noise, the decryption process cannot be done and the information in the QR Code cannot be restored as before. Meanwhile, when using other attack methods such as Complement, Gaussian Blur, Darkened 60%, Flip vertical, Rotate 45 degrees and Rotated 90 degree, the QR decode and decryption process can run well and produce the same information according to the message sent.

4. Conclusion

After conducting research and testing the encryption process using the Vigenere cipher modulo 256, it can be concluded that the encryption process can run well so that it can hide information into ciphertext based on the text and key given. After testing the transformation of the ciphertext into a QR Code, it is concluded that the ciphertext can be stored properly in the QR Code. This is shown from the decoding and decrypting process. When the QR decode process produces the ciphertext contained in the QR Code and after the decryption process is carried out using vigenere cipher and key that used for the encryption process, it produces a message or information that matches the original message or information sent. Therefore, it can be concluded that the process of encryption and encoding into QR can be simple and effective to send and secure the information provided on the barcode. For further research, it is expected to use more complex methods such as AES (Advanced Encryption Standard), Hill cipher, Quantum Cryptography and others. And also further researches are expected to be able to modify the vigenere cipher method used, such as by using a matrix measuring 95 x 95.

References

- [1] Sun, P. J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access*, 7, 147420–147452. <https://doi.org/10.1109/ACCESS.2019.2946185>
- [2] Mondal, S.K., Mukhopadhyay, I., Dutta, S. (2020). Review and Comparison of Face Detection Techniques. In: Chakraborty, M., Chakrabarti, S., Balas, V. (eds) Proceedings of International Ethical Hacking Conference 2019. eHaCON 2019. Advances in Intelligent Systems and Computing, vol 1065. Springer, Singapore. https://doi.org/10.1007/978-981-15-0361-0_1
- [3] Hidayat, T., & Mahardiko, R. (2020). A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing. *International Journal of Artificial Intelligence Research*, 4(1). <https://doi.org/10.29099/ijair.v4i1.154>
- [4] Adil Yazdeen, A. ., Zeebaree , S. R. M. ., Mohammed Sadeeq, M., Kak, S. F. ., Ahmed, O. M. ., & Zebari, R. R. (2021). FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review. *Qubahan Academic Journal*, 1(2), 8–16. <https://doi.org/10.48161/qaj.v1n2a38>
- [5] Machin, J., Batista, E., Martínez-Ballesté, A., & Solanas, A. (2021). Privacy and security in cognitive cities: A systematic review. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 10). MDPI AG. <https://doi.org/10.3390/app11104471>

- [6] Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55–69. <https://doi.org/10.1016/j.tele.2019.03.003>
- [7] A. R. Sai, J. Buckley and A. Le Gear, "Privacy and Security Analysis of Cryptocurrency Mobile Applications," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2019, pp. 1-6, doi: 10.1109/MOBISECSERV.2019.8686583.
- [8] Dave, R., R Sowell Boone, E., & Roy, K. (2019). Efficient Data Privacy and Security in Autonomous Cars. *Journal of Computer Sciences and Applications*, 7(1), 31–36. <https://doi.org/10.12691/jcsa-7-1-5>
- [9] Malik, S., Khattak, H. A., Ameer, Z., Shoaib, U., Rauf, H. T., & Song, H. (2021). Proactive Scheduling and Resource Management for Connected Autonomous Vehicles: A Data Science Perspective. *IEEE Sensors Journal*, 21(22), 25151–25160. <https://doi.org/10.1109/JSEN.2021.3074785>
- [10] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. In *Egyptian Informatics Journal* (Vol. 22, Issue 2, pp. 177–183). Elsevier B.V. <https://doi.org/10.1016/j.eij.2020.07.003>
- [11] Alqadi, Z., Abu-Faraj, M., & Alqadi, Z. A. (2021). Improving the Efficiency and Scalability of Standard Methods for Data Cryptography Improving the Efficiency and Scalability of Standard Methods for Data Cryptography Mua'ad. *IJCSNS International Journal of Computer Science and Network Security*, 21(12). <https://doi.org/10.22937/IJCSNS.2021.21.12.61>
- [12] Navid Bin Anwar, M., Hasan, M., Hasan, M., Loren, J. Z., & Tanjim Hossain, S. M. (2019). Comparative Study of Cryptography Algorithms and Its' Applications. In *International Journal of Computer Networks and Communications Security* (Vol. 7, Issue 5). www.ijcnscs.org
- [13] Benssalah, M., Rhaskali, Y., & Drouiche, K. (2021). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimedia Tools and Applications*, 80(2), 2081–2107. <https://doi.org/10.1007/s11042-020-09775-9>
- [14] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2020). Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 73–80. <https://doi.org/10.1109/TSMC.2019.2903785>
- [15] Wahab, O. F. A., Khalaf, A. A. M., Hussein, A. I., & Hamed, H. F. A. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE Access*, 9, 31805–31815. <https://doi.org/10.1109/ACCESS.2021.3060317>
- [16] Hureib, E., Gutub, A., bin Hureib, E. S., & Gutub, A. A. (2020). Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography Steganography and Secret sharing View project Cryptography and Steganography View project Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 20, Issue 8). <https://www.researchgate.net/publication/344311992>
- [17] Alyousuf, F. Q., Qasim, F., Al-Yousuf, A., & Din, R. (2020). Review on secured data capabilities of cryptography, steganography, and watermarking domain Topic identification using filtering and rule generation algorithm for textual document View project The modeling of E-Supervised (E-SUV) for distance learning centre View project Review on secured data capabilities of cryptography, steganography, and watermarking domain. *Indonesian Journal of Electrical Engineering and Computer Science*, 17(2), 1053–1059. <https://doi.org/10.11591/ijeecs.v17.i2.pp1053-1059>
- [18] Alqad, Z., Majid Oraiqat, ;, Almujafet, ; Hisham, Al-Saleh, S., Hind, ;, Husban, A., & Al-Rimawi, S. (2019). International Journal of Computer Science and Mobile Computing A New Approach for Data Cryptography. In *International Journal of Computer Science and Mobile Computing* (Vol. 8, Issue 9). www.ijcsmc.com
- [19] Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, 1918(4). <https://doi.org/10.1088/1742-6596/1918/4/042009>
- [20] Abu-Faraj, M. M., Aldebei, K., & Alqadi, Z. A. (2022). Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography. *Traitement Du Signal*, 39(1), 173–178. <https://doi.org/10.18280/ts.390117>
- [21] Nahar, K., & Chakraborty, P. (2020). A Modified Version of Vigenere Cipher using 95 95 Table. *International Journal of Engineering and Advanced Technology*, 9(5), 1144–1148. <https://doi.org/10.35940/ijeat.E9941.069520>
- [22] Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, 1918(4). <https://doi.org/10.1088/1742-6596/1918/4/042009>
- [23] Voleti, L., Balajee, R. M., Vallepu, S. K., Bayoju, K., & Srinivas, D. (2021). A Secure Image Steganography Using Improved Lsb Technique and Vigenere Cipher Algorithm. *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, 1005–1010. <https://doi.org/10.1109/ICAIS50930.2021.9395794>
- [24] Hameed, T. H., & Sadeeq, H. T. (2022). Modified Vigenère cipher algorithm based on new key generation method. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(2), 954–961. <https://doi.org/10.11591/ijeecs.v28.i2.pp954-961>
- [25] Sermen, J. P., Secugal, K. A. S., & Mistio, N. E. (2021). Modified Vigenere cryptosystem: An integrated data encryption module for learning management system. *International Journal of Applied Science and Engineering*, 18(4(Special Issue)), 1–10. [https://doi.org/10.6703/IJASE.202106_18\(4\).003](https://doi.org/10.6703/IJASE.202106_18(4).003)
- [26] Banday, S.A., Pandit, M.K., Khan, A.R. (2021). Securing Medical Images via a Texture and Chaotic Key Framework. In: Giri, K.J., Parah, S.A., Bashir, R., Muhammad, K. (eds) *Multimedia Security. Algorithms for Intelligent Systems*. Springer, Singapore. https://doi.org/10.1007/978-981-15-8711-5_1
- [27] Politeknik Ganesha Medan, R. (2020). Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security. *International Journal of Information System & Technology Akreditasi*, 4(1), 471–481. <https://doi.org/10.30645/ijstech.v4i1.85>
- [28] Kumar Mittal, V., Mukhija, M., & Tech, M. (2019). Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique the Creative Commons Attribution License (CC BY 4.0). *International Journal of Trend in Scientific Research and Development (IJTSRD) International Journal of Trend in Scientific Research and Development*, 5, 1936–1939. <https://doi.org/10.31142/ijtsrd27878>
- [29] Khasanah, Nguyen, P. T., Gunawan, G., & Rahim, R. (2020). Three-pass protocol scheme on vigenere cipher to avoid key Distribution. *Journal of Critical Reviews*, 7(1), 68–71. <https://doi.org/10.22159/jcr.07.01.13>
- [30] Jaithunbi, A. K., Sabena, S., & Sairamesh, L. (2023). Preservation of Data Integrity in Public Cloud Using Enhanced Vigenere Cipher Based Obfuscation. *Wireless Personal Communications*, 129(1), 271–284. <https://doi.org/10.1007/s11277-022-10097-2>
- [31] Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *Journal of Physics: Conference Series*, 1997(1). <https://doi.org/10.1088/1742-6596/1997/1/012021>
- [32] Rizal, A., Utomo, D. S. B., Rihartanto, R., Hiswati, M. E., & Haviluddin, H. (2019). Modified key using multi-cycle key in vigenere cipher. *International Journal of Recent Technology and Engineering*, 8(2 Special Issue 11), 2600–2606. <https://doi.org/10.35940/ijrte.B1313.0982S1119>
- [33] S. Vatshayan, R. A. Haidri and J. Kumar Verma, "Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher," 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 848-852, doi: 10.1109/ComPE49325.2020.9199997.
- [34] Uniyal, N., Dobhal, G., Rawat, A., & Sikander, A. (2021). A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication. *Wireless Personal Communications*, 119(2), 1577–1587. <https://doi.org/10.1007/s11277-021-08295-5>

- [35] Ahamed, B. B., & Krishnamoorthy, M. (2022). SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm. *Journal of the Operations Research Society of China*, 10(4), 835–848. <https://doi.org/10.1007/s40305-020-00320-x>
- [36] A. Nuhi, A. Memeti, F. Imeri and B. Cico, "Smart Attendance System using QR Code," 2020 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2020, pp. 1-4, doi: 10.1109/MECO49872.2020.9134225.
- [37] Tiantian Wang , Fei Jia, The impact of health QR code system on older people in China during the COVID-19 outbreak, Age and Ageing, Volume 50, Issue 1, January 2021, Pages 55–56, <https://doi.org/10.1093/ageing/afaa222>
- [38] A. G. Khan, A. H. Zahid, M. Hussain and U. Riaz, "Security Of Cryptocurrency Using Hardware Wallet And QR Code," 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 2019, pp. 1-10, doi: 10.1109/ICIC48496.2019.8966739.
- [39] Dey, S., Saha, S., Singh, A. K., & McDonald-Maier, K. (2021). FoodSQRBlock: Digitizing food production and the supply chain with blockchain and QR code in the cloud. *Sustainability (Switzerland)*, 13(6). <https://doi.org/10.3390/su13063486>
- [40] Mohammed Ali, A., & Farhan, A. K. (2020). Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document. *IEEE Access*, 8, 27448–27458. <https://doi.org/10.1109/ACCESS.2020.2971779>
- [41] Putra, I. P., Witriyono, H. ., Rifqo, M. H. ., & Muntahanah, M. (2022). Utilization of Base64 Encryption Repetition for QR Code Presence on Online Attendance. *Jurnal Komputer, Informasi Dan Teknologi (JKOMITEK)*, 2(2), 519–528. <https://doi.org/10.53697/jkomitek.v2i2.942>
- [42] Ichsan, M., & Hutrianto, H. (2022). Implementasi Algoritma Vignere Chiper Berbasis QRCode Untuk Absensi Pegawai PT. Delameta Bilano Cabang Ruas Tol Palembang - Inderalaya. *Journal of Software Engineering Ampere*, 3(3), 170–185. <https://doi.org/10.51519/journalsea.v3i3.267>
- [43] Hameed, T. H., & Sadeeq, H. T. (2022). Modified Vigenère cipher algorithm based on new key generation method. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(2), 954–961. <https://doi.org/10.11591/ijeecs.v28.i2.pp954-961>
- [44] Pujeri, Dr. U., & Pujeri, Dr. R. (2020). Symmetric Encryption Algorithm using ASCII Values. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(5), 2355–2359. <https://doi.org/10.35940/ijrte.E5980.018520>