International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 5, July-August 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Data Security by AES (Advanced Encryption Standard)

Prateek Goyal[1], Ms. Shalini Bhadola[2], Ms. Kirti Bhatia[3]

[1]M Tech Student, [2]Assistant Professor, [3]HOD,
[1, 2, 3]Computer Science & Engineering, Sat Kabir Institute of Technology and Management Bahadurgarh (HR) Affiliated by Maharshi Dayanand University (Rohtak), Haryana, India

ABSTRACT

Now a days with the rapid development of multimedia technologies, research on safety and security are becoming more important. Multimedia data are generated and transmitted through the communication channels and the wireless media. The efficiencies of encryption based on different existing algorithms are not up to the satisfactory limit. Hence researchers are trying to modify the existing algorithm or even develop new algorithms that help to increase security with a little encryption time. Here in this paper, we have furnished a new technology to modify the AES algorithm which gives more security with a little encryption time and which can be used to encrypt using 128-bit key. Theoretical analysis on the proposed algorithm with the existing reveals the novelty of our work. Here we have proposed a technique to randomize the key and hidden the key data into an encrypted digital image using the basics concept of cryptography and also using the concept of digital watermarking, the concept of key-hide has also been encrypted. We have also proposed a new technique to reposition the pixels to break the correlation between them. So, the proposed scheme offers a more secure and cost effective mechanism for encryption. Next on the AES criteria list: good performance. Widespread market adoption will require reasonably good performance on a variety of platforms, ranging from easy-tocrack smart cards to the largest servers. Good algorithm performance includes speed for the encryption and decryption process as well as the key schedule.

KEYWORDS: *AES algorithm, Cryptography, Decryption, Encryption*

How to cite this paper: Prateek Goyal | Ms. Shalini Bhadola | Ms. Kirti Bhatia "Data Security by AES (Advanced Encryption Standard)" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-5, August 2021, pp.1417-1421, URL: www.ijtsrd.com/papers/ijtsrd45073.pdf

IJTSRD45073

INTRODUCTION

1. Data Security

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. Data security is also known as information security (IS) or computer security.

Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers. One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three

different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a **symmetric-key algorithm**, meaning the same key is used for both encrypting and decrypting the data.

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first and convenience-oriented applications aimed at mobile phone users (termed mobile tagging).

designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) to efficiently store data; extensions may also be used.

The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, general marketing, and much more.

A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted; data is then extracted from patterns present in both horizontal and vertical components of the image.

The QR code system was invented in 1994 by Denso Wave. Its purpose was to track vehicles during manufacture; it was designed to allow high-speed component scanning. Although initially used for tracking parts in vehicle manufacturing, QR codes now are used in a much broader context, including both commercial tracking applications one of the most-used types of two dimensional barcode.

QR codes may be used to display text to the user, to add a vCard contact to the user's device, to open a Uniform Resource Identifier (URI), or to compose an e-mail or text message. Users can generate and print their own QR codes for others to scan and use by visiting one of several paid and free QR code generating sites or apps. It has since become

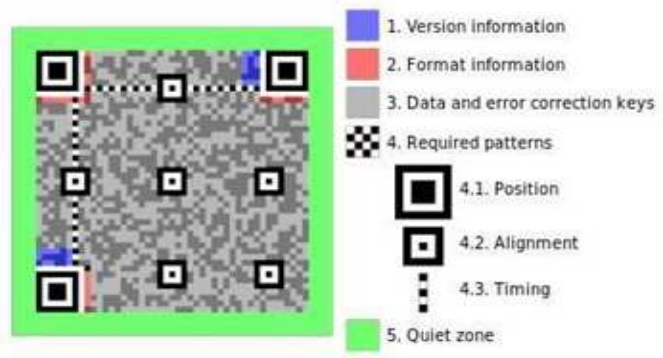


Figure 1.1 QR Code

Originally designed for industrial uses, QR codes have become common in consumer advertising. Typically, a smart phone is used as a QR code scanner, displaying the code and converting it to some useful form (such as a standard URL for a website, thereby obviating the need for a user to type it into a web browser).

It can also be used in storing personal information for use by organizations. An example of this is Philippines National Bureau of Investigation (NBI) where NBI clearances now come with a QR code. Many of these applications target mobile-phone users (via mobile tagging). Users may receive text, add a vCard contact to their device, open a Uniform Resource Identifier (URI), or compose an e-mail or text message after scanning QR codes.

2. CRYPTOGRAPHY:-

Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data secret and for verifying data integrity.

AES encryption works Each **cipher** encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192and 256-bits, respectively. The Rijndael **cipher** was designed to accept additional block sizes and key lengths, but for **AES**, those functions were not adopted.

The features of AES Algorithm are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys•
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

3. DECRYPTION:-

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with unencrypting the data using the proper codes or keys.

ICSF supports these two main types of cryptographic processes:

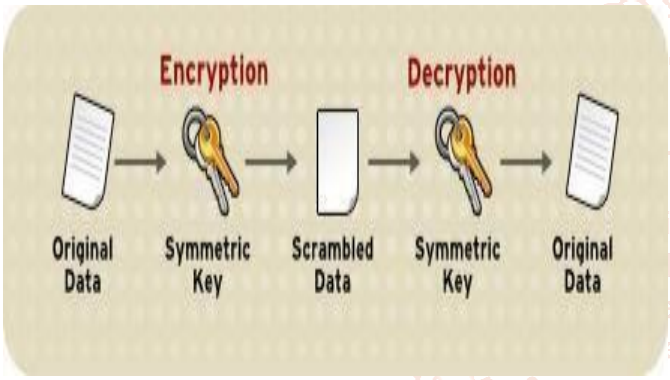
- Symmetric algorithms, in which the same key value is used in both the encryption and decryption calculations
- Asymmetric algorithms, in which a different key is used in the decryption calculation than was used in the encryption calculation

Symmetric Cryptography Asymmetric Algorithm or Public

Key Cryptography

4. AES ALGORITHM:-

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes.



5. ENCRYPTION:-

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudorandom encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed

encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

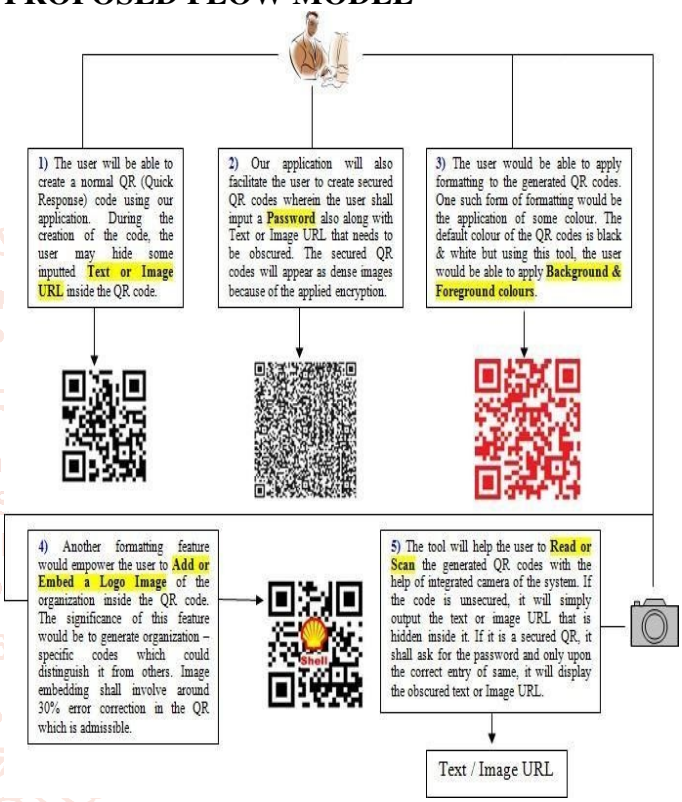
6. PROBLEM STATEMENT

QR CODES:

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) to efficiently store data; extensions may also be used.

The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, general marketing, and much more.

PROPOSED FLOW MODEL



A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted; data is then extracted from patterns present in both horizontal and vertical components of the image.

Before developing the application, we assumed that there is a manufacturing organization which has a multi – dimensional objective of dispensing vital information and data to the public in a more cost – effective, secure and obscured way. As the organization makes the use of text or image content for the distribution of data or information, it now wishes to make the use of graphic for achieving same.

Our objective behind developing this application is to realize the significance of data, information and distribute it in such an obscured or non – obscured

way so that authorized people should be able to view it. At the same time, the data should remain publicly accessible but it should either be accessible to the authorized personnel or the ones who have the appropriate tools to view it.

Through our application, we aim to hide text data and images (in the form of their corresponding URLs) by a use of a graphic called *Quick Response Codes or QR codes*. The main advantage of using a graphic is that it can obscure big chunks of vital data conveniently along with some formatting and optimizing hard disk space. There are

similar graphics available in the market called *Bar Codes* through the use of which one can hide data.

But using our application, we plan to eliminate certain disadvantages associated with the usage of bar codes and wish to improvise the distribution of data in a secured and hidden manner by applying some formatting, security options and scanning operations in our tool.

7. ADVANTAGES AND DISADVANTAES:

ADVANTAGES

1. As it is implemented in both hardware and software, it is most robust security protocol.
2. It uses higher length key sizes such as 128, 192 and 256 bits for encryption.
3. It is most common security protocol used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage,etc.
4. It is one of the most spread commercial
5. and open source solutions used all over theworld.
6. For 128 bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

8. APPLICATIONS:

QR USING THIS APPLICATION:

The user will be able to generate a QR code using 2 options namely

- Text
- Image

1. Under “Text” option, the user will input some text (in a text field) that needs to be hidden inside the QR code.
2. Under “Image” option, the user will input web URL of the image location.
3. After that, we will ask the user whether he wants to encrypt the QR code. If the user selects “Yes”, we shall ask for a password in a text field in order to encrypt the QR code. Once the password is inputted, the encrypted QR code shall be generated. If the user selects “No”, the QR code will be generated without a password and displayed on the screen.
4. After that, we will ask the user whether he wants to encrypt the QR code. If the user selects “Yes”, we shall ask for a password in a text field in order to encrypt the QR code. Once the password is inputted, the encrypted QR code shall be generated. If the user selects “No”, the QR code will be generated without a password and displayed on the screen.
5. Once a QR code is generated, it will be displayed on the screen as well as saved as an image file at a specific destination folder/directory within the hard drive of the user PC.
6. After the QR code is generated, the user will be able to scan it through the “Scan” option present in our application. Under the "Scan" option, the integrated camera of the laptop shall turn ON. The user will put a printed out image of the stored QR codes before the camera for capturing.
7. If the QR code is encrypted, it will ask for a password for decryption on the PC screen. Once the correct password is inputted, it will show the text or URL that is hidden inside the QR code. But if the QR code is not encrypted, it won’t ask for a password and upon “Scan”, it will directly show the text or URL hidden inside it.
8. The encrypted QR codes will only be scanned by our application. In other words, if some another 3rd party QR code scanning application scans it, junk characters will be displayed. But if scanning is done through our application, the password will be asked first and only upon its correct entry, the hidden text or URL will be displayed.
9. If the URL is displayed after scanning a QR code, there should be an option to visit that URL.
10. There will “QR Customization” options present in our application namely,

- Apply Color
- Add Logo
- Add Label.

9. CONCLUSION

Businesses are beginning to use QR codes in large U.S. cities to promote their brands and entice customers in new ways. They are following the trends that show we may soon have a critical mass of the population with the equipment in their hands to leverage this technology. Big name brands like Ralph Lauren and Calvin Klein are beginning to embrace QR codes as a key component of their marketing

efforts in magazine ads and posters. Luxury Manhattan retailer Michael C. Fina recently debuted its "mobile storefront" on 5th Avenue with QR codes to celebrate a line of featured designer jewellery.

In July, a giant QR code was displayed on the Thomas Reuters billboard in Times Square. When scanned, the code took users to a well-designed mobile site where they could watch the "Be the One" campaign video and sign a petition to help clean up the Gulf oil spill. More major brand use of QR codes is in development (television ads are coming), which will raise awareness and eventually lead to their mainstream use.

FUTURE SCOPE

Under the future scope,

- We may further enhance this application to formulate encrypted QR codes with multi – level encryption techniques.
- The QR codes could be integrated with different biometrics and ERP applications for the exchange of data between B2B and B2C in a secured environment with the use of hardware
- We may utilize QR codes for their storage on cloud as encrypted images which have data stored in them that is further encrypted using several encryption techniques.

10. REFERENCES

[1] M. Kurdziel, J. Fitton, "Baseline Requirements for Government & Military Encryption Algorithms" , Proc. IEEE, Mil. C

[2] Ferguson, N., & Schneier, B. (2016). Practical Cryptography , proc. IEEE ,New York: John Wiley & Sons.

[3] Trappe, W., & Washington, L.C. (2015). Introduction to Cryptography with Theory, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.

[4] H. Trang, N. Loi, "An efficient FPGA implementation of the Advanced Encryption Standard", *Computing and Communication Technalogies Research Innavation and Visian for the Future (RIVF) 2012 IEEE RIVF International Conference on*, March 2016. From: https://ieeexplore.ieee.org/document/7905466/

[5] Designer QR Codes; Ensuring the "beep" Kevin Berisso, OHIO University, Spring 2013.

[6] QR Codes and Security Solutions, International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012].