JURNAL PENDIDIKAN TEKNOLOGI KEJURUAN
Vol. 3, No. 4 November 2020 P-ISSN: 2621-3273
E-ISSN: 2621-1548

Implementation of AES-192 Cryptography and QR Code to Verify The Authenticity of Budi Luhur University Student Certificate

Wahyu Pramusinto[1], Bruri Trya Sartana[2], Sri Mulyati[3] dan Safrina Amini[4]
[1]Manajemen Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[2]Sistem Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[3,4]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Wahyu.pramusinto@budiluhur.ac.id[1]

Abstract— Nowadays a letter can easily be falsified and used for things that are not appropriate. Budi Luhur University has a work unit that serves student requests for certificate of active students and certificate of graduation. Students need that certificate for apply a job or get a scholarship. To prevent the falsification of letters, a system using PHP programming language and MariaDB database was used to verify the letters. The certificate released by this system will be equipped with a QR Code containing the URL with parameters that have been encrypted with the cryptographic method AES-192. If accessed, this URL will display the data number, name, letter number and date of the letter. The recipient letter can verify the authenticity of the letter by comparing the data in the letter with the data in the system. If the two data are the same, the letter is the original. Based on test results, this system can be used to guarantee the authenticity of a letter.

Keywords: **Cryptography, QR Code, AES-192, letter verification**

I. INTRODUCTION

Crimes regarding falsification or abbreviated as crimes of forgery are crimes in which they contain an element of an untruth or false state or an object, something that appears from the outside as if it is true even though it is true. actually contradicts the truth (Ismail, 2018). The crimes of counterfeiting are grouped into 4 groups, namely crimes of perjury, money counterfeiting, crime of stamp and mark forgery, crime of letter forgery.

The development of the criminal act of letter or document forgery basically has experienced extraordinary developments in terms of qualifications and types of documents (Zulfa, E.A., 2018). The certificate of passing was also falsified and included violating the Criminal Code Article 263 paragraph 2 Regarding Letter Forgery (Tirto, 2019).

A letter that has been printed can easily be faked and used by others for things that are not supposed to. This occurs because there is no method to verify the authenticity of the printed letter.

Budi Luhur University has a work unit that serves student requests to print active student certificates and graduation certificates. Usually this certificate is needed by students to get scholarships and to apply for jobs.

The problem that occurs is that this printed certificate is likely to be forged. Therefore, we need a method to guarantee the authenticity of this certificate.

To prevent the forgery of this certificate, a system was created using the PHP programming language and the MariaDB database which is useful for securing letter. This certificate is equipped with a QR code containing a URL with parameters that have been encrypted with the AES-192 cryptographic method.

The purpose of this research is to build an application to print graduation certificates and active student statements equipped with a QR code that has been encrypted with AES-192 to verify the authenticity of the letter.

In general, QR codes are in the form of small white rectangles with black geometric shapes. The information encoded in the QR Code can be in the form of a URL, phone number, SMS message, V-Card, or any text. QR Code can also store image data (Nugraha and Munir, 2011)

Figure 1 is an example of a QR Code with a message containing the text of AES-192

Cryptography Implementation and QR Code for Verification of the Authenticity of Budi Luhur University Student Certificate

Figure 1. An example of QR Code

In general, cryptography is the science and art of encryption that aims to maintain the security and confidentiality of data. Cryptography also does not mean only providing information security, but cryptography is more about the techniques (Bhaudhayana and Widiartha, 2015).

Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to secure data. The AES algorithm is a symmetric block ciphertext that can encrypt (encipher) and decrypt (decipher) information. Encryption changes data that can no longer be read called ciphertext, on the other hand decryption is changing the ciphertext data into its original form known as plaintext. The AES algorithm uses 128,192 and 256 bit cryptographic keys to encrypt and decrypt data in 128 bit blocks.

Previous research entitled Development of Certificate Authentication Authentication Method Using QR Code Images made an application for letter security. This study adds a QR Code to the certificate to make it easier to detect the authenticity of certificate ownership information via mobile devices. From this research, it can be concluded that the QR Code can be used quickly to verify the certificate of a graduate of Stikubank UNISBANK University quickly and accurately. However, the authors suggest that it is necessary to think about internet security to encrypt diploma data (Ardhianto *et all*, 2016).

Another research on QR Code that has been conducted is entitled Development of QR Code Generator Application and QR Code Reader from Image-Shaped Data. This application is successful in making QR Code with image data, but it is considered not feasible to be implemented in the real world because of its large size and difficult to read (Nugraha and Munir, 2011).

The research entitled Certificate Verification System Using Qrcode at the Central Event Information creates a certificate security system with a QR Code. Certificates that are printed through this system are added with a QR Code for security. QR Code can be scanned using QR Code Reader on smartphone. If the QR Code is successfully scanned, it will be redirected to a verification page which will provide detailed information regarding certificate ownership, type of activity, and activity time. Students can also view certificates in digital form which can be scanned and verified so that if there is damage to the certificate it has been printed, the student still has the digital certificate document (Febriyanto *et all*, 2019).

Research entitled Securing Digital Land Certificates using the Digital Signature SHA-512 and RSA has developed a digital signature mechanism for PDF files. The cryptographic algorithm used in this study is RSA. The system created is very useful because it can quickly identify the manipulation process of certificate documents so that it can solve the problem of forgery of land certificates by BPN or PPAT without the need for a more time consuming manual checking process (Refialy *et all*, 2015).

Research related to securing academic documents entitled Model Digital Signature on Academic Formal Documents adds digital signatures to academic documents. This study aims to solve the problem of the length of time it takes to validate academic documents by developing a model signature on formal academic documents at Raharja University (Henderi, Rositawati, Romansyah, 2020).

The research entitled Implementation of AES 256 Cryptographic Algorithm and LSB Steganography Method on Bitmap Images creates a security application for image files. This study combines AES-256 cryptography and LSB steganography. According to this study, both methods can be implemented in securing image files whose confidentiality is strictly maintained (Ardhianto *et all*, 2016).

Research using QR Code has been made with the title Using QR Code to Simplify the Goods Census in Cilegon City. In this study, made a QR code that is printed on the item identity label. This QR Code can be read through a QR Code Reader on a smartphone, so that data collection can be carried out properly and easily (Pramudyo, 2015).

The research entitled Email Security Using the Advanced Encryption Standard (AES) Algorithm, Rivest Cipher 4 (RC4) and Caesar Cipher uses 2 encryption methods to encrypt email messages. Emails that have been sent are converted into cipher text and can be decrypted using the specified key (Pramusinto, Putra, 2018).

Another research related to data security has been made in a study entitled Web-Based File Security Application with AES 192 Cryptography Methods, RC4 and Huffman Compression Methods. In this study, it was concluded that the application made was successful in securing files so that they

could not be read. This application can also restore files that have been encrypted to be like before (Pramusinto, Wizaksono, Saputro, 2019).

II. METHOD

The steps used in conducting this research can be seen in Figure 2

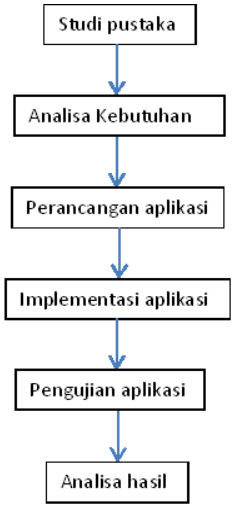


Figure 2 Reasearch Methods

The literature study stage is carried out by collecting, reading and also understanding journals, papers and other references in order to obtain the information needed to support this research.

At the needs analysis stage, an analysis of what is needed in making the application is carried out. In this stage, interviews are also conducted with related parties. At the application design stage, a description of the application will be made, database structure creation and selection of the programming language used.

At the application implementation stage, a web-based application is made with the PHP program language to verify the authenticity of the certificate. Implementation of QR Code and cryptography AES-192 used on the letter to be printed.

At the application testing stage, testing of the application that has been made is carried out, and evaluates if there are still errors and deficiencies. The application is tested directly by the related parties so that they can find out whether the application made is on demand or not.

The final stage is to analyze the results of applications made based on several input variables.

III. RESULT

A. Hardware and Software specifications

In order for the application to run properly, the device specifications used for implementation must also support it. The hardware used in this application test is a laptop with an Intel i53570 Processor specification, 4 GB DDR3 RAM, 2GB DDR5 VGA HD7850, 14 "1920x1080 monitor, keyboard, mouse and 1 TB hard drive. For testing QR Code reading, an Android-based smartphone is used.

The software or software used in this application developer is the Windows 10 64 bit Operating System, XAMPP Version 5.6.23 (PHP, Apache, MariaDB), Google Chrome Browser, CodeIgniter Library as a PHP framework, QRlib Library for creating QR Code, FPDF library to create PDF files, Foxit PDF Reader, and Sublime Text. To test QR Code reading, a QR Code Reader application installed on the smartphone is required.

B. Class Diagram

This application requires a database to store the information contained in it. In Figure 3 you can see the class diagram for the application that has been made

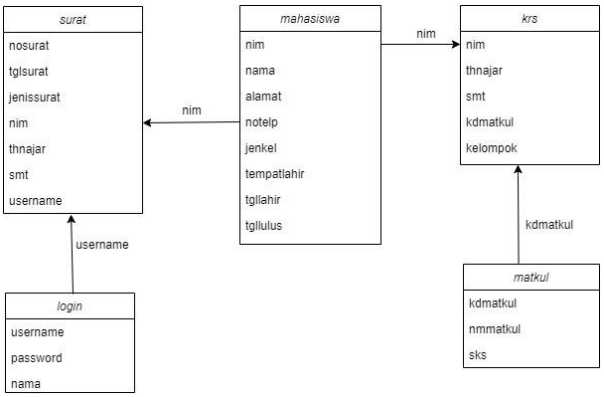


Figure 3 Class Diagram

In the class diagram, there are several tables that are needed by this application. The login table is used to store admin data that can print a certificate. The student table stores data for all students. Matkul table stores data for all courses. The KRS table contains data on the courses taken by students. The letter table is used to store letter data that has been created.

C. How the Application Works

To use this application, unit officers must first log in to enter the admin page. The admin must fill in the student's name, academic year and semester before printing a graduation certificate or active student certificate.

Before the letter is printed, student data will be checked first. To make an active certificate, checks are made to the KRS table to see if the student is still actively studying. Meanwhile, checking the pass certificate, checking is carried out to the student table

to see whether the graduated field has been filled or not.

If the data is declared valid, the letter data will be stored in the letter table. The letter type and letter number will be AES-192 encrypted and included in the QR Code in the letter. This QR Code can be read by the QR Code Reader application on a smartphone. When a QR Code is scanned, it contains a URL to check the authenticity of the letter. The URL contains parameters in the form of letter number and type of letter that has been encrypted with AES-192.

If the URL is clicked, the system will decrypt the parameters in the URL with AES-192. The letter number will be checked whether it is in the letter table. If not found, the system will display a fake letter message. If there is, the system will display the letter number, letter type, letter date, student ID and name on the screen. Authenticity checking is done manually by comparing the data on the screen with the data on the letter.

D. Flowchart

Flowchart of the process of printing a certificate can be seen in Figure 4

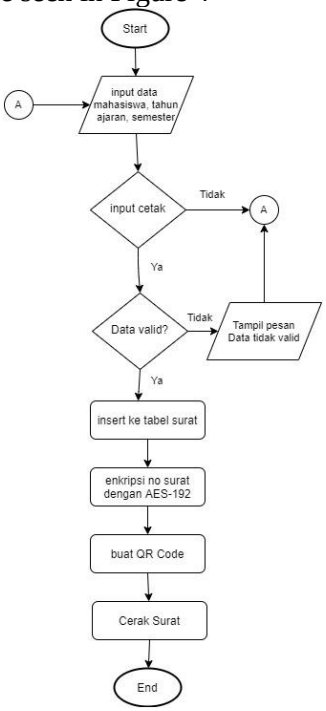


Figure 4 Letter printing flowchart

Flowchart of checking the authenticity of letters can be seen in Figure 5

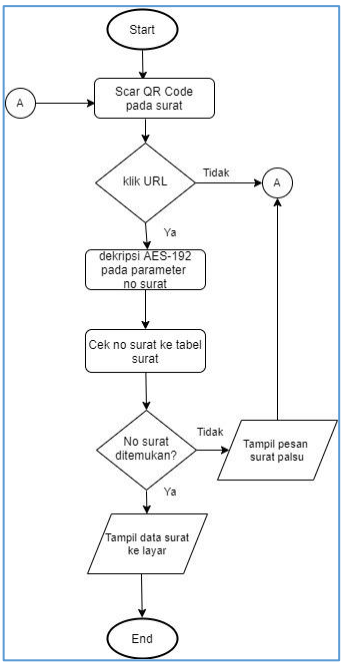


Figure 5 Letter authenticity check flowchart

E. Screen Display

In Figure 6 you can see the admin login screen display. The admin in this application is the officer who will print the letter.

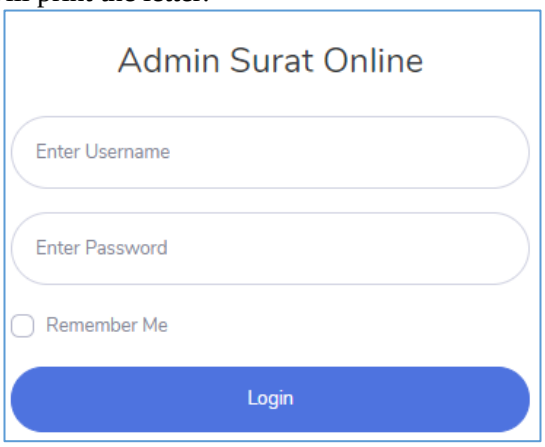


Figure 6 Login Page Views

In figure 7 you can see the screen display for printing letters. Officers must select student data, academic year and semester. Furthermore, the system will check whether students can print letters or not.

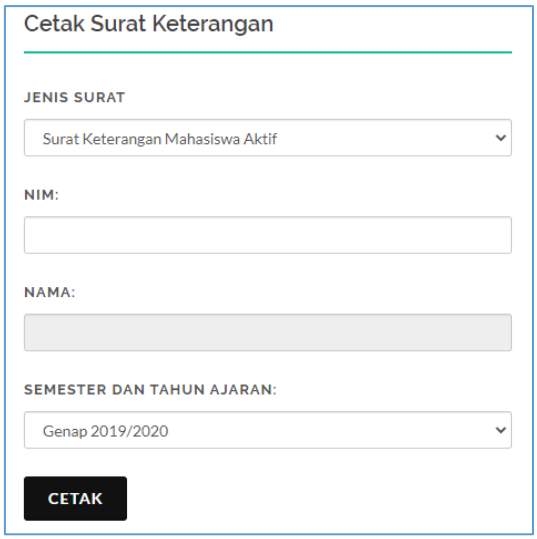
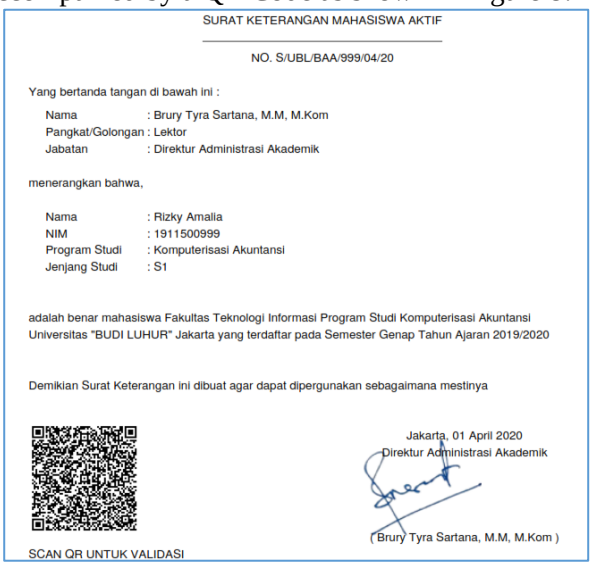


Figure 7 Print Letters page

If an Active Student Certificate is selected, an active student certificate will be printed in PDF form accompanied by a QR Code as shown in Figure 8.



SURAT KETERANGAN MAHASISWA AKTIF

NO. S/UBL/BAA/999/04/20

Yang bertanda tangan di bawah ini :

Nama : Brury Tyra Sartana, M.M, M.Kom
Pangkat/Golongan : Lektor
Jabatan : Direktur Administrasi Akademik

menerangkan bahwa,

Nama : Rizky Amalia
NIM : 1911500999
Program Studi : Komputerisasi Akuntansi
Jenjang Studi : S1

adalah benar mahasiswa Fakultas Teknologi Informasi Program Studi Komputerisasi Akuntansi Universitas "BUDI LUHUR" Jakarta yang terdaftar pada Semester Genap Tahun Ajaran 2019/2020

Demikian Surat Keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya

Jakarta, 01 April 2020
Direktur Administrasi Akademik

(Brury Tyra Sartana, M.M, M.Kom)

SCAN QR UNTUK VALIDASI

Figure 8 Display Print Certificate of Active Student

If a Pass Certificate is selected, a pass certificate will be printed in PDF form accompanied by a QR Code as shown in Figure 9

SURAT KETERANGAN LULUS

NO. S/UBL/BAA/004/07/2020

Yang bertandatangan di bawah ini, Direktur Administrasi Akademik menerangkan bahwa:

Nama : Rizky Amalia
NIM : 1911500999
Tempat / Tgl. Lahir : Jakarta, 1988-08-21
Alamat : Jalan Karyawan 2 RT 007/05, Kel Karang Tengah, Kec

adalah mahasiswa Universitas Budi Luhur Jakarta :

Fakultas : Fakultas Teknologi Informasi
Jenjang Pendidikan : S1
Program Studi : Komputerisasi Akuntansi

yang sampai tahun akademik 2019/2020 telah menyelesaikan 144 SKS termasuk KKP (Kuliah Kerja Praktek) dan tugas akhir. Sampai saat ini mahasiswa tersebut sedang menunggu waktu wisuda dan penyerahan ijazah

Demikian Surat Keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya

Jakarta, 01 April 2020
Direktur Administrasi Akademik

(Brury Tyra Sartana, M.M, M.Kom)

SCAN QR UNTUK VALIDASI

Figure 9 Display Print Certificate of Active Student

The QR Code in the letter contains a URL that checks the authenticity of the letter. The contents of the QR Code when read using the QR Code reader application as shown in Figure 10

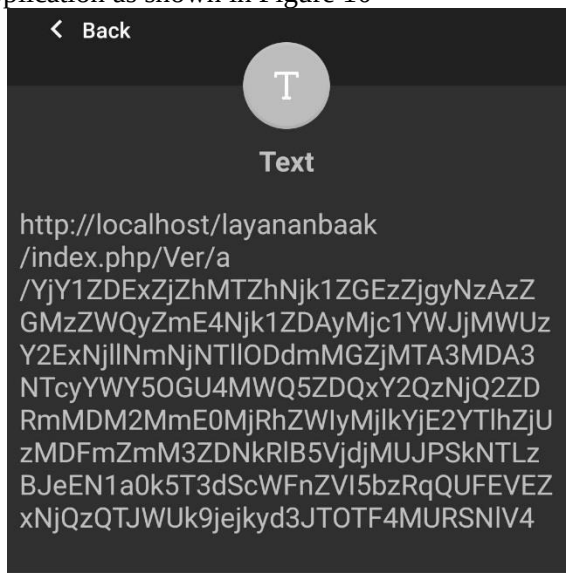


Figure 10 The contents of the QR Code are read with the QR Code Reader Application

The encrypted part contains the letter type and letter number. Encryption using AES-192 by adding the base64_encode function so that there are no characters other than letters and numbers in the URL. When the URL is opened in the browser, it will display the letter number, letter date, letter type, ID and name information. If the data on the screen is clogged with the data on the physical letter, that means the letter is valid. Display of valid certificate information can be seen in Figure 11

Figure 11 Information Display Certificate

If the parameters in the URL are changed, during the decryption process a letter number that is not in the database will be generated, so the display will appear as shown in Figure 12.

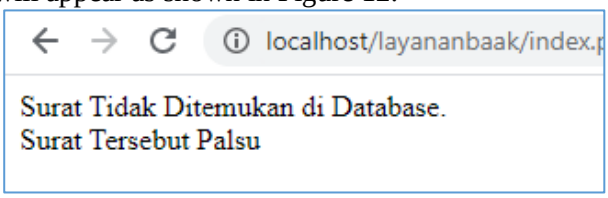


Figure 12 Fake Letter Information Display

F. Testing Table

Data encryption trials using AES-192 and base 64_encode can be seen in table 1.

Table 1 Encryption Trial Table

Jenis Surat		No Surat	Hasil Enkripsi
Surat Lulus	Ket	S/UBL/BAA/123/04/20	N2U5N2Q2ODllYWY2ZDQxMzYzOTE5NTRhM2JjMmJmYjExOWI5ZjNjOGYxZGI5Zjc1OGYzODk3MTZiZGVmYTVkZDU4Mzk2NTk2NmIwOTM2OWI3NGQzMzU4ZTU5OWY1ZGZlYTI4ZGY2NzcwZTlkODlmNTVlMmE4N2YwZmJjYWJkNTcxWlJCK09SWE8xdDFHUk43MHZKS3p1ejRlVllKZjZEUmRIRGFhWXgwa1J5UDFvaXBQaC9mTFpINWhqVk16SkRp
Surat Lulus	Ket	S/UBL/BAA/456/04/20	MjcxNDk3NzdhYTFjNjhhOWYzYjg2ZmM0YmU5MWIzNzc4NzdiOThjODM0NjRkNjMwYWI3ODExNWJhN2JhOTAyYTk5ZmFjY2IyMmIyNWE5ZGIyOTEyNDJiOTQ2NTIxNGMyNWE4MTg3NmIxODc1ODkwYTMzNjYyMzQxOTBmYTIwN2ZZK2VmeVdjdHBzcDZpK2NYRFpqU3FSODB1M2tTQmpIQml3R1NHYkZOODhvTGVpZnl3c3g1eUh6dythZGFuSFpw
Surat Lulus	Ket	S/UBL/BAA/789/04/20	Njg0ODY1YjFiZDM0MjYxMDE1OTM3NmFkMjA3NmJlN2NjZmZjOGVlNzZiMmY0ZDFmM2ZkNTZlMDg2Mzc1YmMyOTY3YTkyZGNjNmY1Y2E4MmE0OTQ5MjkwYjBhNGY3OGE2ODczOGY2YzI5N2ZjZGFjYWQ2MDZhMmVjZWU2NzI4NmVtSlV1ZUNIMzhyRWk3cVVXMXlaVVRTN2pVY3JsR3lnd1pyZFdNSWgrZWxadE1TVUxQQm55cE13WWMzTExkZjZK
Surat Aktif	Mhs	S/UBL/BAA/111/04/20	NmE3M2IxMmQ5N2U1N2JjODM3YWJmM2RlMDBkMDI4YmQwOTgyZWQ5N2U4MjUyMzJkMzFmOTA5NDhiMTA0OGQ3YjNmNjZmZGU0ODc0NjA0NzdmZWFiZjUwNmNiZDljZmEwYzI3NzJmOTdmYmFlMzY1NGZiOTcwODg4MDUxNmY4ZmJQU3llRjdtT2hXNThaVp0NEF5Qk9uYXFQaEMwZEREM2xXQXRGcm9MOUVqQzRRbHorNWNQS3NVa1RkbXZzS2kv
Surat Aktif	Mhs	S/UBL/BAA/222/04/20	ODY2ZTMwMTMxZmY3Y2M5N2UyODcxYmNjMDc4OGJlZDM5MmYzYmJhMmMwZDc5MTFhYWVjMDI3ZTQ5ODBjNGEwNTJhMzQ1N2I5OTZjMWMyYWYxOGFiNTJmZTAyMTc2ZWY1OWRkY2MzYjcxNzEyNTdkZmFkZTZjMjk3MzNjMTNjZTlmUVlFRkpoVmFwbWc3VGNWRlNTR2tnMG9yOTkwd3BYTmNuYWxScXNZMUs0NnhZUVNUWkZtbUNJaXlzcjlqdVJv
Surat Aktif	Mhs	S/UBL/BAA/333/04/20	ODA4Zjc1MTM3Y2M2Nzc0ZTQ2ZDY5NmQ1YjEzN2FjMmM1YjU0NWEyYzgyZDZhOGQzMTJiNjgwOGQzZDQxNTYwM2JiYmIzOTk4MjRlMTlhNzk0NmE0ZmVlMjM4MTU5OWJlYTU1OTJjMjM4ZGI2OWVkMjQ4NzE1YmM2ODEzODhjOThjdW9mc3ZVZ1JHNlFJMkFqditLd2ZrMzY1Q2NyRjc1RGRQMGFWNTdWSWVmWE1KU3RaMFRXeDVQR2Y2RkNnSzk2

In table 2, you can see the results of the RR Code reading test using several QR Code Reader applications on an Android Smartphone.

Table 2 QR Code Reading Trial Table

Application Name	Apps Developer	QR Code Reading Results
QR & Barcode Reader	TeaCapps	It can be read well
QR & Barcode Scanner	Gamma Play	It can be read well
QR Code Reader	BACHA Soft	It can be read well
Free QR Code Scanner App	Application4u	It can be read well
QR Code Reader & Scanner App for Android	Kaspersky Lab Switzerland	It can be read well
QR Code Reader	LookandFeel Lab	It can be read well

From the test results, it can be seen that QR Code can be read properly using several QR Code Reader applications on an Android smartphone

IV. CONCLUSION

Based on the research that has been made to verify student certificates, the following conclusions can be made

a. Applications made can be used to secure graduation certificates and active student certificates.
b. QR Code printed on letters can be easily read by the QR Code Reader application on a smartphone.
c. The process of verifying the authenticity of student certificates can be done quickly and easily.

REFERENCES

Ardhianto E., Handoko, W.T, and Wahyudi, W.N., 2016. Pengembangan Metode Otentikasi Keaslian Ijasah Dengan Memanfaatkan Gambar Qr Code. *Jurnal Teknologi Informasi Dinamik.*, vol. 20, no. 2, p. 106-114.

Bhaudhayana, G. W. and Widiartha, I. M., 2015. Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB Pada Gambar Bitmap. *Jurnal Ilmu Komputer Universitas Udayana*, Vol 8 no 2, pp. 15–25.

Digital Signature Pada Dokumen Formal Akademik. *Jurnal CICES*, Vol 6, No. 1, pp. 22-32.

Febriyanto,E., Rahardja, U., Faturahman, A., and Lutfiani, N.,2019. Sistem Verifikasi Sertifikat Menggunakan Qrcode pada Central Event Information. *Techno.Com*, vol. 18, no. 1, pp. 50–63.

Henderi, Rositawati, D., Romansyah, P, 2020. Model Digital Signature Pada Dokumen Formal Akademik. *Jurnal CICES*, Vol 6, No. 1, pp. 22-32.

Ismail, 2018. Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Pemalsuan Akta Nikah. *Jurnal Hukum Samudra Keadilan*, Vol 13, no. 1, pp. 153-175.

Nugraha, M.P., and Munir, R., 2011. Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image. *Konferensi. Naional. Informatika. – KNIF 2011*, Bandung, 23 November 2011.

Pramudyo, A.S., 2015. Penggunaan QR Code Untuk Mempermudah Sensus Barang di Kota Cilegon. Konferensi Nasional Sistem Informasi 2014, Makassar, 27 Februari 2014.

Pramusinto, W., Putra, R.A, 2018. Pengamanan Email Dengan Algoritma Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) dan Caesar Cipher. Prosiding Seminar Nasional Sains dan Teknologi 2018, Semarang, 18 Juli 2018.

Pramusinto, W., Wizaksono, N., and Saputro, A., 2019. Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman. *Jurnal BIT* , vol. 16, no. 2, pp. 47–53

Refialy, L., Sediyono, E., and Setiawan, A., 2015. Pengamanan Sertifikat Tanah Digital menggunakan Digital Signature SHA-512 dan RSA. *Jurnal Teknik Informatika dan Sistem Informasi.*, vol. 1, no. 3, pp. 229–234

Tirto, 2019. *Kasus Ijazah Palsu, Pelawak Nurul Qomar Divonis 17 Bulan Penjara*. [online]. Retrieved from https://tirto.id/kasus-ijazah-palsu-pelawak-nurul-qomar-divonis-17-bulan-penjara-eluP. [Accesses 1 April 2020].

Zulfa, E.A., 2018. Menghancurkan Kepalsuan (Studi Tentang Tindak Pidana Pemalsuan dan Problema Penerapannya). *Jurnal Hukum & Pembangunan*, Vol. 48, no 8, pp. 345-360.