E-PASSPORT SECURITY USING ADVANCED ENCRYPTION STANDARD (AES)

Nik Shahidah Afifi Mohd Taujuddin, Mohd Helmy Abd Wahab and Christina a/p Hanif
Faculty of Electrical and Electronic Engineering, Tun Hussein Onn University of Malaysia, Johor, Malaysia.
Email: shahidah@kuittho.edu.my

ABSTRACT

This paper presents basic design approach for securing the information in the E-passport by using Advanced Encryption Standard (AES) algorithm. AES is a new cryptographic algorithm that can be used to protect electronic data. Furthermore, AES is an iterative; symmetric-key block ciphers that can use keys of 128, 192, and 256 bits, and encrypt and decrypt data in blocks of 128 bits (16 bytes). An algorithm successfully implemented using Visual Basic. The purpose of AES algorithm is to protect the information stored in E-passport. E-passport is the new version of the conventional passport that usually contain the holder's profiles such as photograph, signature, date of birth, nationality, and sometimes other means of individual identification. The E-passport is very similar to the previous passport, but the different only having an embedded microchip in the centre page but for this prototype, microchip will be replaced with the memory stick.

Keyword: AES, E-Passport, embedded, microchip, data

INTRODUCTION

The Advanced Encryption Standard (AES) is proven by a national Institute of Standards and Technology (NIST) for encryption of electronic data.[1] It is expected to become the accepted means of encrypting digital information, including financial, telecommunications, and government data. In this research, AES used to protect the information in E-passport. This E-passport is the new version of the conventional passport. But in this project a collective passport will be used. The collective passport is used for a purpose of travelling in groups between five to twenty persons to ASEAN country only. The major purpose of doing this application is to secure the data in the E-passport. The security system that has been used nowadays is currently not effective because the data in the E-passport can be hacked or stolen. Below are a few attackers in E-passport:

a) Clandestine scanning
b) Clandestine tracking
c) Skimming and cloning
d) Eavesdropping
e) Biometric data-leakage
f) Cryptography weakness

The objectives of the research are as follows:

1 To build an E-passport prototype
2 To enhance the security of the E-passport
3 To ensure the confidentiality of the information in E-passport

A prototype of the E-passport has been created with an embedded memory stick. A memory stick with the capacity of 64MB is used to store the user personal information. Besides that, the database for ten users including the personal information such as holder’s name, photograph, date of birth, nationality, E-passport number and E-passport expiry date are stored using Microsoft Access 2000 using Visual Basic 6.0 as interface. AES algorithm is used as encryption algorithm to secure the information in the E-passport.
RELATED WORK

TRADITIONAL PASSPORT

A passport is a formal identity document or certification issued by a national government that identifies the holder as a national of a particular state, and requests permission, in the name of the sovereign or government of the issuing country, for the bearer to be permitted to enter and pass through other countries. Passports usually contain the holder’s name, photograph, date of birth, nationality, passport number and passport expiry date.

E-PASSPORT

The E-passport is very similar to the previous passport, only differ in having an embedded microchip in the centre page and a gold international E-passport symbol on the front cover. [2] The chip embedded in the centre pages stores the holder's informations same like in the conventional passport.

HARDWARE AND SOFTWARE

A 64MB Memory stick and the memory stick reader is used in this project A memory stick is a solid-state electronic flash memory data storage devices used with digital cameras, handheld and laptop computers, telephones, music players, video game consoles, and other electronics. They offer high re-recordability, power-free storage, small form factor, and rugged environmental specifications. The Memory Stick Reader/Writer will allow the Memory Stick cards to be used as portable storage for computers as well as for uploading or downloading data. There are two software that is used in this project. Microsoft Access to build the user’s database and Microsoft Visual Basic 6.0 to build the interface for the system.

CRYPTOGRAPHY

Cryptography is the science of encrypting information. [3] Each of the encryption and decryption process needs the same private key to encrypt and decrypt data. Data input is called plaintext, after going through the encryption process known as cipher text. Data output from the decryption process will be converted back to plaintext.

Advanced Encryption Standard (AES)

AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). For Cipher (encryption), each round of AES (except the last round) consists of fours transformations:

a. $SubBytes$ – a non linear substitution step where each byte is replaced with another according to a lookup table.
b. $ShiftRows$ - a transposition step where each row of the state is shifted cyclically a certain number of steps.
c. $MixColumns$ – a mixing operation which operates the columns of the state, combining the four bytes in each column using a linear transformation.
d. $AddRoundKey$ - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

For Inverse Cipher (decryption) there 4 transformations involved:

a. $InvSubBytes$ – transformation in the inverse cipher that is the inverse of $SubBytes$
b. $InvShiftRows$ - transformation in the inverse cipher that is the inverse of $ShiftRows$
c. $MixColumns$ - transformation in the inverse cipher that is the inverse of $MixColumns$
d. $Inverse$ of the $AddRoundKey$
METHODOLOGY

In order to perform the development of E-passport, the following steps were considered (see Fig. 1)

![Diagram showing the methodology steps]

**Figure 1: Framework of the methodology**

Generally, methodology of the research is divided into 5 phases. These are the phases to design the system

a) Building the user’s database phase
b) Developing the AES algorithm phase
   • Encryption phase
   • Decryption phase
c) Design and build the prototype phase
d) Implementation phase
e) Analyze and testing the prototype phase

The prototype for this project E-Passport is the same as a regular passport with the addition of a memory stick embedded in the first page. The prototype will appear as Figure 3.
DEVELOPMENT

ADMINISTRATOR AUTHENTICATION

The login page is used to authenticate which user can access to the system. In this case, the login page is only applied to the administration because it is used to prevent any unauthorized and suspicious top up process or registration. From the admin system, a person can modify the database. Therefore, only authorized person with the correct password can access the system at administration.

DATABASE DESIGN

Figure 3 refer shows the database of the system. 12 Tables has been created while attributes of tables in the database is shown in table 4.
INTERFACE DESIGN

The Project Explorer Window, often called the Project Window, gives a tree-structured view of all the files in the application. It displays forms, modules (files that hold supporting code for the application), classes (advanced modules), and more. Figure 5 shows the main page for administrator. It has five command buttons that is used to select any menus such as to view bearer’s personal information, travelling information, visas, securing the data and to exit the system. Figure 6 shows the page that displays all the bearers’ personal information while Figure 7 shows the page that display all the bearers’ travelling record. The visas information for all bearers are display in the visa’s page as shown in Figure 8. Bearers’ personal information page, traveling page and visas page come out with a Data Bar. The Data Bar is used to view other bearer’s information. Figure 9 shows the data safety page that contains the program to allow the administrator to encrypt and decrypt the data.

Figure 4: Table properties

Figure 5: Main page for the administrator
Figure 6: Personal’s bearer’s information

Figure 7: Bearer’s traveling record

Figure 8: Bearer’s visas
AES

The AES algorithm is written in VB’s programming language. This language is fairly simple and uses common English word and phrases for the most part [4] Figure 10 shows the page that contains the interface for AES program. There are five command buttons that allow the user to select the file to be encrypted, to encrypt and decrypt data, to view file properties, to view file and to open or start file. This algorithm provides a progress bar as shown in Figure 4.10 to view the quality of the key inserted.

IMPLEMENTATION

The system is tested to ensure that interfaces between software and hardware and that the system meet the requirement.

The E-passport’s prototype contains six pages. Figure 11 below shows the cover of the E-passport’s prototype.
Figure 11: Front cover of the E-passport’s prototype

Figure 12 shows the first page of the E-passport’s prototype. This page contains the passport holder’s information such as name, passport’s Number, Type, Country Code, Date of Issue and Date of Expiry. 64MB memory stick is embedded at the upper right side of this page.

<table>
<thead>
<tr>
<th>Name / Name</th>
<th>Passport No. / Passport No.</th>
<th>No. Pengenalan / Identity No.</th>
<th>Jenis / Tyype</th>
<th>Kod Negara / Country Code</th>
<th>Tarikh dike luarkan / Date of Issue</th>
<th>Tarikh Tamat Sahluaku / Date of Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. AHMAD B. ISMAIL</td>
<td>A1554998</td>
<td>651231155221</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>2. MAZNAH BT. ABU</td>
<td>306016150226</td>
<td>650101155226</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>3. CHOON WILING</td>
<td>309021200513</td>
<td>650212145678</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>4. RAJAN MARK AT. SAMY</td>
<td>650714152051</td>
<td>660714065431</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>5. LIM MAI HIANG</td>
<td>670524010242</td>
<td>670524010242</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>6. MAZITAH BT. DURALIM</td>
<td>70021558447</td>
<td>70021558447</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>7. MUZUL B. IKRAM</td>
<td>633814658555</td>
<td>830103145111</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>8. AMALI B. ADHAM</td>
<td>830721055224</td>
<td>830721055224</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
<tr>
<td>9. SULAIMAN B. SAMAD</td>
<td>830405145812</td>
<td>830405145812</td>
<td>P</td>
<td>MYS</td>
<td>03 MAR 2005</td>
<td>03 DEC 2005</td>
</tr>
</tbody>
</table>

Figure 12: First page of the E-passport’s prototype

Figure 13 below shows the second page of the E-passport’s prototype. It has been stated in this page that the passport holder can enter any country freely in the name of the Supreme Head of Malaysia and have a right to be helped and protected.

Bahawasanya atas nama Yang Di-Pertuan Agong Malaysia serma yang berkenaan supaya membenarkan yang pertubuhan pasport ini untuk dihantar ke tempat-tempat di luar seluruh tanah di Malaysia atau setiap negara yang memerlukan pasport untuk perjalanan sahaja dan memberi apa-apa bantuan dan perlindungan yang perlu kepada yang berasal daripada pasport ini.

These are required and required in the name of the Supreme Head of Malaysia all those who may concern to allow the bearer to pass freely in any part of the world, and to afford the bearer such assistance and protection as may be necessary.

Figure 13: Second page of the E-passport’s prototype

Figure 14 shows the third page of the E-passport’s prototype. This page contains the passport’s number and information where the passport is valid.
Figure 14: Third page of the E-passport’s prototype

Figure 15: Fourth page of the E-passport’s prototype

Figure 16: Fifth page of the E-passport’s prototype

Figure 17: Sixth page of the E-passport’s prototype
RESULT AND ANALYSIS

This section outlines the result and analysis of the system. It presents the results obtained from processes and testing as a part of this research project. Besides that, analysis regarding the system has been done to verify whether the whole system integrated with hardware is functioning properly or not.

AES PROGRAM INTERFACE

Only authorized person from the administration can encrypt or decrypt the data in the E-passport. There are 3 steps involved in the encryption process.

a) Select the file to be encrypted (Figure 18)
b) Insert the key (Figure 10). If the key entered is too small, the dialog box will appear as shown in Figure 19
c) Response the dialog box to overwrite data in the file (Figure 20) and Figure 21 shows the encryption process

Users are unable to view the interface if the database has been encrypted. Figure 22 shows the dialog box appears after the user try to push command buttons in the main menu page. The program cannot find the encrypted database unless if it been decrypted first. The user still can view the interface but without linked with the database as shown in Figure 23. So the database has to be decrypted first before viewing the page.

There are also 3 steps involved in the decryption process.

a) Select the file to be decrypted (Figure 18)
b) Insert the key (Figure 24) if the key entered is wrong, the dialog box will appear as shown in Figure 25
c) Response the dialog box to overwrite data in the file (Figure 20) and Figure 26 shows the decryption process.
ANALYSIS

Key plays the most important role in this application due to without key, encryption or decryption process cannot be done. To produce the higher quality of key, user has to ensure the key includes the combination of numbers, symbols and alphabets. Examples below show the differences key quality if user inserts the same number of character but with the different combinations.

a) Example 1 (alphabets only)
   Number of character inserted : 8
   Key combinations : christin
   Numbers of bars/boxes : 7

Figure 27 shows the key quality

![Figure 27: Key quality when 'christin' inserted](image)

b) Example 2 (alphabets and numbers)
   Number of character inserted : 8
Key combinations : c1h2r3i4  
Numbers of bars/boxes : 10

Figure 28 shows the key quality

![Key Quality][1]

Figure 28: Key quality when 'c1h2r3i4' inserted

c) Example 3 (alphabets, numbers and symbols)  
Number of character inserted : 8  
Key combinations : c2@h7*h4  
Numbers of bars/boxes : 14

Figure 29 shows the key quality

![Key Quality][2]

Figure 29: Key quality when 'c2@h7*h4' inserted
Table 1 below shows the comparison of key quality with different characters.

<table>
<thead>
<tr>
<th>No.</th>
<th>Number of Characters</th>
<th>Key Combinations</th>
<th>Key Quality (boxes in the Progress Bar)</th>
</tr>
</thead>
</table>
| 1.  | 12 (g8i33@h9#%i9) | Alphabets : 4  
Numbers  : 3  
Symbols   : 4 | 21 |
| 2.  | 12 (cfg%g4hu7bh0) | Alphabets : 8  
Numbers  : 3  
Symbols   : 1 | 21 |
| 3.  | 14 (n7h9m@10**nk03) | Alphabets : 5  
Numbers  : 6  
Symbols   : 3 | 24 |
| 4.  | 14 (njki56cfdei@ki#) | Alphabets : 11  
Numbers  : 2  
Symbols   : 1 | 23 |
| 5.  | 18 (cvgf0nj876bhg@n#8$) | Alphabets : 10  
Numbers  : 5  
Symbols   : 3 | 27 |
| 6.  | 18 (6uh6789bfg+yhbj%f6) | Alphabets : 11  
Numbers  : 6  
Symbols   : 1 | 27 |
| 7.  | 20 (k10*3p4ar%@t4b0+b^a) | Alphabets : 8  
Numbers  : 6  
Symbols   : 6 | 27 |
| 8.  | 20 (abcdefghiklm1234*#%+g) | Alphabets : 12  
Numbers  : 4  
Symbols   : 4 | 27 |
| 9.  | 24 (*%vacf678+zy367-8379cobt) | Alphabets : 9  
Numbers  : 10  
Symbols   : 5 | 27 |
| 10. | 24 (abcde12345%+*a#ab1<2f) | Alphabets : 9  
Numbers  : 8  
Symbols   : 7 | 27 |

27 = (highest key quality)

CONCLUSION AND RECOMMENDATION

The application has described the basic design approach for securing the information in the E-passport by using Advanced Encryption Standard (AES). The four main aspects in this project are Visual Basic programming language, Microsoft Access database design, AES programming code, and interfaces between hardware and software. One significant aspect is to do it step by step. This project can be considered important due to the E-passport prototype is very practical passport for travelling in groups. This is because only one passport is needed for 5 to 20 persons. By using memory stick, the passport holder’s information can be viewed and checked faster rather than read it page by page. AES algorithm is used as the encryption algorithm can keep the information in the E-passport secured. Other than that, the availability and integrity of the asset is also being considered. Only an authorized person at the administration can access and change the information in the E-passport. This makes the E-passport prototype more reliable. The security system in the E-passport can be further improved for future development. Therefore, it is highly recommended that the prototype should use the microchip to store all the information of the passport holder. This is because microchip is smaller than the memory stick in size and provides the higher capacity. By using microchip, the data can be read faster by flash it to the microchip reader.
REFERENCES