Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system

Ratnadewi, Roy P. Adhie, Yonatan Hutama, Johnny Christian & Denny Wijaya

Maranatha Christian University
Bandung, Indonesia

ABSTRACT: In this computer and Internet era, the cryptography method is commonly used to create secure communications between two or more parties. A message sent via computer can be protected by manipulating its content using cryptography, so only the intended party can know the real content of the message. One of the most commonly used cryptography methods, especially in the form of text, is the advanced encryption standard (AES). Within this context, several issues have been addressed in this study. These include the way AES works in protecting data, especially for the AES-128 variant and software engineering through the creation of an application using the C++ programming language to realise and analyse the performance of AES-128 in the encrypting process for data writing and decrypting process for data reading of smart cards that work in the near field communication (NFC) based communication system.

INTRODUCTION

Messages or data exchange occur in the communication process. The delivery process of a message that is sensitive and personal must be protected in order to avoid information theft by irresponsible parties. One way to protect that delivery process is to use cryptography. One method that is commonly used nowadays in securing messages, especially in the form of text, is the advanced encryption standard (AES). The AES cryptography method was developed in 1999 via a competition set up by the National Institute of Standards and Technology (NIST) to replace outdated cryptography methods, the data encryption standard (DES) and the triple data encryption standard (3DES/TDES) [1]. The competition was won by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who proposed the Rijndael cipher, which has now become the standard of the digital text data encryption process.

The main difference between AES, DES and 3DES is the key length for the encryption and decryption processes. AES uses three variants of key length that are 128 bit, 192 bit and 256 bit, whilst DES and 3DES use 56 bit and 168 bit of key length, respectively. Theoretically, the longer the key length used, the stronger the security level of the encrypted message, while it is attacked, especially by a brute - force attack. Another difference between these cryptography methods is the length of plaintext processed at a time. AES processes 128 bit plaintext, whilst DES and 3DES process 64 bit plaintext.

Near field communication (NFC) is a set of protocols and interfaces used for the data exchange process in wireless communication system devices and now widely used for many purposes, such as payment for public transportation, access control for security areas and user authentication for bank transactions. NFC itself is one of many developments of radio frequency identification (RFID) communication technology and is included in the high frequency (HF) category with a working frequency of 13.56 MHz. Examples of devices that support NFC-based communication technology are the contactless smart card and the contactless smart card reader. A contactless smart card reader is used as a supporting device for data exchange media between a contactless smart card reader and computer.

THEORETICAL BASIS

Advanced Encryption Standard (AES)

AES is a symmetric - key block cipher type of cryptography method. It consists of two processes, the encryption process and the decryption process. Each of them has six steps. The decryption process is done by reversing the steps of the encryption process. There are three variants of AES: AES-128, AES-192 and AES-256 [2]. The number after AES indicates the key length used for encryption and decryption process.

The encryption process using AES cryptography consists of a six-step process, namely: 1) key expansion - this process step manipulates key and produces round keys that will be used in the sixth process step (add round key); 2) initial transformation - that can be called add round key round - 0. This process step will XOR each bit of 128 bit plaintext with a 128 bit key used to encrypt a data; 3) substitute bytes - this process step will substitute each byte from the result of the second process step (initial transformation) using substitution box (S - box); 4) shift rows - this process step will permute each row from the result of the third process step (substitute bytes), which are made in matrix logic form; 5) mix columns - this process step will multiply the result of the fourth process step (shift rows) with multiplier matrix in the form of matrix multiplication; and 6) add round key - this process step will XOR each bit from the result of the fifth process step (mix columns) with round key produced by the first process step (key expansion) [3][4].

The second process step is done only once at the beginning of the AES encryption process. The third up to the sixth process step will be done 10 to 14 times repeatedly, according to the number of rounds used by the AES encryption process depending of its variant, except for the mix columns process step that will not be done in the last round of AES encryption process. AES-128 will do 10 round processes, whilst AES-192 and AES-256 will do 12 round and 14 round processes respectively [5-7]. The AES encryption and decryption process block diagram is shown in Figure 1.

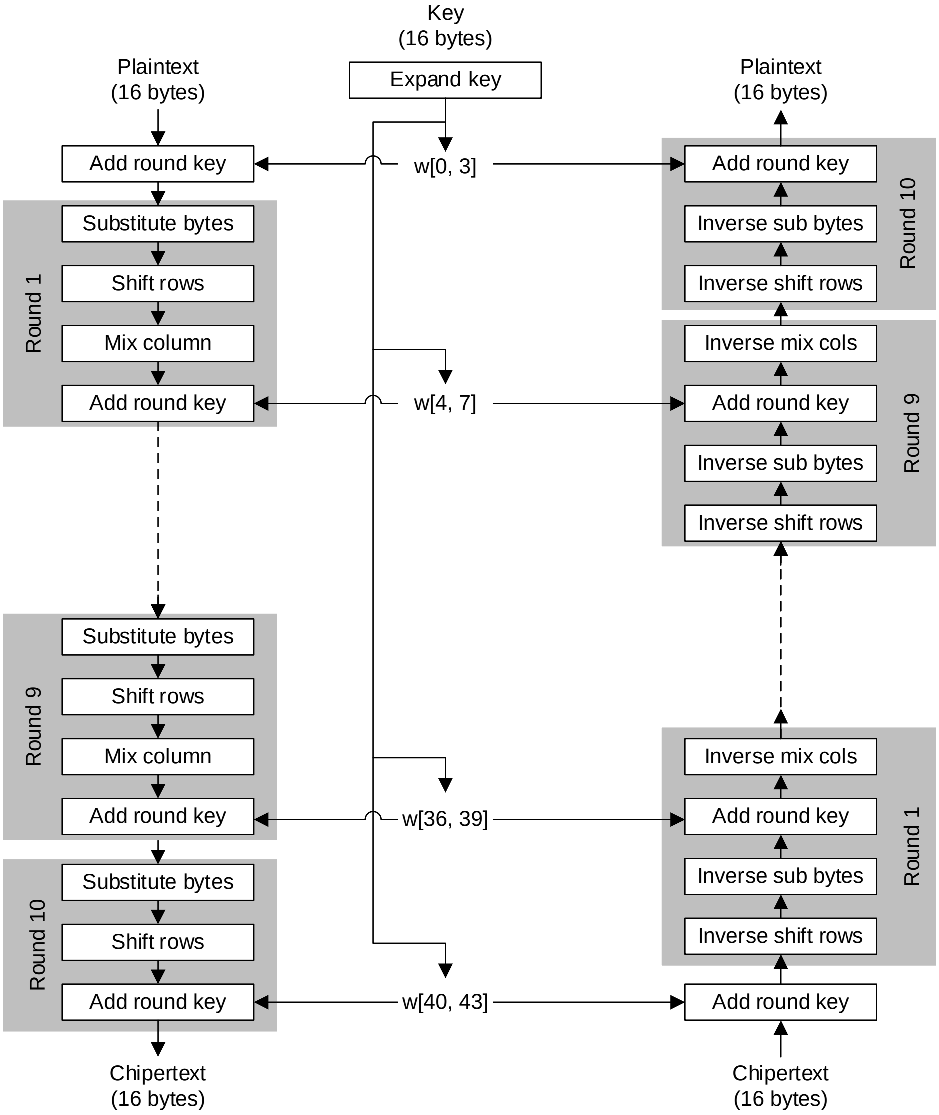


Figure 1: AES encryption and decryption process block diagram [4].

Near Field Communication (NFC)

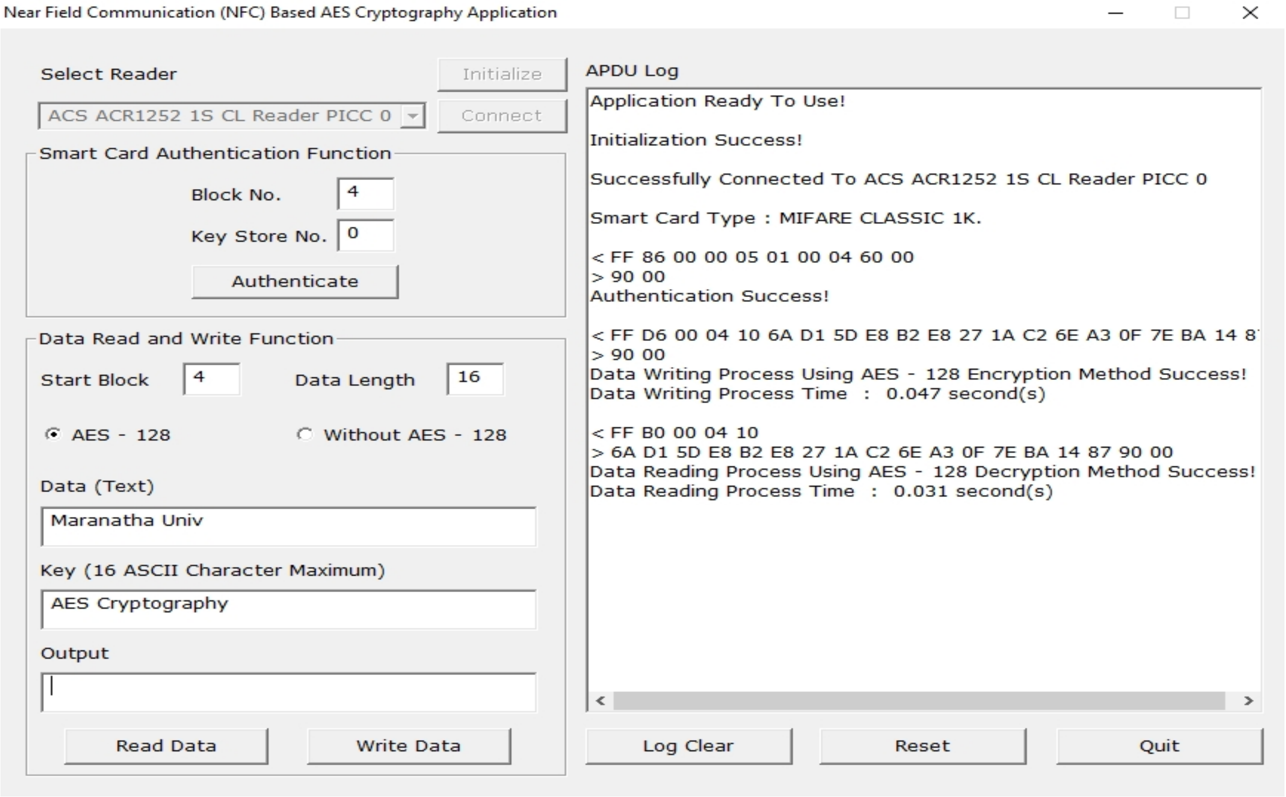
NFC is one of the latest sophisticated communication technologies. It was developed from RFID communication technology and has a working frequency of 13.56 MHz. Every device used in the NFC-based communication process is divided into two types, active and passive devices. An example of an active device is a contactless smart card reader, while an example of a passive device is a contactless smart card. Each NFC-based active device can work in three modes of operation that are: 1) card emulation; 2) card reader/writer; and 3) peer-to-peer [8].

The card emulation mode is used to change the function of active devices such as smart phones so they can be used like a smart card. The card reader/writer mode is used to perform the writing and reading processes of the data contained in passive devices. The peer-to-peer mode is used to perform data exchange processes between two active devices with similar characteristics, such as two smart phones. The second mode will be used in this research to examine the performance of AES cryptography method.

IMPLEMENTATION, EXAMINATION AND ANALYSIS

Program Implementation

The authors of this research implemented AES-128 cryptography methods into created programs using Microsoft Visual Studio 2008 software and in C++ programming language. Programs built in the form of applications can be used on computers that have been based on .NET framework. There is one application in this research that is the application of data writing and data reading of MIFARE 1K smart card using AES cryptography in NFC-based systems. The contactless smart card and smart card reader that will be used in this research are MIFARE 1K smart card and ACS ACR1252U reader. The application can be seen in Figure 2.


Near Field Communication (NFC) Based AES Cryptography Application
Initialize
Connect
Smart Card Authentication Function
Authenticate
Data Read and Write Function
Read Data
Write Data
Log Clear
Reset
Quit

Select Reader: ACS ACR1252 1S CL Reader PICC 0

Block No.: 4

Key Store No.: 0

Start Block: 4

Data Length: 16

● AES - 128 ○ Without AES - 128

Data (Text): Maranatha Univ

Key (16 ASCII Character Maximum): AES Cryptography

Output:

APDU Log

```
Application Ready To Use!

Initialization Success!

Successfully Connected To ACS ACR1252 1S CL Reader PICC 0

Smart Card Type : MIFARE CLASSIC 1K.

< FF 86 00 00 05 01 00 04 60 00
> 90 00
Authentication Success!

< FF D6 00 04 10 6A D1 5D E8 B2 E8 27 1A C2 6E A3 0F 7E BA 14 8
> 90 00
Data Writing Process Using AES - 128 Encryption Method Success!
Data Writing Process Time  :  0.047 second(s)

< FF B0 00 04 10
> 6A D1 5D E8 B2 E8 27 1A C2 6E A3 0F 7E BA 14 87 90 00
Data Reading Process Using AES - 128 Decryption Method Success!
Data Reading Process Time  :  0.031 second(s)
```

Figure 2: The application of data writing and data reading of MIFARE 1K smart card using AES cryptography method in the NFC-based system.

The MIFARE 1K smart card data writing process using the AES encryption method has two inputs, the message that will be encrypted (plaintext/data) and key, and a single output, that is the message that has been encrypted perfectly and will be loaded into the MIFARE 1K smart card (cipher text). The data writing process is executed by pressing the *write data* button. The MIFARE 1K smart card data reading process using the AES decryption method has two inputs, the cipher text and key, and also a single output, the message that has been perfectly decrypted (plaintext) and also will be displayed in the *data* text box in the application. The data reading process is executed by pressing the *read data* button.

AES-128 Performance Examinations

A performance examination was conducted to examine two things: the data writing process time and data reading process time of MIFARE 1K smart card using the AES cryptography method. This performance examination also included the DES and 3DES cryptography method from the authors' previous research to determine AES performance compared with DES and 3DES [9].

There are 10 sets of observational data for each trial based on the length of processed data, starting from 16 ASCII characters up to 672 ASCII characters. Each data observation was tested three times to generate the average process time. The performance examination results table that is carried out can be seen in Table 1 to Table 4.

The performance examination that is done shows the result that the data writing process time using AES encryption method is slower than using DES and 3DES encryption methods for each observational data. It is also the case that the data reading process using AES decryption method is slower than using DES and 3DES decryption methods for observational data. The process time between these three cryptography methods grows along with the increasing length of the data processed.

Table 1: AES performance examination results.

No.	Data length (ASCII character)	Process time AES cryptography method (milliseconds)							
		Data write process				Data read process			
		Test 1	Test 2	Test 3	Average	Test 1	Test 2	Test 3	Average
1	16	47	47	47	47	62	62	62	62
2	32	62	63	62	63	101	100	102	101
3	48	78	78	79	79	140	140	141	141
4	96	154	155	155	155	266	266	268	267
5	192	313	316	315	316	549	548	546	548
6	288	467	469	464	467	827	829	827	828
7	384	626	623	624	625	1097	1093	1099	1097
8	480	788	785	785	786	1374	1381	1379	1379
9	576	953	951	959	955	1650	1652	1656	1653
10	672	1110	1113	1108	1111	1942	1943	1938	1941

Table 2: DES performance examination results.

No.	Data length (ASCII character)	Process time DES cryptography method (milliseconds)							
		Data write process				Data read process			
		Test 1	Test 2	Test 3	Average	Test 1	Test 2	Test 3	Average
1	16	61	60	61	61	42	42	44	43
2	32	64	63	65	64	42	42	44	43
3	48	71	73	74	73	48	46	46	47
4	96	88	89	86	88	51	52	51	52
5	192	131	133	129	131	100	98	103	101
6	288	153	151	150	152	117	115	117	117
7	384	182	184	184	184	132	133	135	134
8	480	197	199	198	198	142	140	139	141
9	576	214	216	217	216	153	155	150	153
10	672	234	237	233	235	161	160	165	162

Table 3: 3DES performance examination results.

No.	Data length (ASCII character)	Process time 3DES cryptography method (milliseconds)							
		Data write process				Data read process			
		Test 1	Test 2	Test 3	Average	Test 1	Test 2	Test 3	Average
1	16	64	65	63	64	47	45	45	46
2	32	68	72	69	70	52	54	55	54
3	48	76	73	74	75	58	57	57	58
4	96	93	92	95	94	71	69	72	71
5	192	138	139	142	140	124	125	122	124
6	288	173	176	174	175	138	139	143	140
7	384	195	203	201	200	153	149	154	152
8	480	237	236	234	236	186	184	186	186
9	576	279	282	283	282	202	205	206	205
10	672	306	309	312	309	219	223	218	220

Table 4: Performance examination average results.

No.	Data length (ASCII character)	Average process time test (milliseconds)					
		Data write process			Data read process		
		AES	DES	3DES	AES	DES	3DES
1	16	47	61	64	62	43	46
2	32	63	64	70	101	47	54
3	48	79	73	75	141	52	58
4	96	155	88	94	267	67	71
5	192	315	131	140	548	101	124
6	288	467	152	175	828	117	140
7	384	625	184	200	1097	134	152
8	480	786	198	236	1378	141	186
9	576	955	216	282	1653	153	205
10	672	1111	235	309	1941	162	220

Through a performance examination, it was also found that the data writing process time of the MIFARE 1K smart card using AES encryption method is faster than the data reading process time of MIFARE 1K smart card using AES decryption method for the observational data. The average process time chart of the data writing process and data reading process using AES, DES and 3DES cryptography methods for each observational data can be seen in Figure 3 and Figure 4.

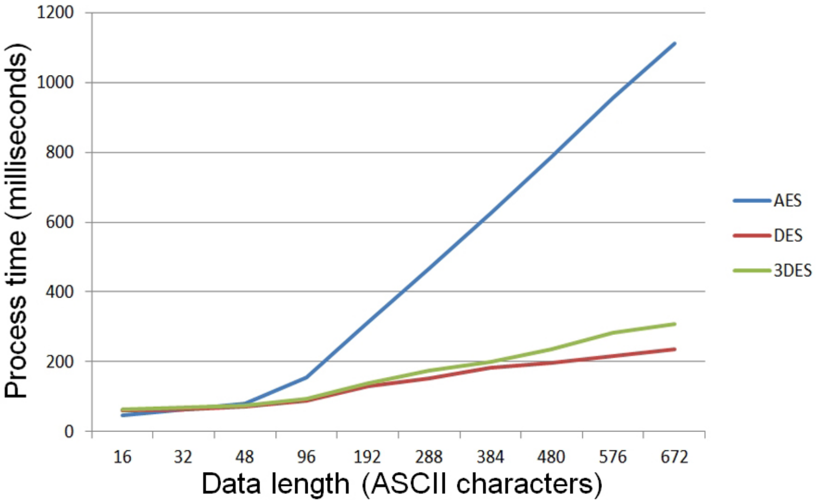


Figure 3: Data writing average process time.

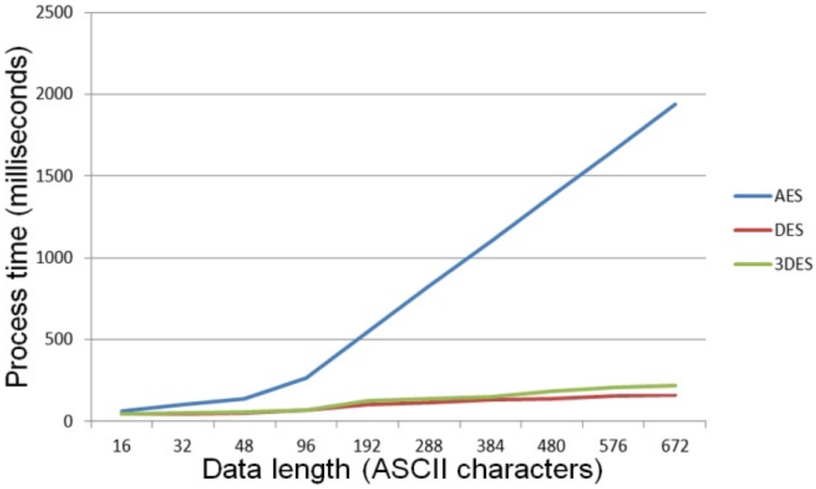


Figure 4: Data reading average process time.

AES-128 Performance Analyses

Based on the performance examination of the AES cryptography method compared with DES and 3DES, there is an issue about the process time needed for AES in data writing and data reading. It takes longer compared to DES and 3DES. The time gap between AES and the other two cryptography methods grows bigger as the data length processed increases. This occurs because of the complexity of the process step used by AES [10]. AES does not only use the permutation and substitution process the way DES and 3DES do. It consists of a mix columns process step that conducts multiplication between two matrices (the most complicated process of the AES encryption process), and also inverse mix columns for the AES decryption process [4][11]. Because of that, the mix columns and inverse mix columns process step need a longer program to be implemented in the application, and it can affect the process time when data writing and data reading processes are executed.

CONCLUSIONS

Based on the research conducted on the AES cryptography method, several conclusions can be reached, that the AES-128 cryptography method has been successfully implemented for securing the data writing and data reading process of MIFARE 1K contactless smart card in an NFC-based system.

The process time of MIFARE 1K contactless smart card data writing and data reading process using AES takes longer compared to DES and 3DES. The process time of data writing process of MIFARE 1K contactless smart card is faster than the data reading process using AES cryptography method.

REFERENCES

1. Singh, G. and Supriya, A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *Inter. J. of Computer Appl.*, 67, 19 (2013).
2. Paar, C. and Pelzl, J., *Understanding Cryptography - a Textbook for Students and Practitioners*. Heidelberg: Springer - Verlag GmbH & Co (2010).
3. Mankotia, S. and Sood, M., A critical analysis of some symmetric key block cipher algorithms. *Inter. J. of Computer Science and Infor. Technol.*, 6 (2015).
4. Stallings, W., *Cryptography and Network Security - Principles and Practice.* (6th Edn), Upper Saddle River, New Jersey: Pearson Education Limited, 130-155 (2014).
5. Garcia, D.F., Performance evaluation of Advanced Encryption Standard algorithm. *Proc. Second Inter. Conf. on Mathematics and Computers in Sciences and in Industry (MCSI)*, Sliema, Malta, 247-252 (2015).
6. Kahate, A., *Cryptography and Network Security*. Singapore: Tata McGraw - Hill Publishing Company Limited, (2003).
7. Joshi, A., Dakhloe, P.K. and Thatere, A., Implementation of S-Box for advanced encryption standard. *Proc. IEEE Inter. Conf. on Engng. and Technol. (ICETECH),* Coimbatore, India, 1-5 (2015).
8. Ofeishat, H. and Rababah, M., Near field communication (NFC). *Inter. J. of Computer Science and Network Security*, 12, 2 (2012).
9. Ratnadewi, Adhie, R.P., Hutama, Y., Christian, J. and Wijaya, D., Implementation of data encryption standard (DES) and triple data encryption standard (3DES) cryptographic method in near field communication (NFC) based communication system. *Proc. 10th Inter. Multidisciplinary Conf. ADRI, Batam, Indonesia*, 1-6 (2017).
10. Pendli, V., Pathuri, M., Yandrathi, S. and Razaque, A., Improvising performance of Advanced Encryption Standard algorithm. *Second International Conf. on Mobile and Secure Services (MobiSecServ),* Gainesville, Florida, United States of America, 1-5 (2016).
11. Shivkumar, S. and Umamaheswari, G., Performance comparison of Advanced Encryption Standard (AES) and AES key dependent S-Box - Simulation using MATLAB. *Proc. Inter. Conf. on Process Automation, Control, and Computing,* Coimbatore, Tamilnadu, India, 1-6 (2011).