IEESE International Journal of Science and Technology (IJSTE), Vol. 5 No.2 , June 2016, 6-11
ISSN : 2252-5297

Implementation Of RC4 Algorithm Of Smart Card Service Applications For Book Borrowing In Library

Dewi Chumairoh

Informatics Engineering
Science and Technology Faculty, Islamic State University Maulana Malik Ibrahim Malang
Indonesia
dewi.cum2@gmail.com

Abstract. The Smart card is one of the technologies that are currently being developed. Along with the development of technology, the problem faced is the insecurity of data stored in the regular card. The data can still be read and manipulated by unauthorized parties. By using smart cards, the advantage that can be obtained is to keep the data confidential of the smart card owner, to provide important data information, and secure data storage. This research is intended to make a smart card application for library lending transaction service. This application is built using RC4 algorithm which is one type of a stream cipher, RC4 algorithm has the same key for encryption and decryption process. Testing is done by entering data in the form of NIM, borrowing ID, and the last date of a library visit. The data is encrypted so that the process changes into a secret code, then the data stored in the smart card. Based on the research that has been done, the results obtained that the RC4 algorithm can be used in the manufacture of smart card application library lending transaction services. The data stored in the smart card cannot be opened in another program. The key to the formation result of the RC4 algorithm has the same character length as the length of the data input character. RC4 algorithm test results with inputs of numbers, letters, and combinations of various characters to produce an average accuracy value of 80%.

Key-words: *smart card, cryptography, RC4*

1. Introduction

In today's era of globalization, it requires humans to develop a wide range of science and technology to help improve their lives. Along with the rapid development of technology, almost all areas of life using information technology to support operational work for the better. Utilization of science and information technology will maximize the potential of educated and educated human resources that can build the nation.

The Smart card is one of the technologies that are currently being developed. Smart cards have several advantages, including the ease of accessing data, the security of data storage, data protection from unauthorized parties, and the flexibility to carry easily in everyday activities, has encouraged the use of this technology applied in the academic sector to store data. Benefits that can be obtained with the use of this smart card is to keep the confidential data of the smart card owner, provide important data information, and secure data storage [1].

Therefore, the author will create a smart card application for library lending transaction services. Smart card technology offers the convenience and security of data storage because of the data encryption mechanism before the data is stored in memory, as well as the existence of a pin (secret code) that keeps the data from being read by unauthorized parties.

In maintaining data security, smart cards have used several methods that exist in cryptography, one of the methods is Rivest Code 4 or commonly known as RC4. The RC4 algorithm is one type of stream cipher so that RC4 processes the unit or inputs data, messages or information at one time. Units or data are generally a byte so in this way encryption or decryption can be executed at variable lengths. The algorithm does not have to wait for some input data, messages or certain information before being processed, or add additional bytes to encrypt [2].

The RC4 algorithm is included in symmetric key cryptography, a cryptographic algorithm that uses the same encryption key as the decryption key. The advantages of symmetric key cryptography include the encryption / decryption process takes a short time, the symmetric key size is relatively short and can be used to generate random numbers, symmetric keys can be arranged to produce more powerful ciphers, the authentication of the message sender is known directly from the received ciphertext The key is known only to senders and recipients only.

2. Literature Study

Smartcards are plastic cards of the same size as credit cards in which there is a silicon chip called a microcontroller. Chip is an integrated circuit consisting of processor and memory. Chip, like a CPU (Central Processing Unit) on a computer, tasked with executing commands and providing power to smartcards [1] (Christine Sariasih, 2009). Smartcards are the development of magnetic cards, but unlike magnetic cards that are used only for data storage, Smartcards have the ability to process and interpret data, and store the data securely. Especially with the development of cryptographic algorithms, the stored data will be encrypted first, so it is not easy to read by unauthorized parties / entitled. This will make it harder for smartcard counterfeiting. In addition to the differences in the presence of chips, smartcards have a larger memory capacity than magnetic cards[1].

In general there are two types of smart card is a memory card and microprocessor card. Memory cards only store and protect data locally, but do not contain a processor to perform computer calculations on the data. While the microprocessor card is a card that has a memory and microprocessor that can perform calculations on data and store data in the card safely [3].

The Rivest Code 4 (RC4) cryptographic algorithm is one of the symmetric key algorithms created by RSA Data Security Inc (RSADSI) in the form of chipper streams. The algorithm was discovered in 1978 by Ronald Rivest and became an RSA security symbol (an abbreviation of three inventors' names: Rivest Shamir Adleman). RC4 uses a key length of from 1 to 256 bytes used to initialize a 256 byte table. This table is used for the following generation of pseudo randoms that use XOR with plaintext to generate ciphertext. Each element in the table is exchanged at least once [4].

RC4 is one type of stream cipher so that RC4 processes the unit or inputs data, messages or information at one time. Units or data are generally a byte so in this way encryption or decryption can be executed at variable lengths. This algorithm does not have to wait for some input data, messages or certain information before being processed, or add additional bytes to encrypt [2].

The RC4 algorithm uses two S-Boxes that are 256-long arrays containing permutations from numbers 0 to 255, and the second S-box, which contains permutations, is a function of a variable length key [2].

In general, the RC4 algorithm is divided into two, state-array initialization and encryption key revenue and its encryption.

A. Initialize State-Array

In the initialization of state-array, there are two state-arrays that must be initialized, S and K. Array S of 256 bits is initialized with numbers from 0 to 255. While the K array of 256 bits is filled with keys of 1-256 bits repeatedly Until the entire K array is fully loaded. After that, Key Scheduling Algorithm is performed to generate permutations of the S array based on available key [5].

B. Encryption key and encryption key

After having a random state array, we re-initialize i and j by 0. After that, we do a pseudo-random generation algorithm or PRGA to generate an encryption key (cipher_byte) that will be XORed with plaintext. To generate an encryption key, the PRGA increments i, adds the S [i] and S [j] values of both, and the resulting key value is S with an index equal to the number S [i] and S [j] Modulo with 256 [5].

After finding the key for each character, an XOR operation is performed between the characters in plaintext and the generated key.

3. System Design

This smart card application will be built using RC4 algorithm. RC4 algorithm is used for the process of encryption and decryption of data in the smart card. The purpose of using this RC4 algorithm is to secure the data on the smart card so that the data cannot be read by unauthorized parties. RC4 algorithm is a symmetric algorithm that is algorithm that has same key for encryption and decryption process. The main process in this application is to encrypt the data that has been entered into the smart card with a secret key that has been formed.

3.1 Context Diagram

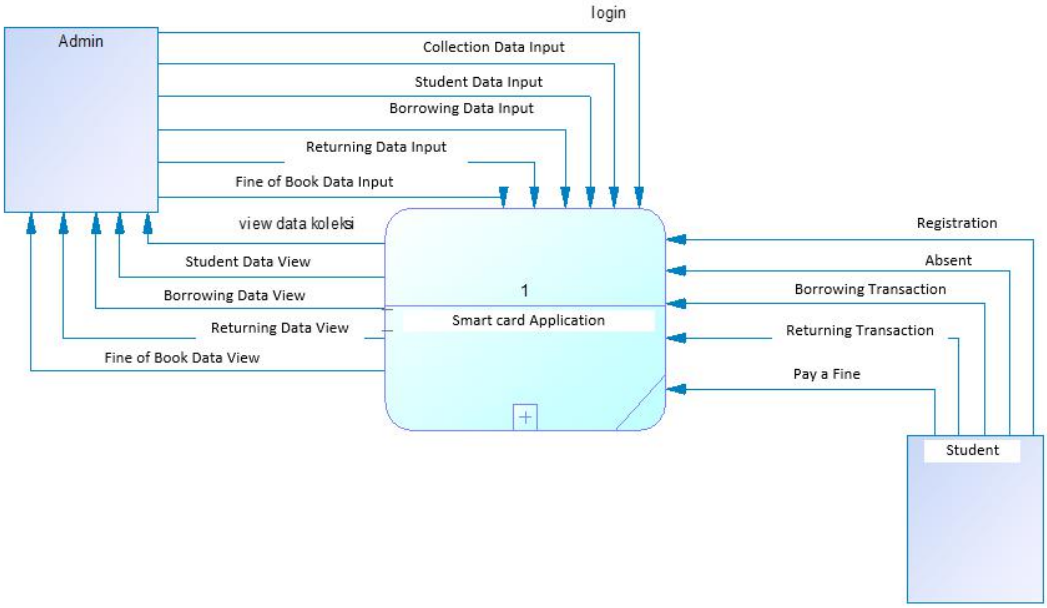

Figure 1. Context Diagram

The picture describes the flow of smart card applications for library book lending services, which generally involves two entities, namely: admins and students. Admin is a library application service provider and there are eleven data streams, of which six data streams go to the application and five data streams out of the application. While the student is a user of the library application and there are five data streams entirely to the application.

3.2 Flowchart Smart Card Application for Data Encryption

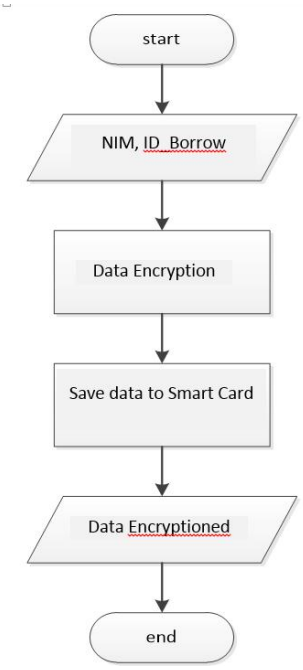

Figure 2. Flowchart Diagram

Flowchart is started with input in the form of NIM data or borrowing ID. Then the input encryption process and the next process data that has been encrypted is stored in the smart card. The output of the flowchart is a NIM data or borrowing ID but in encrypted form.

3.3 Database Design

In database design using Database Access which is one of the database application program that has usability to design, create, and manage database. In the design of the database, there are six tables, namely: admin, collection, students, absent, borrow, and return. For the admin table, the table stands alone and there is no relation with other tables. For the student table in the nim field there is a relation with the absent table in the nim field as well. Table absent in the field nim also there is a relation with the loan table on the field nim. For the borrowed table in the ID_pinjam field there is a relation with the return table in the ID_pinjam field. While the lending table on the book code field there is a relation with the code field of the book in the collection table.

4. Implementation

In the RC4 algorithm there are three steps, namely the formation of keys, encryption process, and the decryption process. Key formation is the initial stage before the process of encryption or decryption of data stored in the smart card. The first is the initialization of an 8-bit S array to form a state-array of S and K, then KSA and PRGA process. In the encryption process is done XOR process between plaintext and key that has been formed. In the process of decryption is done XOR process between cipherteks and keys that have been formed.

In the testing phase, the test will be divided into several items. From the test results will be obtained test results that can be drawn conclusions from the test. This test is done with the purpose of whether the application built is running well and in accordance with the authors expect.

a. RC4 Algorithm Test Results with Numeric Input

Table 1. RC4 Algorithm Test Result With Numeric Input

Message	Character Length	Key	Result
10650101	8	73565424	63335525
10650102	8	70626416	60076514
10650103	8	32072454	22622557
10650012	8	73565424	63335436
10650119	8	35040523	2561043:
10650058	8	40072661	50622639
10650104	8	51104267	41754366
10650062	8	37043144	27613126
10650016	8	15725743	05175755
10650037	8	60615275	70045242

Based on the experiments that have been done, the experiment is done with the input number of 15 times. Accuracy earned by 100%. This experiment is done with the input numbers with the length of character 8. The resulting key is a number with the length of character 8. The resulting output is a number with the length of character 8. Thus, all inputs can be done with good encryption process to produce output that has the same length premises Input.

b. RC4 Algorithm Test Results with Letter Input

Table 2. RC4 Algorithm Test Result With Letter Input

Message	Character Length	Key	Result
ANUGRAH WIDYASARI	17	15 6 14 3 4 16 12 12 15 12 15 3 0 8 8 14 0	NH[DVQD,XEKZA[I\
ADE DUROTUN NISA'	17	15 6 14 3 4 16 12 12 15 12 15 3 0 8 8 14 0	NBK#@E^C[YA#NA[O
PUSPITA DEWI EKASARI	20	0 0 11 9 10 1 5 15 7 1 0 14 2 14 2 15 19 10 0 5	PUXYCUD/CDWG"KIN@KRL
NOVI ANTO	9	4 4 2 7 3 6 2 8 5	JKTN#GL\
NAUFAL WAFIQURRAHMAN	20	0 0 11 9 10 1 5 15 7 1 0 14 2 14 2 15 19 10 0 5	NA^OKM%XFGI_W\PN[GAK
ZAENAL ABIDIN	13	1 5 8 10 12 3 5 4 7 9 8 9 4	[DMDMO%EE@L@
ALDITA RAHMA MML	16	15 0 3 11 14 13 12 9 9 7 9 2 15 9 12 13	NLGBZL,[HODC/DAA
AGUS FADLUN NI'AM	17	15 6 14 3 4 16 12 12 15 12 15 3 0 8 8 14 0	NA[P$VMHCYA#NA/O
JOEHANI ABDILLAH ASLAMI	23	8 10 16 13 11 13 10 11 16 2 8 16 10 3 15 16 9 5 6 4 5 12 15	BEUEJCC+Q@LYFONX)DUHDA
AFIF SUBARKAH	13	1 5 8 10 12 3 5 4 7 9 8 9 4	@CAL,PPFF[CH

Based on experiments that have been done, the experiment is done with the input letters as much as 15 times. Accuracy gained by 80%. This experiment is done by inputting letters of a certain character length. The resulting key is a number with a character length corresponding to the input length. However, there are some outputs that are not equal to input and key length. Thus, not all inputs can be encrypted properly.

c. RC4 Algorithm Test Results with Various Character Inputs

Table 3. RC4 Algorithm Test Result With Various Character Input

Message	Character Length	Key	Result
(A+B)(A-B)=	11	8 10 1 0 5 4 9 8 5 6 8	K*B,,H%G/
QW!E@R	6	5 4 3 3 0 2	TS"F@P
RT$%YU^IO&*	11	8 10 1 0 5 4 9 8 5 6 8	Z^%%\QWAJ
IO*(P)LK=JH_	12	10 5 7 0 11 4 11 11 1 11 5 2	CJ-([-G@<AM]
CJ-([-G@<AM]	11	8 10 1 0 5 4 9 8 5 6 8	@MG=.@OLV]

Based on the experiments that have been done, the experiment was conducted with the input of a combination of various characters 10 times. Accuracy gained by 60%. This experiment is carried out with various inputs of a certain length. The resulting key is a number with a character length corresponding to the input length. However, there are some outputs that are not equal to input and key length. Thus, not all inputs can be encrypted properly. From the three test results above, then obtained the result of the percentage of accuracy percentage of 80%.

5. Conclusion

RC4 algorithm can be used in making smart card application of library lending transaction service. RC4 algorithm is used as a method for the process of encryption and decryption of data in smart cards. The key to the formation result on the RC4 algorithm has the same character length as the length of the data input character. Based on the results of RC4 algorithm testing with inputs in the form of numbers, letters, and combinations of various characters yields an average accuracy of 80%.

References

[1] Sariasih, Christine. 2009. *Rancangan Keamanan Data Sistem Smart Card Kesehatan Sesuai Kebutuhan di Indonesia.* Fakultas Ilmu Komputer Universitas Indonesia.
[2] Ariyanto, Yuri. 2009. *Algoritma RC4 dalam Proteksi Transmisi dan Hasil Query untuk ORDBMS PostgreSQL*. Jurusan Teknik Informatika, Fakultas Teknologi Informasi.
[3] Fauzan, Muhammad. 2012. *Implementasi Algoritma Kriptografi RC4 pada DSP TM320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice Over Internet Protocol(VoIP)*. Jurnal EECCIS.
[4] Wahyu, Febrian dkk. 2012. *Penerapan Algoritma Gabungan RC4 dan Base64 pada Sistem Keamanan E-Commerce*. Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.
[5] Suryani, Karina Novita. 2009. *Algoritma RC4 Sebagai Metode Enkripsi.* Sekolah Tinggi Elektro dan Informatika ITB.