Implementation of Base64 and Rot47 Algorithm Combination For Hospital Patient Database Encryption

1st Dwi Iskandar, 2nd Suriana Ismail, 3rd Canggih Ajika Pamungkas, 4th Edy Susena
1,3,4 Politeknik Indonusa Surakarta, 2 Universiti Kuala Lumpur
1,3 Sistem Informasi, 2 Information Technology
1,3,4 Surakarta, Indonesia, 2 Malaysia
1dwiiskandar@poltekindonusa.ac.id, 2suriana@unikl.edu.my,
3canggihajika@poltekindonusa.ac.id, 4edysusena@poltekindonusa.ac.id

Abstract—All agency agreed bring data is matter Which very important For protected so that problem security data is matter Which need noticed. Matter Which can done to protect data so that it cannot be misused by others is by use technique cryptography. Cryptography consists of a set of algorithms and techniques For change data become form other so that contents No read and can't explained by Who course that No own authority For read or write data which has been changed. In this study the encryption method used is an algorithm ROT47 to encrypt data where the existing data position will be changed in accordance with amount rotation Which There is, Then data return encrypted use Base64 algorithm which is a scheme of encoding binary data into ASCII code strings in accordance index on Base64. Research results This is Combination ROT47 and Base64 algorithms can be implemented to in system patient database encryption with okAll agency agreed bring data is matter Which very important For protected so that problem security data is matter Which need noticed. Matter Which can done to protect data so that it cannot be misused by others is by use technique cryptography. Cryptography consists of a set of algorithms and techniques For change data become form other so that contents No read and can't explained by Who course that No own authority For read or write data which has been changed. In this study the encryption method used is an algorithm ROT47 to encrypt data where the existing data position will be changed in accordance with amount rotation Which There is, Then data return encrypted use Base64 algorithm which is a scheme of encoding binary data into ASCII code strings in accordance index on Base64. Research results This is Combination ROT47 and Base64 algorithms can be implemented to in system patient database encryption with ok.

Keywords: Cryptography, Base64, ROT47, Data, algorithm, ASCII.

I. INTRODUCTION

Technology computer very needed by life man especially personal nor group (organization). Group (organization) the very need exists computerized in every activities. From matter use computerization, then a system is created security for whole its assets, especially important information and data to maintain confidentiality information those data [1] [1].

Security is an important aspect of an data or information, Where delivery data or information need security Which tall [2]. There is a number of method do security data or message, among them is with use data camouflage technique which are called with cryptography. Cryptography is art and knowledge for protect delivery data with change it become code certain And only intended for people only have a key for change code that return Which function in maintaining the confidentiality of data or messages. In the field of cryptography there are two concepts very important or main namely encryption and decryption [3]. Encryption is process Where information or data Which want sent changed become form Which almost No recognized as information at first with use algorithm certain. Decryption is vice versa from encryption that is change turning the disguised form back into information early [4].

On moment This House Sick Still use application patient data processing where the data is in the application the can seen by person other Which no own not quite enough answer to data which there is the. Existing data can be viewed,

duplicated, and also manipulated, matter the naturally can raises problem if data personal patient which there is wrong use by person which no responsible for the crime like fraud.

Security data Which will used for guard data Which There is that is with use a combination of the ROT47 Algorithm and the Base64 Algorithm For encrypt data patient Which There is, where with combine second algorithm the can be one sufficient encryption technique complicated because if There is person Which want to see text original must know key And type combination algorithm Which used For encrypt data which there is [5].

There is a number of reference Which taken as material considerations for research conducted, reference the taken from a number of study that was done before that discussed about which problem almost The same, between other:
1. Study Which done by Koleci, etc, they do something analysis in perspective security data and complexity computing use two type method cryptography Asymmetry For implementation [6].
2. Edward, He designing implement algorithm caesar cipher and hill cipher on the retail industry [7].
3. De Rosal, etc, they designed a web security system use cryptography MD5 and SHA1 Algorithms to Encrypt REST API Authentication on Mobilebased Application [8].

In conducting this research, the problem discussed, and resolved is:

1. How apply algorithm ROT47 and algorithm Base64 for encryption data patientdi House Sick?
2. is with application This can help party House Sick for secure data patient which there is.

Objective from study This, between other:
1. Build And apply A application that can secure personal data patient with combine algorithm ROT47 and Base64 algorithm.
2. Helping the hospital to secure data agar patient can not in Wrong use by people who No responsible.

Cryptography originate and Language Greece, crypto and graphia. Crypto means secret (confidential) and graphia means writing (writing). According to terminology, cryptography is the science and art of guard security message when message sent and something place to another place [9].

Cryptography is the science of keeping data contents or order to stay safe. Safe here means no Can or difficult accessed by person other Which No entitled. Say "rights" here not a right in any sense legal law or permitted in the name of law, however someone authorized by the sender or si owner data to access the data [10].

Base64 Algorithm is Wrong One algorithm for Encoding and Decoding a data to in ASCII format, which is based on numbers basic 64 or can be said as one of the methods Which used For do encoding (encoding) to data binary [11]. This algorithm is many used in world Internet as a media data format for sending data, use the because results and encode base64 is plaintext, then this data will be much more easy sent, compared to with format data Which form binary. Scheme Base64 usually used when there is a need to encode binary data that needs to be stored and transferred over media Which designed for handle data textual.

Algorithm Base64 use code ASCII And code index base64 in do process encryption or the description. In do encryption on website URLs, base64 index code is necessary modified. Symbol "+" modified become "- " And symbol symbol "/" becomes"_" [12].
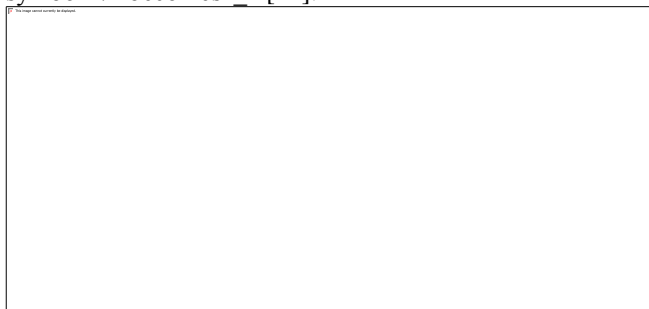

Figure 1. Index algorithm Base64

Algorithm cryptography Base64 This Actually use algorithm key symmetrical or called Also algorithm cryptography conventional, that is algorithm Which use key For process same encryption with key for process decryption.
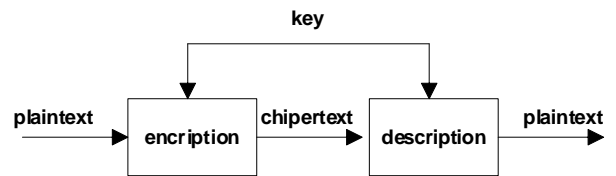

Figure 2. Algorithm symmetrical

The stages-stages of encryption using Algorithm Base64 is as following:
1. Convert character to binary.
2. Take note and be sure that There is 24 beet.
3. Convert 24 beet from three group 8 beet to four group 6 beet.
4. Convert each of the four groups of 6 bits to decimal.
5. Use each decimal For look for code character on index Base64.

As for stages-stages description using Algorithm Base64 is as following:
1. Convert character Base64 to binary with use 6 beet.
2. Conversion 24 beet from four group 6 beet to three group 8 beet.
3. Conversion each three group 8 beet to decimal.
4. Use each three decimal For looking for character ASCII For that value There is.

ROT47 is algorithm Which replaces characters in the ASCII range with character 47 characters after that (rotation) in the table ASCII. This is the algorithm reversed i.e. implementing the same algorithm for entering twice will be get text origin. ROT47 is development from type variant ROT13, Where ROT47 can said more superior because ROT47 which adds numbers and symbols in side basic alphabet.

$$s = ROT_{47}\big(ROT_{47}(s)\big)$$

Where :
S= substitution

"97" then by shifting as much as 47 step will be number "2" with value "50"

Base data is gathering data Which each other related. Data Alone is fact about objects, people, and etc. Data stated with value (a number, string, or symbol). According to James Martin (1975), database is a collection of data Which each other connected (interrelated data) Which saved in a manner together on some media, without any corruption or data duplication, so the process of adding, retrieving and modifying data can done easily and controlled.

II. RESEARCH METHODS

Process planning flow chart consists from two process that is planning flow chart encryption And decryption flowchart.
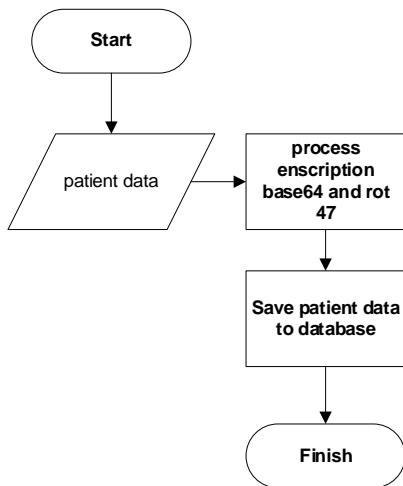

Figure 3. Flow chart scheme process encryption from application

Process encryption Which will in apply to application Which will in design, as for the process that is:
1. Databases patient will process And encrypted use algorithm ROT47 and Base64.
2. Data Which has processed And encrypted use algorithm ROT47 And Base64 furthermore will saved into the databases .

Algorithm ROT47 is derivative from ROT13. ROT47 introduces mixed letters and symbols, by Because That, text Which encoded seen more clear that text has encrypted. ROT47 Also can be easily implemented by the language modern programming in many ways. Ways of working Algorithm ROT47 that is Work based on mark ASCII with value range 33-126 and see mark owned by every character, example letter "a" worth.
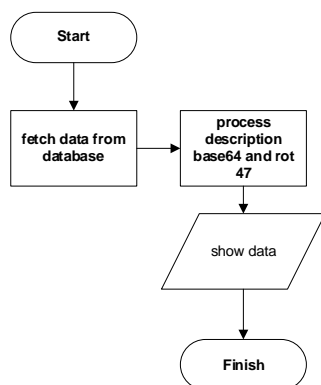

Figure 4. Flow chart scheme process decryption from application

The decryption process that will be applied to application which will in design, as for process that:
1. Databases patient will taken from databases .
2. Data processed And decrypted use algorithm ROT47 And Base64.
3. Data Which has processed will in show on application.

The steps taken by the user application can seen on use case diagram following:
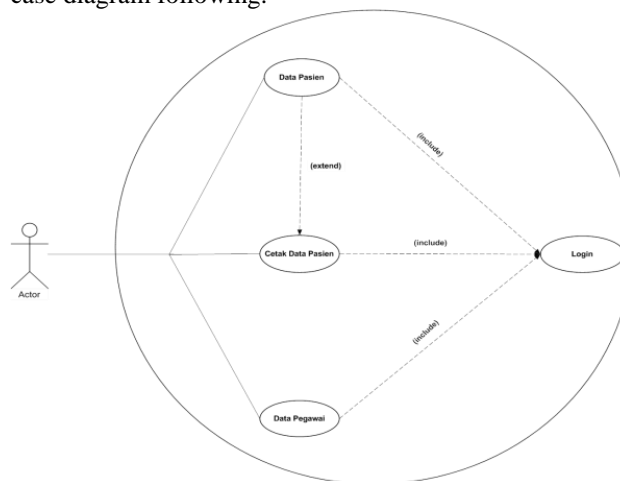

Figure 5. Usecase diagram user application

In the use case diagram there are application users actor in the system Which designed that is as employee . Employee role For add, change, delete patient data and employee data, and only employees can print patient data Which There is.

III. RESULT AND ANALYSIS

On part This, outlined results planning application and discussion from method Which has outlined on.

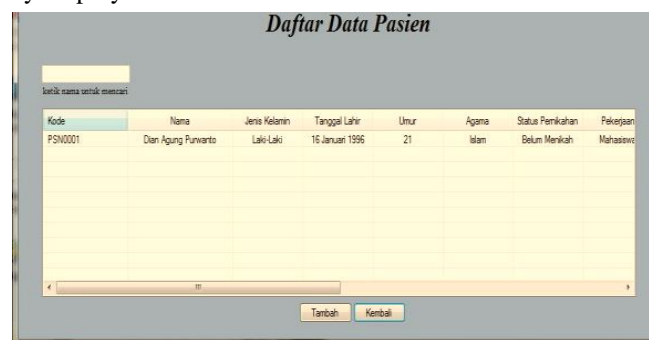The employee main menu is the main view Which in use by employee for enter to some menus.

Figure 6. Menu list data patient

Menu data patient is appearance menu to view patient data, in this menu there is information regarding personal data patient.
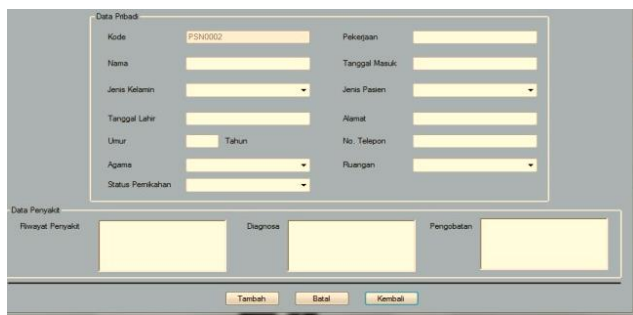
Figure 7. Menu add data patient

On the add menu, employee Can add identity of the new patient and if the data in the listview is in click so will displays menu change data patient.
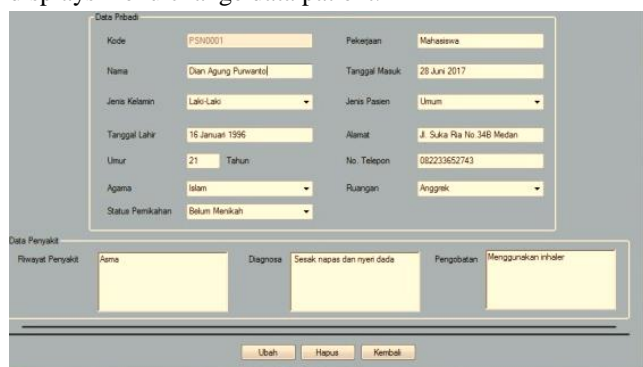

Figure 8. Menu change data patient

On picture on seen a number of data such as name, gender, and date of birth. If the data in one of the textboxes is changed, then the data is not will stored. On picture Also seen knob delete used to delete patient data selected.
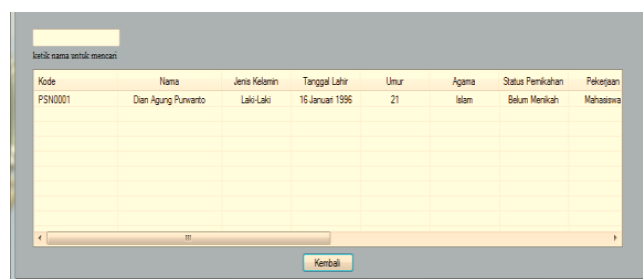

Figure 9. Menu choose data patient for in print

The patient data print menu is a menu display for see and print data patient on House Sick
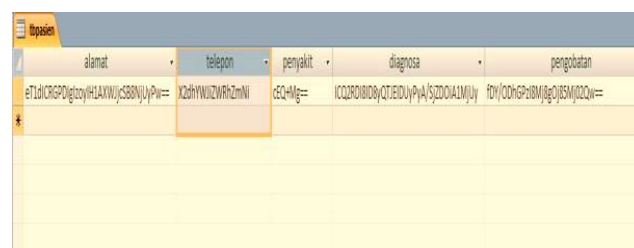

Figure 10. Results print data patient

Figure 11. Data Encryption

Based on picture on seen a number of data Which has encrypted on databases. As for encrypted data is data in the address field, telephone field, disease field, diagnosis field, and field treatment.

VI. CONCLUSION

Based on from description Which has discussed previously through implementation And testing system, so writer can take conclusion as following:
1. Application This designed with use Microsoft Visual Studio 2015 with objective to secure the patient database at home Sick.
2. The combination of ROT47 and Base64 algorithms can become A algorithm with security Which adequate And can used For secure the patient database at the hospital.
3. Algorithm combination ROT47 and Base64 can in implement to in system encryption databases patient with Good.

With designed system This expected can be a means for system development further, in order to improve system performance Which more Good. Following is suggestion writer that is:
1. Expected on development furthermore, design application can more repaired so that seen more interesting.
2. Adding another algorithm to the application in Century future so that can strengthen security on databases.
Adding features/facilities to the application in Century future in order to meet the needs of application, and also function for comfort user.

REFERENCES

[1]   D. Intannia, W. W. Widiyanto, and A. Widyoko, "Analysis of the Medical Record Document Maintenance System in the Filing Room of the Health Center Sei . Asam," vol. 03, no. 01, pp. 37–43, 2022.
[2]   M. K. Kansiime, J. A. Tambo, I. Mugambi, M. Bundi, A. Kara, and C. Owuor, "COVID-19 implications on household income and food security in Kenya and Uganda: Findings from a rapid assessment," *World Dev.*, vol. 137, p. 105199, 2021.
[3]   P. Desain, U. Interface, and S. Informasi, "Journal Health Information Management Indonesian (JHIMI) ISSN 2829-6435 Perancangan Desain User Interface Sistem Informasi Peminjaman dan Pengembalian Dokumen Rekam Medis di Puskesmas Jabung Medical Record Documents at Jabung Public Health Center Journa," vol. 03, no. 01, 2022.
[4]   R. F. Naryanto, M. K. Delimayanti, Kriswanto, A. D. N. I.

Musyono, I. Sukoco, and M. N. Aditya, "Development of a mobile expert system for the diagnosis on motorcycle damage using forward chaining algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 3, pp. 1601–1609, 2022.

[5]   N. Taliasih and I. Afrianto, "Implementation of Rc4 and Base64 Combination Algorithm To Secure Client Database of Pt Infokes," no. 102.

[6]   K. Koleci, M. Baldi, M. Martina, and G. Masera, "A hardware implementation for code-based post-quantum asymmetric cryptography," *CEUR Workshop Proc.*, vol. 2597, pp. 141–152, 2020.

[7]   E. P. Mondol, "The Impact of Block Chain and Smart Inventory System on Supply Chain Performance at Retail Industry," *Int. J. Comput. Inf. Manuf.*, vol. 1, no. 1, pp. 56–76, 2021.

[8]   de Rosal Ignatius Moses Setiadi, A. F. Najib, E. H. Rachmawanto, C. A. Sari, M. K. Sarker, and N. Rijati, "A comparative study MD5 and SHA1 algorithms to encrypt REST API authentication on mobile-based application," *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 206–211, 2019.

[9]   A. Kumar and S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography," *Arch. Comput. Methods Eng.*, vol. 28, no. 5, pp. 3831–3868, 2021.

[10]   S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, p. 1012, 2020.

[11]   W. Muła and D. Lemire, "Base64 encoding and decoding at almost the speed of a memory copy," *Softw. - Pract. Exp.*, vol. 50, no. 2, pp. 89–97, 2020.

[12]   M. Efendi, V. Sihombing, and S. Parulian, "Implementation and Use of Base64 Algorithm in Video File Security," *Sinkron*, vol. 7, no. 1, pp. 243–247, 2022.