Cryptography Generator for Prevention SQL Injection Attack in Big Data

Martiano[1], Yoshida Sary[1], Farhan Al-Iksan[1]
[1]Department of Information System, University Muhammadiyah Sumatera Utara, Indonesia

ABSTRACT

Currently, especially in Indonesia, data leaks occur in domestic agencies and private e-commerce. From these problems, cryptographic researchers are needed to make the data difficult to read, this research forms cryptography through a substitution method which will determine the number of keys that have been used and generated back in the dictionary, in its implementation the researcher uses the Devops design method, this method uses 4 stages, namely 1.) continues development, 2) continues testing, 3) continues integration, 4) continues development. The results obtained by the text can be encrypted and described perfectly and successfully as much as 15864 data, and consumes low resources .

Keyword : e-**commerce** ; **cryptographic**; **number of keys; Data.**

Corresponding Author:
Martiano,
Department of Information System
Universitas Muhammadiyah Sumatera Utara
Jl. Kapten Mukhtar Basri No 3 Medan, 20238, Indonesia.
Email : martiano@umsu.ac.id

Article history:
Received Aug 25, 2022
Revised Sep 01, 2022
Accepted Sep 03, 2022

1. INTRODUCTION

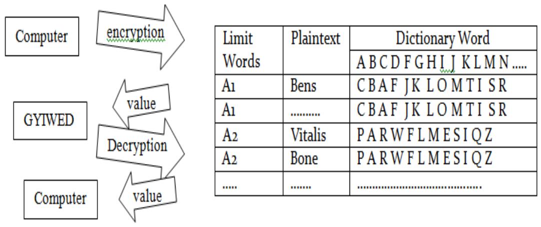
Cases of personal data leakage are increasingly common. As is the case with domestic agencies, large amounts of data leaks are data managed by the health social security agency, in which the leaked data contains information such as card numbers, family data, dependent data and payment status. This data leak occurs when a data buyer with the initials kort wants to resell data in an online forum. The data contains 279 million data on the identity of Indonesian citizens (Widya,2021).

From this case, it is dangerous if the data is scattered and misused, this can harm many parties. A good method to use is to use cryptography used in securing writing that is sent from one place to another (Anggraini,2020). Cryptography includes techniques such as: microdots, combining words with pictures, and other ways to hide information in a storage or transit (Gaurav,2013). Writing is known as plaintext while messages are encoded and called cipertext. This process is known as encryption or encryption (wiliam,2012; Fauzi, 2020; Martiano, 2021).

In this study, the researcher uses a cryptographic substitution method that has been modified and can be generated every month and made in the form of a file, in order to create difficulties in trying to re-decrypt with the brute force method or other techniques (Martiano, 2021; Marnoko, 2020).

2. RESEARCH METHOD

The first thing the researchers did was to design an algorithm, where the plaintext, the key source will be determined, for example A1, the key determination comes from the number of messages that will be limited for example 5 if the number of plains is more than 5 then the algorithm will randomize the cipher text. The results of the cipher text will be equated with the existing plantext so that it can be encrypted properly as shown below:



Limit Words	Plaintext	Dictionary Word
		A B C D F G H I J K L M N .....
A1	Bens	C B A F J K L O M T I S R
A1	....	C B A F J K L O M T I S R
A2	Vitalis	P A R W F L M E S I Q Z
A2	Bone	P A R W F L M E S I Q Z
.....	....	....

Figure 1. Encryption process and word description

To develop this research, the researcher uses the development technique of Devops Life Cycle, so it can be seen in the picture. Devops can shorten the time between software development and operation without reducing its quality (wiliam,2011). In the development of Devops there are 4 phases, namely a. Continuous Development, b. Continuous Testing, c. Continuous Integration, d. Continuous Deployment (thoirin,2020; Lubis, 2020; Lubis, 2019)

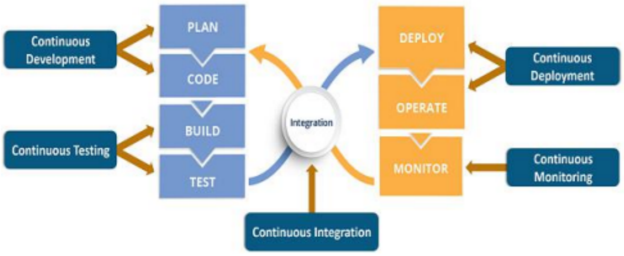


Figure 2. Devops Life cycle (Arvin,2019)

In measuring the suitability of the results, it will compare the suitability of the results of the encryption and its description whether it is good or not.

3. RESULTS AND DISCUSSIONS

During testing and implementation, the stages are design, testing, and implementation. This can be broken down through the following process:

3.1 continuous development

by taking the name data as plaintext in the database, by setting the key as a marker so that it appears in the image below, then the base key will be parsed and marked with the file name as limit. The design can be seen in the image below

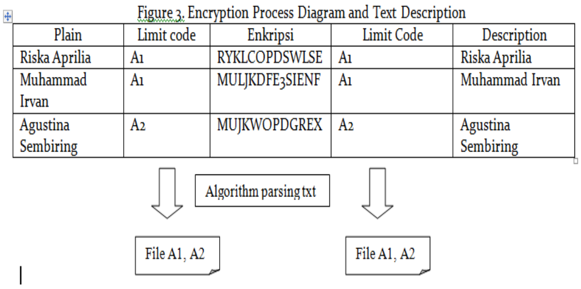


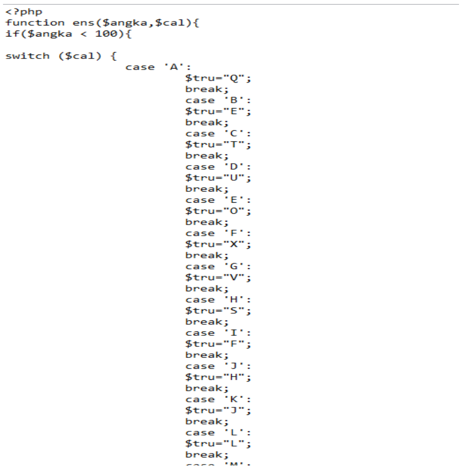
Figure 3. Encryption Process Diagram and Text Description

Plain	Limit code	Enkripsi	Limit Code	Description
Riska Aprilia	A1	RYKLCOPDSWLSE	A1	Riska Aprilia
Muhammad Irvan	A1	MULJKDFE3SIENF	A1	Muhammad Irvan
Agustina Sembiring	A2	MUJKWOPDGREX	A2	Agustina Sembiring

Figure 3. Encryption Process Diagram and Text Description

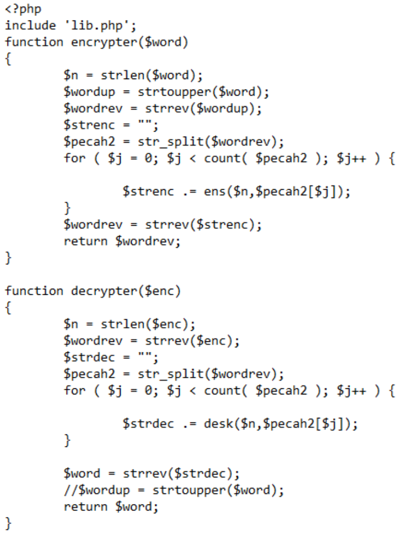
a. countinus testing

In this section, the parsing algorithm tests the key base contained in each file. Is the algorithm successful in encrypting sentences. And also the algorithm should be able to return the text perfectly. The sequence of the algorithm can be seen from the image below:



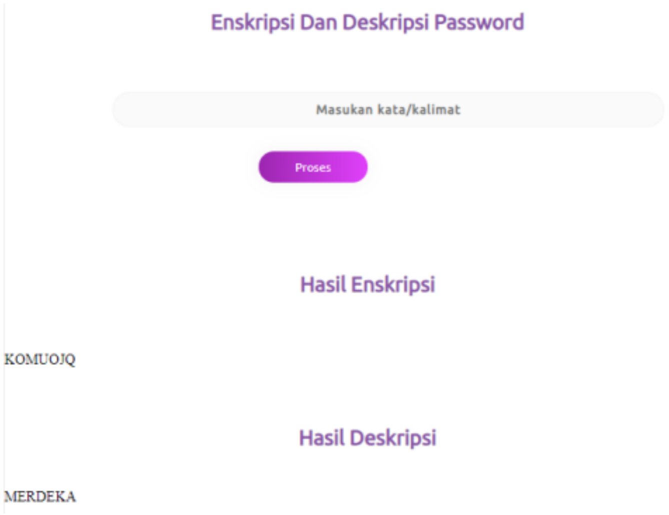
```
<?php
function ens($angka,$cal){
if($angka < 100){

switch ($cal) {
                case 'A':
                        $tru="Q";
                        break;
                        case 'B':
                        $tru="E";
                        break;
                        case 'C':
                        $tru="T";
                        break;
                        case 'D':
                        $tru="U";
                        break;
                        case 'E':
                        $tru="O";
                        break;
                        case 'F':
                        $tru="X";
                        break;
                        case 'G':
                        $tru="V";
                        break;
                        case 'H':
                        $tru="S";
                        break;
                        case 'I':
                        $tru="F";
                        break;
                        case 'J':
                        $tru="H";
                        break;
                        case 'K':
                        $tru="J";
                        break;
                        case 'L':
                        $tru="L";
                        break;
                        case 'M':
```

Figure 4. Testing on Key Base



```
<?php
include 'lib.php';
function encrypter($word)
{
        $n = strlen($word);
        $wordup = strtoupper($word);
        $wordrev = strrev($wordup);
        $strenc = "";
        $pecah2 = str_split($wordrev);
        for ( $j = 0; $j < count( $pecah2 ); $j++ ) {

                $strenc .= ens($n,$pecah2[$j]);
        }
        $wordrev = strrev($strenc);
        return $wordrev;
}

function decrypter($enc)
{
        $n = strlen($enc);
        $wordrev = strrev($enc);
        $strdec = "";
        $pecah2 = str_split($wordrev);
        for ( $j = 0; $j < count( $pecah2 ); $j++ ) {

                $strdec .= desk($n,$pecah2[$j]);
        }

        $word = strrev($strdec);
        //$wordup = strtoupper($word);
        return $word;
}
```

Figure 5. Encryption Algorithm and Description



Enskripsi Dan Deskripsi Password

Hasil Enskripsi

KOMUOJQ

Hasil Deskripsi

MERDEKA

Figure 6. Application encryption and description

3.3 Continues integration

at this stage after the algorithm has successfully encoded the sentence and returns the sentence perfectly then. The algorithm is modified in order to be able to manage data in the database, it is hoped that the algorithm will replace the encryption data that has been provided, the design can be seen in the following figure:

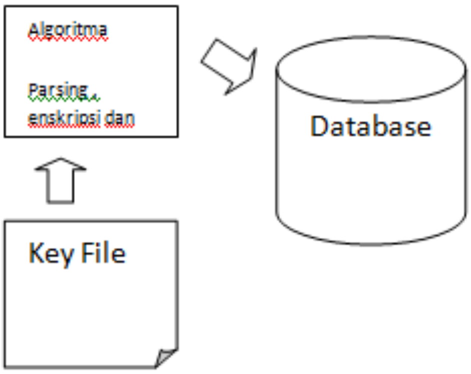
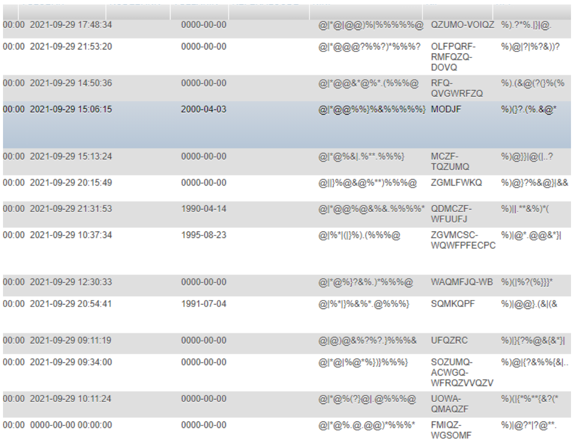


Figure 7. Cryptographic implementation to the database

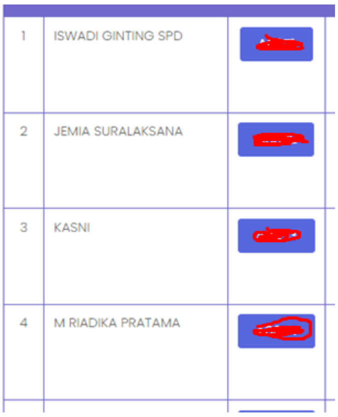
d. Continuous Deployment

In this section the implementation is carried out after testing, the results of the implementation show the success of the algorithm in encrypting and the description of the message and the results are shown in the image below:



00:00	2021-09-29 17:48:34	0000-00-00	@|*@|@@)%|%%%%%@	QZUMO-VOIQZ	%).?*%.|}|@.
00:00	2021-09-29 21:53:20	0000-00-00	@|*@@@?%%?)*%%%?	OLFPQRF-RMFQZQ-DOVQ	%)@|?|%?&))?
00:00	2021-09-29 14:50:36	0000-00-00	@|*@@&*@%*.(%%%@	RFQ-QVGWRFZQ	%).(&@(?{}%(%
00:00	2021-09-29 15:06:15	2000-04-03	@|*@@%%}%&%%%%%}	MODJF	%){}?.(%.&@*
00:00	2021-09-29 15:13:24	0000-00-00	@|*@%&|.%**.%%%}	MCZF-TQZUMQ	%)@}}|@(|..?
00:00	2021-09-29 20:15:49	0000-00-00	@||}%@&@%**)%%%@	ZGMLFWKQ	%)@}?%&@}|&&
00:00	2021-09-29 21:31:53	1990-04-14	@|*@@%@&%&.%%%%*	QDMCZF-WFUUFJ	%)||.**&%)*(
00:00	2021-09-29 10:37:34	1995-08-23	@|%*|(|}%).(%%%@	ZGVMCSC-WQWFPFECPC	%)|@*.@@&*}|
00:00	2021-09-29 12:30:33	0000-00-00	@|*@%}?&%.)*%%%@	WAQMFJQ-WB	%)(|%?(%}}}*
00:00	2021-09-29 20:54:41	1991-07-04	@|%*|}%&%*.@%%%}	SQMKQPF	%)|@@}.(&|(&
00:00	2021-09-29 09:11:19	0000-00-00	@|@)@&%?%?.}%%%&	UFQZRC	%)|}{?%@&{&*}|
00:00	2021-09-29 09:34:00	0000-00-00	@|*@|%@*%})}%%%}	SOZUMQ-ACWGQ-WFRQZVVQZV	%)@|{?&%%{&|..
00:00	2021-09-29 10:11:24	0000-00-00	@|*@%(?}@|.@%%%@	UOWA-QMAQZF	%)(|{*%**{&?(*
00:00	0000-00-00 00:00:00	0000-00-00	@|*@%.@.@@)*%%%*	FMIQZ-WGSOMF	%)|@?*|?@**.

Figure 8. The results of encryption in the data base



1	ISWADI GINTING SPD	[redacted]
2	JEMIA SURALAKSANA	[redacted]
3	KASNI	[redacted]
4	M RIADIKA PRATAMA	[redacted]

Figure 9. Result of description on application

4. CONCLUSION

This research shows good results for the data encrypted in a database in its implementation, this implementation uses Devops design techniques which help researchers in designing software much better. From the results of observations of computer performance in running applications using low resources so that the computer is not burdened to carry out other activities. Computer performance can be seen in the image below.

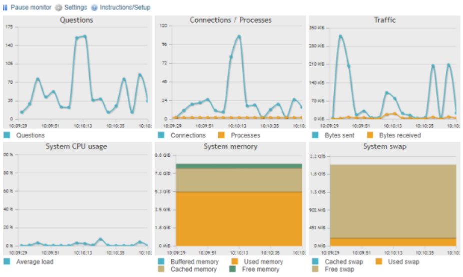


Figure 10. Computer Performance in cryptographic algorithms

As for the shortcomings contained in this study, the authors hope that they can be developed for future research. Amen

5. CONCLUSION

This research shows good results for the data encrypted in a database in its implementation, this implementation uses Devops design techniques which help researchers in designing software much better. From the results of observations of computer performance in running applications using low resources so that the computer is not burdened to carry out other activities. Computer performance can be seen in the image below.

ACKNOWLEDGEMENTS

Praise and gratitude we pray to the presence of Allah SWT for all the abundance and gifts He has given us. And don't forget to say greetings and blessings to our prophet Muhammad SAW. so the opportunity to complete this research, with the title "cryptography generator for prevention sql injection attack in big data". This research was successful with the material support from the rector of the University of Muhammadiyah North Sumatra,. I also don't forget to say to Mrs. Yoshida Sari, M. Kom for her support and support for this research.

REFERENCES

Anggraini E P, 2020, et al "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang " Applied Information Systems and Management (AISM), vol. 3, pp. 69-78.

A. Taryana, A. (2020) Fadli dan S. R. Nurshiami, "Merancang Perangkat Lunak Sistem Penjaminan Mutu Internal (SPMI) Perguruan Tinggi yang Memiliki Daya Adaptasi Terhadap Perubahan Kebutuhan Pengguna secara Cepat dan Sering," Al-Azhar Indonesia Seri Sains dan Teknologi, 2020

Arvind, (2019). "DevOps Life cycle: Everything You Need To Know About DevOps Life cycle Phases," 26 November 2019. [Online]. Available: https://www.edureka.co/blog/devops-lifecycle/. [Diakses 20 April 2020].

Fauzi, F., Al-Khowarizmi, A. K., & Muhathir, M. (2020). The e-Business Community Model is Used to Improve Communication Between Businesses by Utilizing Union Principles. *Journal of Informatics and Telecommunication Engineering*, *3*(2), 252-257.

Martiano, M. (2021). Development of EDUDA as a Media to Build Students' Self-Resistance in Preventing Drugs. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, *2*(1), 169-173.

Martiano, M., & Maulana, H. (2021). Development of A Base Learning Project Model With Online Media In An Effort to Increase Learning Activities During the COVID-19 Pandemic. *International Journal of Basic and Applied Science*, *10*(2), 36-41.

Marnoko, S., & Martiano, M. (2020). Improvement of Quantum Teaching Model Assisted by Comics against Student Learning Outcomes.

Lubis, A. R., & Prayudani, S. (2020, October). Optimization of MSE Accuracy Value Measurement Applying False Alarm Rate in Forecasting on Fuzzy Time Series based on Percentage Change. In *2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE.

Lubis, Arif Ridho, Santi Prayudani, and Muharman Lubis. "Analysis of the Markov Chain Approach to Detect Blood Sugar Level." *Journal of Physics: Conference Series*. Vol. 1361. No. 1. IOP Publishing, 2019.

Tohirin, (2020). "Implementasi DevOps pada Pengembangan Aplikasi e-Skrining Covid-19", jurnal multinetics, vol. 6 no. 1 may 2020

Gaurav Shrivastava, 2013. Using Letters Frequency Analysis in Caesar Cipher with Double Columnar Transposition Technique, International Journal of Engineering Sciences & Research Technology. Vol. 2 Issue 6 ,Page No. 1475-1478, 01 June, ISSN: 2277-9655.

Widyati Suryani, 2021, "Kebocoran Data Pribadi dan Urgensi Pembentukan UU Pelindungan Data Pribadi," Pusat penelitian badan keahlian sekretariat jendral DPR RI,

Wiliam Stalling,(2011). Cryptography and Network Security Principles and Practice, Fifth EditionPearson Education,Inc.,publishing as Prentice Hall, USA,

BIOGRAPHIES OF AUTHORS

	I am a programmer with a magister of computer science from Universitas Sumatera utara and 6 years of software development experience in appsindonesia. And am also a lecturer in information system department in university muhammadiyah Sumatera utara, my research focus on data mining, computer security, and operating system.
	Experienced Founder with a demonstrated history of working in the information technology and services industry. Skilled in User Experience (UX), PHP, User Interface Design, Graphic Design, and Web Design. Strong business development professional with a Pasca Sarjana focused in Sistem Informasi from S2 Sistem Informasi UPI YPTK Padang.