Proceeding of International Conference on Digital Advance Tourism, Management and Technology 2023
Volume. 1 No. 1 2023 e-ISSN : 3031-5999, Hal 243-252
DOI: https://doi.org/10.56910/ictmt.v1i1.67

Implementation Of The Rivest Cipher 4 Method Web-Based Employee Data

Dwi Kuswanto [1], Ach. Khozaimi [2], Deden Nur Eka Abdi [3]
[1,2,3] Universitas Trunojoyo Madura, Bangkalan, Indonesia

Corresponding email: dwi.kuswanto@trunojoyo.ac.id

Abstract. *Data security has always been an exciting topic to discuss in the era of globalization and industrial revolution 5.0. Along with the development of Cryptographic techniques, which continue to develop. Security of data storage techniques is essential in a data security system. The method used in this research is the Rivest Chiper 4 Algorithm. This research takes a case study of employee data storage security in a company that uses local storage as a medium for storing employee data. A web-based employee data collection system with the Rivest Chiper 4 algorithm implemented on the server side. The research results show that in testing the Avalanche Effect Rivest Chiper 4 algorithm with three key character length variations, an average value of 50.87% was obtained. The test results show that the average Avalanche Effect value is more than 50%, indicating that small changes to the plaintext can impact the ciphertext. With the help of Cryptool 1, using Brute Force time testing results with variations in key length, the password cracking time was 33 years with a 6-character key length. The longer the key is used, the longer the completion process will take to crack the ciphertext. Meanwhile, plaintext length is linearly correlated with the length of Brute Force testing time but is insignificant. Hardware performance also affects the estimated time of Brute Force.*

Keywords. *Rivest Chiper 4; kriptografi; Avalanche Effect; Brute Force.*

INTRODUCTION

Data security has always been an exciting topic to discuss in the era of globalization and Industrial Revolution 5.0. Along with the development of cryptographic techniques, which continue to develop. The security of data storage techniques is essential in a data security system. The method used in this research is the Rivest Chiper 4 algorithm. This research takes the form of a case study of employee data storage security in a company that uses local storage as a medium for storing employee data. A web-based employee data collection system with the Rivest Chiper 4 algorithm implemented on the server side.

This research implemented the RC4 encryption algorithm in the company website system, which runs on the server side. In addition, the quality of encryption was analysed using the Avalanche Effect method and a brute force attack to measure the estimated time needed to crack all possible encryption keys.

This research aims to implement the RC4 encryption algorithm method in a web-based employee data collection system and test the quality of encryption using the Avalanche Effect method and the estimated time required for the RC4 algorithm with a brute force attack experiment. Implementing the RC4 algorithm on the company's website system is hoped to protect employee data and minimize the risk of leaking sensitive information. Implementing

Received November 19, 2023; Revised Desember 01 , 2023; Accepted Desember 31, 2023
* Dwi Kuswanto , *dwi.kuswanto@trunojoyo.ac.id*

the RC4 algorithm is also expected to increase efficiency and security in the company's employee data collection process.

METHOD

In order to assess the web application system under development, there are two different kinds of requirements: functional and non-functional. *Functional requirements* are requirements that contain the processes carried out by the system. Non-functional requirements are requirements that focus on the operating characteristics of the system.

- Functional Requirements
  - The user inputs data as a string that will be encrypted and decrypted..
  - The user presses the input button, which will immediately encrypt the input form..
  - The server can carry out the encryption process on data that the user has entered.
  - The server can carry out the decryption process from the database to the interface without destroying the data..
- Non-functional Requirements
  - An analysis of non-functional requirements is needed to support system development with the minimum specifications required to work and run well.

■ System planning

System design explains how the author designs a system. Figure 1 explains the system flowchart as follows:

1. Admin starts accessing the company website.
2. Admin logs in
3. Admin carries out the process of adding employee data
4. Admin fills in the employee data form
5. If the data is valid, the program completes the submission process. If the data is invalid, then repeat the form-filling process.
6. Data is entered into the database
7. Admin can review data that has been encrypted and decrypted
8. Done

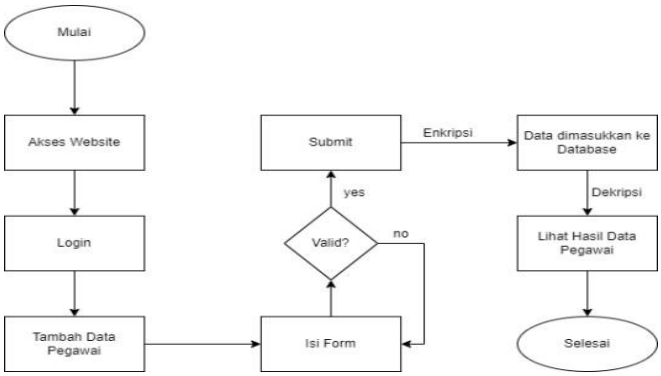


Figure 1: *Flowchart* Sistem

■ System Architecture

The following is the website application system architecture by implementing the RC4 cryptographic algorithm. Figure 2 displays the architectural layout.

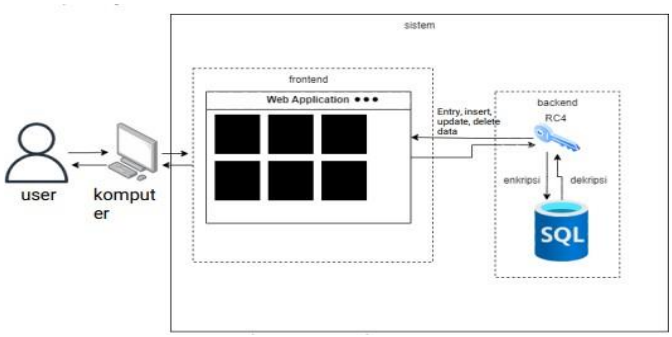


Figure 2: System Architecture

In Figure 2. When a user accesses a website application and processes CRUD data, the system will read the data as plaintext and carry out a cryptographic algorithm process using the RC4 method. The ciphertext will be kept in the website database after the encryption process. The decryption process is the process of calling up data from the database by the user. The user calls data from the database, and the system will carry out the decryption process from ciphertext to plaintext so that the user can easily read the data. This study handles the encryption and decryption procedure on the server side.

After sending data via the HTTP protocol, the server will capture the data; then, the server carries out an encryption process before being entered into the database.

■ Field Encryption

The following database table shows the field columns used to encrypt important employee data.

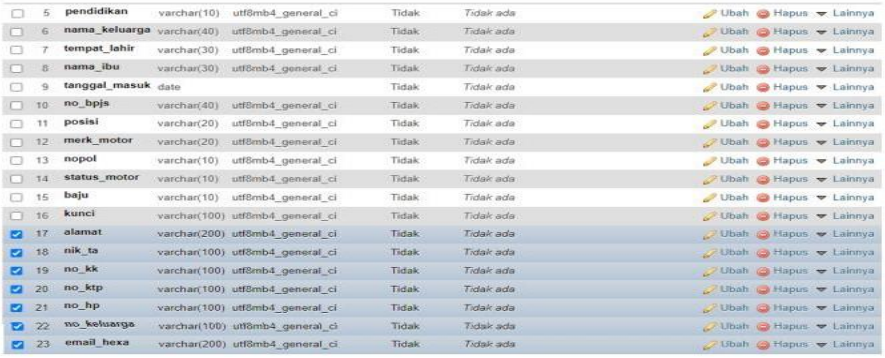


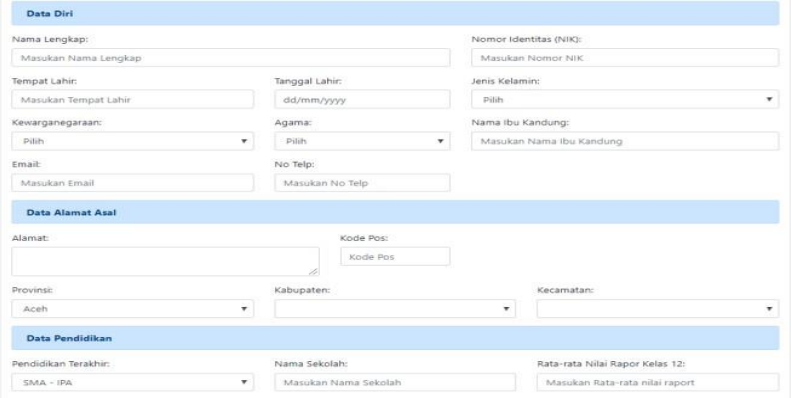
Figure 3: *Field Database*

In Figure 3 it can be seen that the fields in the encryption process are:

a. Alamat
b. Nik_ta
c. No_kk
d. No_ktp
e. No_hp
f. No_keluarga
g. Email

■ Desain Application

The design of this application is made as simple and efficient as possible to make it easier for users to operate it. The following is the form and login design for users to fill in their data:



Gambar 4: *Form* Data Pegawai

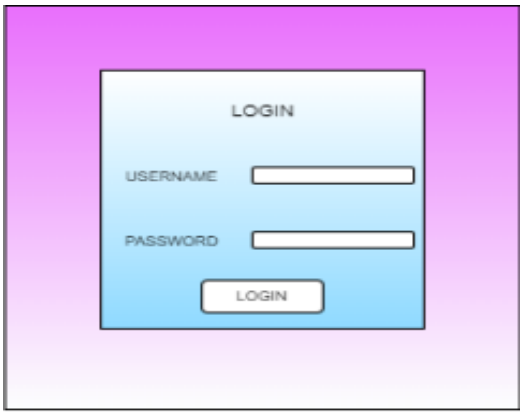
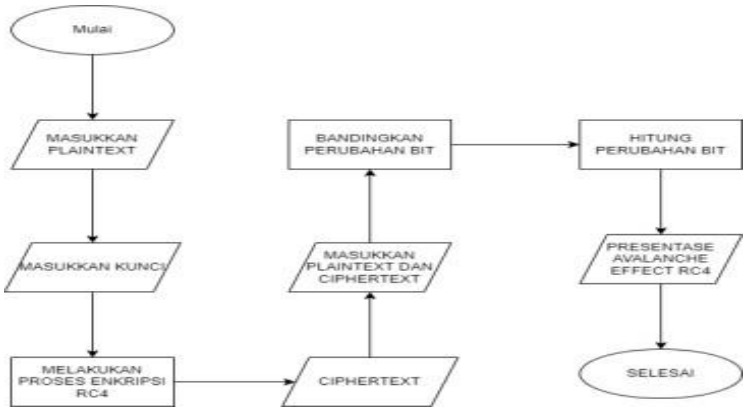


Figure 5: *Form Log In*

■ Testing Scenarios

After designing the system, it continues with the testing process for the RC4 encryption algorithm. The following is a research and testing scenario:

1. **The testing the quality of the RC4 encryption method by calculating the Avalanche Effect Value.**



Gambar 6: Flowchart Testing Avalanche Effect

After designing the system, it continues with the testing process for the RC4 encryption algorithm. The following is a research testing scenario:

Based on Figure 6, the Flowchart flow for testing the Avalanche effect can be explained as follows:

a. Employees enter plaintext employee data
b. Enter the key for encryption
c. The system carries out the encryption process
d. The encryption process produces ciphertext
e. Test the Avalanche Effect by entering plaintext and ciphertext first
f. Comparing bit changes in ciphertext and plaintext
g. Calculating bit changes with the Avalanche effect formula
h. Get the Avalanche Effect percentage

$$\text{Avalanche Effect} = \frac{\sum \text{Perubahan bit}}{\sum \text{seluruh bit chipertext}} \times 100\%$$

2. Testing RC4 encryption using Brute Force Attack

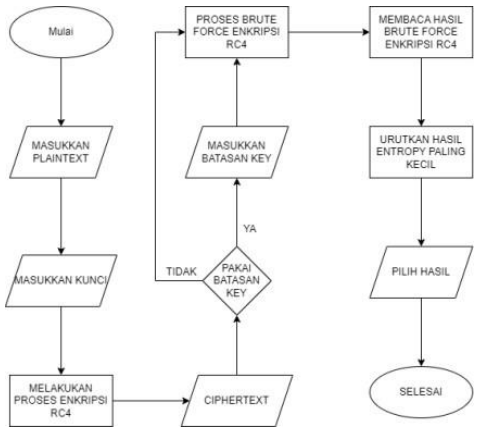


Figure 7: RC4 Encryption Brute Force Testing Flowchart.

Based on Figure 7, the Flowchart flow for testing Brute Force encryption for RC4 can be explained as follows :

a. Employees enter plaintext employee data
b. Enter the key for the encryption process
c. Carry out the encryption process
d. Get the ciphertext
e. Using key constraints
f. Enter the Constraint key
g. Carry out the RC4 encryption brute force process
h. Reads brute force results of RC4 encryption
i. Sort the results with the smallest entropy value
j. Choose brute force results from the smallest entropy value.

RESULT AND DISCUSSION

The user interface display of the employee website includes the login page, employee data input and employee details.

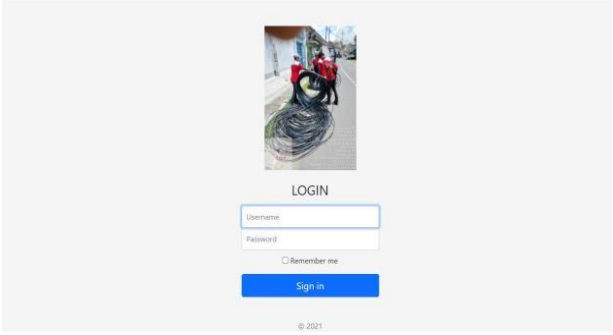


Figure 8: login page

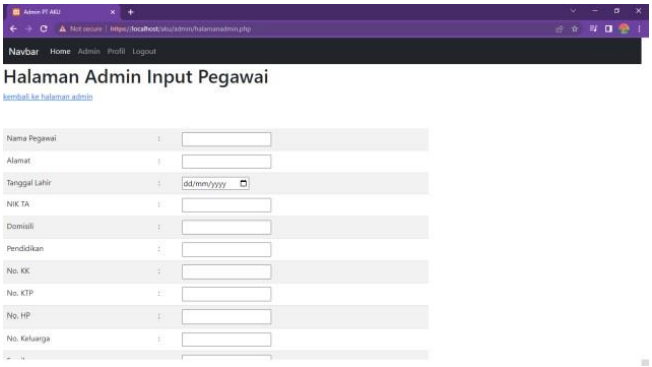


Figure 9: Input data pegawai

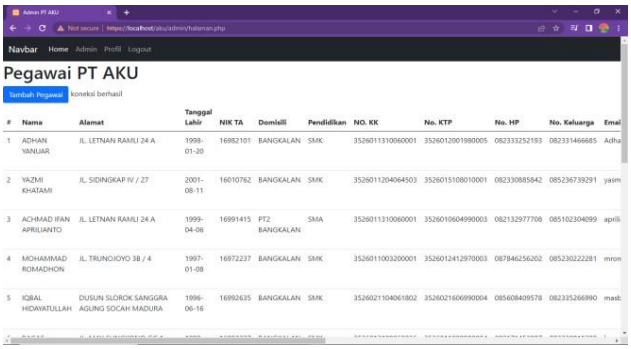


Figure 10: laman detail data pegawai

The employee detail display is the result of RC4 cryptographic decryption.

- **Implementation of RC4 on the Website**

There are several stages to implementing RC4 on a website. The first stage is creating the UI and Database. The author uses Native UI with Bootstrap and uses a MySQL database. RC4 decryption has the same algorithm as encryption because the nature of the RC4 encryption algorithm is symmetric. RC4 decryption uses the encryption function and ciphertext, which will be XORed with a keystream with the same key.

First, capture the array from the POST form. After capturing the value, several variables will be decrypted. The $ SQL function will insert variables in the employee table with columns that correspond to the variables in displaying data by carrying out the decryption process. The function of HEX2BIN is to convert hexadecimal numbers to binary numbers.

■ Website Database

Data that has undergone an encryption process on the server side will be stored in the website database. Data that has undergone an encryption process will become a hexadecimal number. The ciphertext is then stored in the appropriate field.

nik_ta_hexa	no_kk_hexa	no_ktp_hexa	no_hp_hexa	no_keluarga_hexa
62C686BAD74534CA	60C58DB4D54535C8145333BC4E2B9088	60C58DB4D54536CB15523AB24E2B9084	63C88DB1D64736CE17523AB9	63C88DB1D64530CD13
9AF01DFD12EC565D	98F31FFA12EA515D231E833C64481DCF	98F31FFA12EA555E2312833B604D1DCD	9BFE1FFF11EB585726128738	9BFE18FE11ED575C2A
C352728B9CE272A0	C15179849DE772A602F6B5A8C6499F07	C15179849DE773A303F2BCA7C6499F05	C25C79839EE47AA204F1B5A6	C25C7E839DE470A507
AB9BEE854976DE50	A998E5844B75DC5794E8B8D011882BEE	A998E5844B75DF5395E9B3D711882BEC	AA95E08A4F72DF5292E9BAD2	AA95E2804874DF5596E
354CDB555AE7C0B5	374FD05A58E3C2B1A9BFFF9B2A859997	374FD05A58E3C2B6A9BDF6942B8D9991	3442D75A58E9C7B0A0BEF895	3442D05F5BE4C1B6AF
9AF014F410E85258	98F31FFA12EA525E2313833C604D1ECA	98F31FFA12EA515623128A32604D1DC8	9BFE1FFD15EA545A2013833D	9BFE1FFF11EB585E2B
662FF7C854B0CB49	642CF9C055BACF4936CC3A7938574C07	642CF9C055BACE4B36CD317938574E03	6721FFCA57B0CF4731CF3F7C	6721FFCB56B0C64B33
6A8C4FA3612D3702	688F44A7602D3F0799388136EAC471B8	688F44A7602D3C0799348832EBC775B7	6B8244A2632F3E0C90358832	6B8247A863253D069C3
0720F16E431C2EF5	0523FA6E401C2DFB8AD339E25497D2EA	0523FA6E401C2DF38AD331E55497D2EE	062EFF6F44192BF489D13DE4	062EFD6A421C2DF28A

Figure 11: Hasil enkripsi pada database

■ Avalanche Effect Test Results

Test results were obtained from 3 variations of key characters (5, 9 and 16, respectively) with the same plaintext and key. Plaintext is obtained from the names of employees at the company. The test scheme compares the number of plaintext bit changes with the total amount of plaintext multiplied by 100%.

Table 1. Avalanche effect test results with 5 key characters

Nomor	Nama (plaintext)	Key	Ciphertext	Binary plaintext	Binary ciphertext	Bit yang berubah	Total bit	*Avalanche effect (%)*
1	ACHMAD IFAN APRILIANTO	12345	vp/mZ,&Ýbš□™6□_µ/xwé ['\x11', 'v', 'p', '/', 'm', 'Z', ',', '&', 'Ý', 'b', '\x9a', '\x90', '\x99', '6', '\x80', '_', 'µ', '/', 'x', 'w', 'é', '\x07']	01000001 01000011 01001000 01001101 01000001 01000100 00100000 01001001 01000110 01000001 01001110 00100000 01000001 01010000 01010010 01001001 01001100 01001001 01000001 01001110 01010100 01001111	00010001 01110110 01110000 00101111 01101101 01011010 00101100 00100110 11011101 01100010 10011010 10010000 10011001 00110110 10000000 01011111 10110101 00101111 01111000 01110111 11101001 00000111	83	176	47,2%
2	MOHAMMAD ROMADHON	12345	zp#aSM»q›ý™"šY· ['\x1d', 'z', 'p', '#', 'a', 'S', 'M', '+', '»', 'q', '\x9b', 'ý', '\x99', '"', '\x9a', 'Y', '·']	01001101 01001111 01001000 01000001 01001101 01001101 01000001 01000100 00100000 01010010 01001111 01001101 01000001 01000100 01001000 01001111 01001110	00011101 01111010 01110000 00100011 01100001 01010011 01001101 00101011 10111011 01110001 10011011 11111101 10011001 00100010 10011010 01011001 10110111	63	136	46,3%
3	ALBAYQONI SIMANJUTAK	12345	yz#uOC!Ò‡ù•'œ\¬2xr ['\x11', 'y', 'z', '#', 'u', 'O', 'C', '!', 'Ò', '\x03', '\x87', 'ù', '\x95', '"', '\x9c', '\\', '¬', '2', 'x', 'r']	01000001 01001100 01000010 01000001 01011001 01010001 01001111 01001110 01001001 00100000 01010011 01001001 01001101 01000001 01001110 01001010 01010101 01010100 01000001 01001011	00010001 01111001 01111010 00100011 01110101 01001111 01000011 00100001 11010010 00000011 10000111 11111001 10010101 00100111 10011100 01011100 10101100 00110010 01111000 01110010	75	160	46,9%
4	BAGAS RINALDIY WIBOWO	12345	t□#□>^&Õbˆô‘?òA°$vnò ['\x12', 't', '\x7f', '#', '\x7f', '>', '^', '&', 'Õ', 'b', '\x98', 'ô', '\x91', '?', 'ò', 'A', '°', '$', 'v', 'n', 'ò']	01000010 01000001 01000111 01000001 01010011 00100000 01010010 01001001 01001110 01000001 01001100 01000100 01001001 01011001 00100000 01010111 01001001 01000010 01001111 01010111 01001111	00010010 01110100 01111111 00100011 01111111 00111110 01011110 00100110 11010101 01100010 10011000 11110100 10010001 00111111 11110010 01000001 10110000 00100100 01110110 01101110 11110010	81	168	48,2%
Presentase Rata Rata %								47,15%

Table 2. Avalanche effect test results with 9 key characters

Nomor	Nama (plaintext)	Key	Ciphertext	Binary plaintext	Binary ciphertext	Bit yang berubah	Total bit	*Avalanche effect (%)*
1	ACHMAD IFAN APRILIANTO	BANGKALAN	<ÍI[ê_ `Ì`º-+t@ó- (['<', 'Í', 'I', '\x16', '[', 'ê', '_', '\xa0', '`', 'Ì', '\x93', 'º', '\x0f', '\xad', '+', 't', '\x0c', '\x10', '@', 'ó', '\xad', '\x0b'])	01000001 01000011 01001000 01001101 01000001 01000100 00100000 01001001 01000110 01000001 01001110 00100000 01000001 01010000 01010010 01001001 01001100 01001001 01000001 01001110 01010100 01001111	00111100 11001101 01001001 00010110 01011011 11101010 01011111 10100000 01100000 11001100 10010011 10111010 00001111 10101101 00101011 01110100 00001100 00010000 01000000 11110011 10101101 00001011	94	176	53,4%
2	MOHAMMAD ROMADHON	BANGKALAN	0ÁIWã>-ß'×¹1r ['0', 'Á', 'I', '\x1a', 'W', 'ã', '>', '\xad', '\x06', 'ß', '\x92', '×', '\x0f', '¹', '1', 'r', '\x0e']	01001101 01001111 01001000 01000001 01001101 01001101 01000001 01000100 00100000 01010010 01001111 01001101 01000001 01000100 01001000 01001111 01001110	00110000 11000001 01001001 00011010 01010111 11100011 00111110 10101101 00000110 11011111 10010010 11010111 00001111 10111001 00110001 01110010 00001110	75	136	55,1%
3	ALBAYQONI SIMANJUTAK	BANGKALAN	<ÂCCÿ0§o-Ž Ó¼7w @ö ['<', 'Â', 'C', '\x1a', 'C', 'ÿ', '0', '§', 'o', '\xad', '\x8e', 'Ó', '\x03', '¼', '7', 'w', '\x15', '\r', '@', 'ö']	01000001 01001100 01000010 01000001 01011001 01010001 01001111 01001110 01001001 00100000 01010011 01001001 01001101 01000001 01001110 01001010 01010101 01010100 01000001 01001011	00111100 11000010 01000011 00011010 01000011 11111111 00110000 10100111 01101111 10101101 10001110 11010011 00000011 10111100 00110111 01110111 00010101 00001101 01000000 11110110	86	160	51,2%
4	BAGAS RINALDIY WIBOWO	BANGKALAN	?ÏFIŽ - hÌ'Þ¤Yj Nê¶ ['?', 'Ï', 'F', '\x1a', 'I', '\x8e', '-', '\xa0', 'h', 'Ì', '\x91', 'Þ', '\x07', '¤', 'Y', 'j', '\t', '\x1b', 'N', 'ê', '¶']	01000010 01000001 01000111 01000001 01010011 00100000 01010010 01001001 01001110 01000001 01001100 01000100 01001001 01011001 00100000 01010111 01001001 01000010 01001111 01010111 01001111	00111111 11001111 01000110 00011010 01001001 10001110 00101101 10100000 01101000 11001100 10010001 11011110 00000111 10100100 01011001 01101010 00001001 00011011 01001110 11101010 10110110	92	168	54,8%
Presentase Rata Rata %								53,62%

Table 3. Avalanche effect test results with 16 key characters

Nomor	Nama (plaintext)	Key	Ciphertext	Binary plaintext	Binary ciphertext	Bit yang berubah	Total bit	*Avalanche effect (%)*
1	ACHMAD IFAN APRILIANTO	3526012001980005	Ù□î•zéo□□m·ƒ□ƒÓäÑ§F ['Ù', '\x7f', 'î', '\x95', 'z', 'é', 'o', '\x90', '\x9d', 'm', '·', '\x83', '\x80', '\x83', '\x01', 'Ó', 'ä', 'Ñ', '\r', '§', 'F', '\r']	01000001 01000011 01001000 01001101 01000001 01000100 00100000 01001001 01000110 01000001 01001110 00100000 01000001 01010000 01010010 01001001 01001100 01001001 01000001 01001110 01010100 01001111	11011001 01111111 11101110 10010101 01111010 11101001 01101111 10010000 10011101 01101101 10110111 10000011 10000000 10000011 00000001 11010011 11100100 11010001 00001101 10100111 01000110 00001101	88	176	50%
2	MOHAMMAD ROMADHON	3526012001980005	Õsî™và• û~¶î€ —Õæ ['Õ', 's', 'î', '\x99', 'v', 'à', '\x0e', '\x9d', 'û', '~', '¶', 'î', '\x80', '\x97', '\x1b', 'Õ', 'æ']	01001101 01001111 01001000 01000001 01001101 01001101 01000001 01000100 00100000 01010010 01001111 01001101 01000001 01000100 01001000 01001111 01001110	11010101 01110011 11101110 10011001 01110110 11100000 00001110 10011101 11111011 01111110 10110110 11101110 10000000 10010111 00011011 11010101 11100110	73	136	53,7%
3	ALBAYQONI SIMANJUTAK	3526012001980005	Ùpä™bü ['Ù', 'p', 'ä', '\x99', 'b', 'ü', '\x00', '\x97', '\x92', '\x0c', 'ª', 'ê', '\x8c', '\x92', '\x1d', 'Ð', 'ý', 'Ì', '\r', '¢']	01000001 01001100 01000010 01000001 01011001 01010001 01001111 01001110 01001001 00100000 01010011 01001001 01001101 01000001 01001110 01001010 01010101 01010100 01000001 01001011	11011001 01110000 11100100 10011001 01100010 11111100 00000000 10010111 10010010 00001100 10101010 11101010 10001100 10010010 00011101 11010000 11111101 11001100 00001101 10100010	84	160	52,5%
4	BAGAS RINALDIY WIBOWO	3526012001980005	Ú}á™h□□•mµçˆŠsÍáÚ¾] ['Ú', '}', 'á', '\x99', 'h', '\x8d', '\x1d', '\x90', '\x95', 'm', 'µ', 'ç', '\x88', '\x8a', 's', 'Í', 'á', 'Ú', '\x03', '¾', ']']	01000010 01000001 01000111 01000001 01010011 00100000 01010010 01001001 01001110 01000001 01001100 01000100 01001001 01011001 00100000 01010111 01001001 01000010 01001111 01010111 01001111	11011010 01111101 11100001 10011001 01101000 10001101 00011101 10010000 10010101 01101101 10110101 11100111 10001000 10001010 01110011 11001101 11100001 11011010 00000011 10111110 01011101	86	168	51,2%
Presentase Rata Rata %								51,85%

The table above makes it possible to compute the average percentage of the Avalanche Effect:

$$\text{Rata} - \text{rata Avalanche Effect} = \frac{47.15 + 53.62 + 51.85}{3} \times 100\%$$
$$= \frac{152.62}{3} \times 100\%$$
$$= 50{,}87\%$$

The average results of the Avalanche Effect test showed that it was 50.87%, indicating that the average Avalanche Effect value was more than 50%. This indicates that small changes to the plaintext can impact the ciphertext..

■ Brute Force Results

In Brute force testing, the RC4 encryption algorithm uses CrypTool 1 software for testing in brute force attacks. The table above shows that in the Brute Force process in the RC4 encryption algorithm, the key length greatly influences the length of the attack process. With the plaintext "Deden Nur Eka Abdi" and with key lengths "3, 4, 5, and 6", the resulting Brute Force processing time data is 56 seconds each for key length 3, 4 hours for key length 4, 40 days for key length 5, and 33 years for key length 6. The length of time in the Brute Force process results from the estimated system completing the experiment for all possibilities. Password cracking time refers to the permutation of the key length. The longer the key is used, the longer the completion process will take to crack the ciphertext using the Brute Force method.

Table 4: Results of Brute Force time testing compared to a critical length.

No	Plaintext (Nama)	Kunci	Panjang Kunci	Waktu Bruteforce
1	Deden Nur Eka Abdi	123	3	56 detik
2		1927	4	4 jam
3		Setro	5	40 hari
4		madiun	6	33 tahun

Table 5: Brute Force testing with 3 key bits

No	Jumlah Karakter	Waktu Bruteforce
1	100	59 detik
2	200	1 menit 4 detik
3	300	1 menit 5 detik
4	400	1 menit 9 detik
5	500	1 menit 10 detik

Table 6: Brute Force testing with 4 key bits

No	Jumlah Karakter	Waktu Bruteforce
1	100	4 jam 16 menit
2	200	4 jam 18 menit
3	300	4 jam 20 menit
4	400	4 jam 21 menit
5	500	4 jam 25 menit

Table 7: Brute Force testing with 5 key bits

No	Jumlah Karakter	Waktu Bruteforce
1	100	46 hari 14 jam
2	200	47 hari 5 jam
3	300	47 hari 14 jam
4	400	47 hari 21 jam
5	500	47 hari 22 jam

Plaintext length can affect Brute Force testing duration, but not very much, according to the Brute Force testing chart with plaintext character length. Hardware performance also affects the estimated time for the Brute Force to complete the attack process.

CONCLUSION

From the results of several research trials that have been carried out, it can be concluded.

1. The Avalanche Effect method in testing carried out with crucial character lengths of 5, 9 and 16, respectively, obtained an average Avalanche Effect of 50.87%. This shows that the average Avalanche Effect value is more than 50%, indicating that small changes to the plaintext can impact the ciphertext.
2. With the help of Cryptool 1 for Brute Force time testing results with variations in key length, it was obtained that the password cracking time was 33 years with a 6-character key length. The longer the key is used, the longer the completion process will take to crack the ciphertext. Meanwhile, plaintext length is linearly correlated with the length of Brute Force testing time but is not significant. Hardware performance also affects the estimated time of Brute Force.

REFERENCES

Nugroho, N. B. Z. Azmi, and S. N. J. J. S. Arif. (2016). Aplikasi Keamanan Email Menggunakan Algoritma Rc4.

Munir, R. J. I. (2006). Diktat Kuliah IF5054 Kriptografi. ProgramStudi Teknik Informatika, Sekolah Teknik Elektro dan Informatika. Bandung.

Andrico, A. and M. J. S. Syafrullah. (2018). Aplikasi Enkripsi Database Menggunakan Algortima RC4 Berbasis Desktop, vol. 1, no. 3, pp. 1011- 1017.

Ammary, G. and S. J. S. Mulyati. (2018). Aplikasi Kriptografi Untuk Keamanan Databse Dengan Metode RC4 Dan Elgamal Berbasis Web Pada Jxl DesignCo, vol. 1, no. 2, pp. 815-820, 2018.

Stiawan, D. (2005). Sistem Keamanan Komputer. Elex Media Komputindo. Jakarta.

Munir, R. J. I. (2006). Kriptografi. Bandung.

Irfianti, A. D. (2007). Metode pengamanan enskripsi RC4 streamcipher untuk aplikasi pelayanan gangguan. Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

Jindal,P. and B. Singh. 2014. Performance analysis of modified RC4 encryption algorithm. International conference on recent advances and innovations in engineering (ICRAIE-2014): IEEE, pp. 1-5.

Putra, Y. P., F. Nuraeni, and A. M. J. I. J. Sahrin. 2021. Implementasi Steganografi dan Algorithma RC4 untuk meningkatkan keamanan data penjualan voucher game elektronik (Studi Kasus: Berewek Cell), vol. 9, no. 2, pp. 186-200.

Sriadhi, S., R. Rahim, and A. S. Ahmar. 2018. RC4 Algorithm visualization for cryptography education. Journal of Physics: Conference Series, vol. 1028, no. 1: IOP Publishing, p. 012057.