3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

PENERAPAN ALGORITMA *RIVEST CODE 4 (RC4)* BERBASIS *WEB* UNTUK KEAMANAN DATA PADA SMP NEGERI 25 TANGERANG

Dhimaz Syaleh Bagaskara[1*], Pipin Farida Ariyani[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]1911501276@student.budiluhur.ac.id, [2]pipin.faridaariyani@budiluhur.ac.id
(* : corresponding author)

Abstrak-Kriptografi merupakan ilmu yang berfokus pada keamanan data melalui algoritma enkripsi dan dekripsi. Penggunaan metode kriptografi pada SMP *NEGERI 25 KOTA TANGERANG* dengan institusi pendidikan yang *progresif*, sangat penting. Di sini, terdapat sistem pengarsipan penyimpanan berkas berharga seperti soal ujian dan daftar nilai siswa dalam direktori lokal. Untuk melindungi *integritas* dan kerahasiaan data serta meminimalkan risiko kehilangan, sistem pengarsipan harus ditingkatkan. Dalam hal ini, metode kriptografi dapat diandalkan dengan menggunakan algoritma seperti *Rivest Code (RC4). RC4*, sebagai algoritma *stream cipher* yang mampu mengamankan data dengan baik. Dengan penerapan kriptografi ini, berkas-berkas penting pada SMP *Negeri 25 Tangerang* akan terlindungi karena hanya pihak berwenang yang dapat mengaksesnya melalui penggunaan kunci yang dirahasiakan. Hasil penelitian, perancangan, dan pengujian menunjukkan bahwa aplikasi ini efektif menerapkan algoritma *RC4*, sehingga berkas-berkas seperti ujian sekolah dan daftar nilai siswa akan aman terenkripsi dan dapat kembali seperti semula setelah didekripsi.

Kata Kunci: *Kriptografi, Rivest Code 4 (RC4), Enkripsi, Dekripsi*

APPLICATION OF WEB-BASED RIVEST CODE 4 (RC4) ALGORITHM FOR DATA SECURITY AT SMP NEGERI 25 TANGERANG

Abstract-*Cryptography is a science that focuses on data security through encryption and decryption algorithms. The use of cryptographic methods at SMP Negeri 25 Kota Tangerang, a progressive educational institution, is of utmost importance. Here, there is a valuable file storage and archiving system, including exam questions and student grade lists, within the local directory. To safeguard data integrity and confidentiality while minimizing the risk of loss, the archiving system needs enhancement. In this regard, cryptography methods can be relied upon by employing algorithms such as the Rivest Cipher (RC4). RC4, serving as a stream cipher algorithm, is capable of effectively securing data. By implementing this cryptography method, important files at SMP Negeri 25 Tangerang will be protected, as only authorized personnel can access them through the use of a confidential key. Research, design, and testing results indicate that this application effectively implements the RC4 algorithm, ensuring that files such as school exams and student grade lists will be securely encrypted and can be restored to their original state after decryption.*

Keywords*: Cryptography, Rivest Code (RC4), Encryption, Decryption*

1. PENDAHULUAN

SMP *NEGERI 25 KOTA TANGERANG* merupakan salah satu institusi pendidikan yang maju dan progresif, terdapat sebuah sistem pengarsipan yang menggunakan direktori lokal untuk menyimpan file-file penting Setiap harinya. Para staf harus bekerja keras untuk mengelola dan menyimpan berbagai dokumen penting dalam direktori lokal tersebut. File-file berharga, seperti soal ujian setiap mata pelajaran dan daftar nilai siswa yang ditempatkan di dalam folder yang tertata dengan baik. Namun tetap ada risiko kehilangan atau akses yang tidak sah terhadap file-file tersebut. Lembaga ini menyadari betapa pentingnya menjaga keamanan dan kerahasiaan data dalam era digital ini. Dengan demikian, diperlukan sebuah sistem keamanan data yang mampu memastikan kerahasiaan informasi dan teks. [1]. Sehingga dapat mengurangi risiko dan memastikan kelancaran operasional mereka dalam memberikan pendidikan yang berkualitas[2].

Kriptografi adalah disiplin ilmu yang memfokuskan pada penggunaan ilmu matematika untuk menjaga keamanan data atau informasi, memastikan integritas data agar tidak diubah tanpa izin, *mengotentikasi entitas* yang terlibat dalam proses, dan *mengotentikasi* asal data untuk memastikan data berasal dari sumber yang sah. [3]. Tujuan Kriptografi sendiri untuk mengubah pesan teks asli *(plainteks)* menjadi pesan terenkripsi *(cipherteks)*[4]. Peluang bagi seseorang yang tidak memiliki kunci dekripsi untuk mendapatkan naskah asli dalam waktu singkat sangat kecil. [5]. Oleh karena itu metode kriptografi diperlukan untuk mengatasi masalah tersebut

dengan menggunakan algoritma untuk proses enkripsi dan dekripsinya. Dengan hal ini, dapat dipastikan bahwa data akan tetap terlindungi dan hanya dapat diakses oleh pihak yang memiliki kunci.

Aplikasi yang akan dibuat menggunakan algoritma enkripsi *Rivest Code (RC4)*. Perbedaan penelitian ini dengan penelitian sebelumnya yaitu aplikasi ini menggunakan 1 user untuk login dan meng-enkripsi file asli yang artinya file sebelum dienkripsi akan diganti dengan file yang ter-enkripsi. RC4 adalah algoritma yang bersifat *stream cipher* dimana proses pengamanannya berfokus pada satu *bit* per *byte* data[6]. RC4 adalah algoritma kriptografi yang menggunakan kunci berukuran 1 hingga 256 *byte* untuk menginisialisasi sebuah tabel sepanjang 256 *byte*. Tabel ini berfungsi sebagai dasar untuk menghasilkan deretan bilangan acak yang digunakan dalam metode *XOR* untuk mengubah teks biasa menjadi teks terenkripsi *(ciphertext)*[7]. Karena RC4 adalah algoritma simetris yang kuncinya harus dirahasiakan, algoritma ini banyak digunakan dalam berbagai aplikasi dan umumnya dianggap aman[8]. [9]Algoritma ini memiliki kecepatan yang tinggi dalam melakukan enkripsi serta dekripsi data dan relatif sederhana dibandingkan algoritma enkripsi yang lainnya. Tahap pertama dalam algoritma RC4 adalah *KSA (Key Scheduling Algorithm)*, di mana proses ini menciptakan *S-Box (Array S)* dengan panjang 256 *byte* (*indeks* 0 sampai 255) berdasarkan kunci enkripsi. Berikut adalah gambaran *KSA* dalam bentuk *pseudocode:*

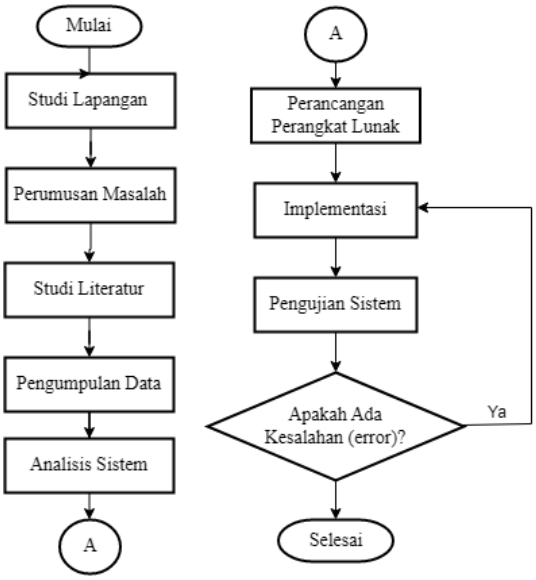
For i = 0 to 255
S[i] := i
J := 0
For i = 0 to 255
j := (j + S[1] + *key[mod keylength]) mod* 256
swap (S[i] ,S[j])

Langkah selanjutnya dalam algoritma RC4 adalah *PRGA (Pseudo-Random Generation Algorithm)*, yang merupakan tahap pembangkitan bilangan *pseudo*-acak di mana *state automaton* beroperasi untuk menghasilkan *keystream.* Pada setiap putaran, bagian *keystream* sebesar 1 *byte* (dengan nilai antara 0 sampai dengan 255) yang dikeluarkan oleh *PRGA* berdasarkan *state S.* Berikut adalah algoritma *PRGA* dalam bentuk *pseudo-code*:

i = 0; j = i
for i = 0 <= jumlah_karakter_*plaintext* – 1 do
i <= (i + 1) *mod* 256
j <= (j + S[i]) *mod* 256
swap (S[i], S[j] *mod* 256
t <= (S[i] + S[j] *mod* 256
K <= S[t] *(*keystream*)*
c <= K + i

2. METODE PENELITIAN

Metode penelitian digunakan bertujuan untuk memberikan pedoman atau panduan dasar dalam melaksanakan penelitian. Penelitian dimulai dengan melakukan kunjingan ke lokasi yaitu SMP *Negeri 25 Tangerang* dan melakukan wawancara dengan salah satu staf pada institusi pendidikan tersebut untuk mengidentifikasi permasalahan yang ada dan meminta data yang diperlukan untuk penelitian. Pada gambar 1 adalah flowchart urutan metode penelitian yang digunakan.



Gambar 1. Metode Penelitian

2.1 Analisis Masalah

SMP *NEGERI 25 KOTA TANGERANG* menghadapi masalah keamanan terkait dokumen penting yang sering kali hanya disimpan dalam komputer tanpa perlindungan yang memadai. Karena situasi ini, ada potensi besar terjadinya pencurian data. Oleh karena itu, diperlukan suatu aplikasi keamanan data untuk melindungi dokumen secara efektif, sehingga hanya pihak yang berwenang dan memiliki akses untuk melihat dan mengubahnya.[10]

2.2 Penyelesaian Masalah

Dalam masalah ini, dibutuhkan sebuah sistem untuk menjaga kerahasiaan data agar tidak dapat diakses oleh pihak lain. Oleh karena itu, sebuah aplikasi berbasis web akan dibuat menggunakan bahasa pemrograman PHP. Aplikasi ini menggunakan algoritma kriptografi RC4 untuk mengenkripsi data asli, sehingga data tetap aman dan tidak dapat dilihat atau diubah oleh pihak yang tidak berwenang. Proses enkripsi ini akan mengubah data asli menjadi data ter-enkripsi, dan data tersebut dapat dikembalikan ke keadaan semula atau didekripsi tanpa mengalami perubahan atau kerusakan. Dengan adanya aplikasi ini, diharapkan beberapa aspek keamanan data dapat terpenuhi sehingga data sensitif akan tetap terjaga dan tidak dapat diakses oleh pihak yang tidak berwenang[10].

2.3 Rancangan Pengujian

Rancangan pengujian akan dilakukan untuk menguji fungsi pada fitur halaman *web* yang dibuat, antara lain halaman *web login*, halaman *web home*, halaman *web encryption*, halaman *web decryption*. Dapat dilihat pada tabel 1.

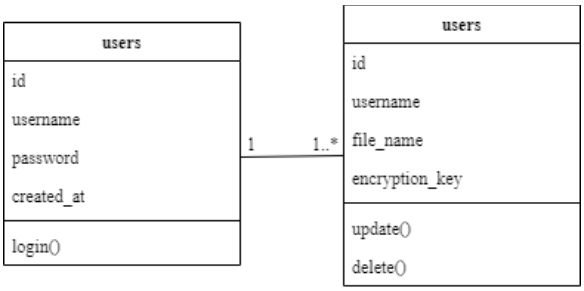
Tabel 1. Rancangan Pengujian

No	Skenario Pengujian	Hasil Yang Diharapkan
1	Mengisi *username* dan *password*	Masuk ke halaman *Home*
2	Tombol menu *Encryption*	Masuk ke halaman enkripsi
3	Mengisi *form* untuk enkripsi	*File* Berhasil di enkripsi dan otomatis download
4	Tombol menu *Decryption*	Masuk ke halaman dekripsi
5	Mengisi *form* untuk dekripsi	*File* Berhasil di dekripsi dan otomatis download
6	Tombol menu *Encryption Data File*	Memunculkan *file* terenkripsi

2.4 Rancangan Basis Data

a. *Class Diagram*

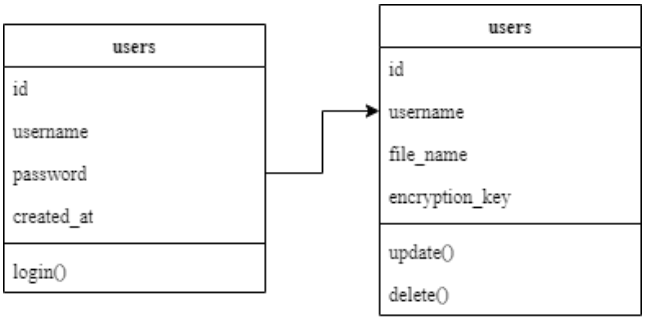
Class Diagram berguna untuk menggambarkan struktur dan hubungan antara kelas dalam sistem. Diagram ini memberikan penjelasan *atribut* dan *metode* pada setiap kelas yang dapat dilihat pada gambar 2.



Gambar 2. *Class Diagram*

b. *Logical Record Structure (LRS)*

Logika Record Structure (LRS) adalah struktur data yang menggambarkan cara setip informasi dapat di organisasikan dalam satu rekaman pada *basis data*. Dengan menggunakan *Logika Record Structure (LRS), sistem basis data* dapat mengatur dan menyimpan informasi yang akan disimpan. Pada gambar 3 adalah *Logika Record Structure (LRS)* yang dibuat.



Gambar 3. *Logical Record Structure*

c. Spesifikasi *Basis Data*

1) Tabel users

Nama Database : db_tugas_akhir
Nama Tabel : *users*
Isi : Data pengguna
Primary Key : *id*

Tabel 2. *users*

No	*Field*	Tipe *Data*	Panjang	Keterangan
1	*Id*	*Int*	11	*Id* Pengguna
2	*username*	*Varchar*	40	*Username*
3	*password*	*Varchar*	100	Kata Sandi
4	*Created_at*	*Date*	-	Tanggal Dibuat

2) Tabel files

Nama Database : db_tugas_akhir
Nama Tabel : *files*
Isi : Data file enkripsi
Primary Key : *id*

Tabel 3. *Files*

No	*Field*	Tipe Data	Panjang	Keterangan
1	*Id*	*Int*	11	*Id* Pengguna
2	*username*	*Varchar*	40	*Username*
3	*file_name*	*Varchar*	100	Nama File
4	*encryption_key*	*Varchar*	20	Kunci *encryption*
5	*Created_at*	*Date*	-	Tanggal Dibuat

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Analisa masalah dilakukan untuk menentukan ketetapan aplikasi yang akan dibuat berdasarkan informasi yang dikumpulkan sebelumnya. Aplikasi ini harus memiliki dua proses utama yaitu proses enkripsi untuk pegamanan data dan proses dekripsi untuk mengembalikan seperti semula agar dapat dibaca pengguna. Selain itu adanya proses *validasi* untuk memastikan hanya pengguna yang memiliki izin yang dapat mengakses aplikasi.

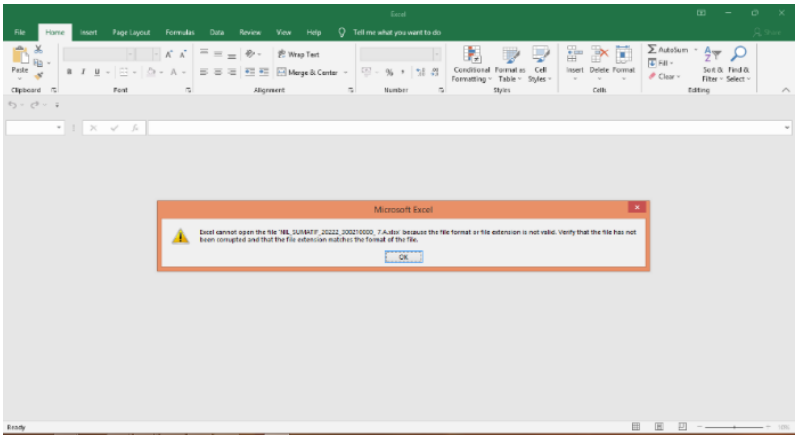
3.2 Menu *Encryption* dan *Decryption*

a. Tampilan menu *form Encryption*

Halaman *encryption* akan muncul saat pengguna memilih menu *encryption* dan berisi perintah untuk memasukan file beserta *key* (kunci) untuk melakukan pengamanan data. Berikut tampilan menu *form encryption* pada gambar 4.

Gambar 4. Tampilan menu *form Encryption*

Pada gambar 5 dapat dilihat file setelah di enkripsi.



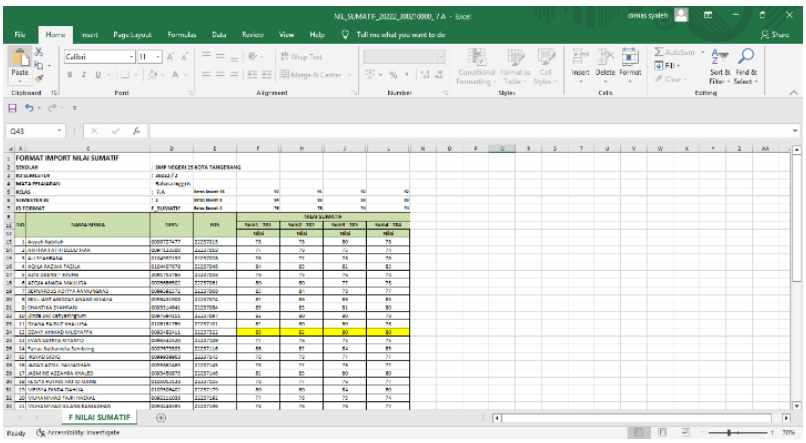
Gambar 5. file setelah di enkripsi

b. Tampilan menu *form Decryption*

Halaman *decryption* akan muncul saat pengguna memilih menu *decryption* dan berisi perintah untuk memasukan file beserta *key* (kunci) dimana *key* (kunci) yang diinput harus sama dengan *key* (kunci) yang diinput saat enkripsi untuk melakukan pengembalikan ke data asli. Tampilan menu *form decryption* yang terlampir pada gambar 6.

Gambar 6. Tampilan menu *form Decryption*

Pada gambar 7 dapat dilihat file setelah di dekripsi.



Gambar 7. file setelah di dekripsi

3.3 Pengujian Proses Encryption dan Decryption

Pengujian ini akan dilakukan dengan cara membandingan antara besar file yang diupload dengan waktu proses enkripsi dan dekripsi. Yang terlampir pada tabel 4 dan tabel 5.

Tabel 4. Pengujian *Proses Encryption*

No	Ukuran File Asli *(byte)*	Nama File	Ukuran File *Encryption (byte)*	Waktu *Encryption (Milisecond)*
1	538624	SOAL TRY OUT B.ING KLS 9 2023.pdf	538624	810
2	411648	SOAL PTS GENAP B.ING KLS 8 SMT 2 THN 2021	411648	600
3	13312	NIL_SAS_20222_300210000_ 7.A	13312	20
4	15360	NIL_SUMATIF_20222_300210000_ 7.A	15360	30
5	13312	NIL_SAS_20222_300210000_ 7.B	13312	20
6	15360	NIL_SUMATIF_20222_300210000_ 7.B	15360	30

7	13312	NIL_SAS_20222_300210000_ 7.C	13312	20
8	15360	NIL_SUMATIF_20222_300210000_ 7.C	15360	30

Tabel 5. Pengujian *Proses Decryption*

No	Ukuran File Asli *(byte)*	Nama File	Ukuran File *Decryption (byte)*	Waktu *Decryption (Milisecond)*
1	538624	SOAL TRY OUT B.ING KLS 9 2023.pdf	538624	910
2	411648	SOAL PTS GENAP B.ING KLS 8 SMT 2 THN 2021	411648	710
3	13312	NIL_SAS_20222_300210000_ 7.A	13312	20
4	15360	NIL_SUMATIF_20222_300210000_ 7.A	15360	20
5	13312	NIL_SAS_20222_300210000_ 7.B	13312	20
6	15360	NIL_SUMATIF_20222_300210000_ 7.B	15360	20
7	13312	NIL_SAS_20222_300210000_ 7.C	13312	20
8	15360	NIL_SUMATIF_20222_300210000_ 7.C	15360	20

4. KESIMPULAN

Setelah melalui tahap penelitian, perancangan, dan pengujian aplikasi enkripsi dan dekripsi file menggunakan algoritma RC4, diperoleh beberapa kesimpulan penting. Pertama, algoritma RC4 terbukti berperan penting dalam melaksanakan fungsi enkripsi dan dekripsi, dimaksudkan untuk memberikan perlindungan yang kokoh terhadap berkas-berkas ujian. Proses enkripsi melibatkan pengacakan isi berkas ujian dengan menggunakan kunci yang diinputkan pada saat enkripsi dilakukan. Selanjutnya, dalam tahap dekripsi, berkas ujian dapat dikembalikan ke bentuk aslinya dengan memasukkan kunci yang sama seperti yang digunakan pada proses enkripsi.

Mengacu pada hasil kesimpulan di atas, maka terdapat beberapa saran yang dapat diusulkan guna mengembangkan sistem ini menjadi lebih relevan. Pertama, perlu dilakukan pengembangan dengan mengadopsi algoritma terbaru dan lebih unggul agar proses enkripsi dan dekripsi menjadi lebih aman dan efisien. Selanjutnya, potensi pengembangan sistem ini dapat meluas hingga mencakup enkripsi dan dekripsi berbagai format file seperti video, audio (mp3), dan lainnya. Poin penting lainnya adalah menambahkan fitur-fitur yang dapat memenuhi kebutuhan masa depan, mengantisipasi perubahan dan tuntutan yang akan muncul seiring berjalannya waktu.

DAFTAR PUSTAKA

[1] Yusfrizal, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, pp. 29–37, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/index

[2] Y. S. Japriadi and D. Novianto, "PENERAPAN RC5 UNTUK PENGAMANAN NILAI MATAKULIAH MAHASISWA PADA KAMPUS XYZ," *Jurnal Algoritma, Logika dan Komputasi*, vol. 2, no. 2, pp. 190–194, Nov. 2019, [Online]. Available: https://journal.ubm.ac.id/index.php/alu

[3] D. Adhar, "IMPLEMENTASI ALGORITMA DES (DATA ENCRYPTION STANDARD) PADA ENKRIPSI DAN DESKRIPSI SMS BERBASIS ANDROID," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, pp. 53–60, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/index

[4] Fatonah, D. I. Mulyana, A. P. Heryani, and V. Khoirunnisa, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *Jurnal Informatika dan Teknik Komputer (JICOM)*, vol. 3, no. 1, pp. 32–39, 2022, [Online]. Available: https://ejurnalunsam.id/index.php/jicom/

[5] I. N. Purnama, "IMPLEMENTASI ALGORITMA ENKRIPSI RC5 UNTUK MENGAMANKAN GAMBAR PADA PERANGKAT ANDROID," *JIRE (Jurnal Informatika & Rekayasa Elektronika)*, vol. 2, no. 2, pp. 1–9, 2019, [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jire

[6] M. D. Hariyanto and D. V. S. Y. Sakti, "PENERAPAN ALGORITMA RC4 UNTUK PENGAMANAN FILE BERBASIS WEB PADA CV. MERPATI GRAPHIC INDONESIA," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, vol. 1, no. 1, pp. 193–201, 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index

[7] F. Casio and D. Kusumaningsih, "PENGAMANAN DATA PASIEN MENGGUNAKAN METODE RC-4 BERBASIS WEB PADA RSIA PKU MUHAMMADIYAH CIPONDOH," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, vol. 1, no. 1, pp. 68–74, 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index

[8] I. D. Mahendra, Mufti, and P. F. Ariyani, "APLIKASI PENGAMANAN FILE MENGGUNAKAN ALGORITMA RIVEST CODE 4 (RC4) BERBASIS WEB PADA KOPI TYADATARA," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, vol. 2, no. 1, pp. 134–140, 2023, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index

[9] R. Maulana and R. M. Simanjorang, "Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 4, no. 6, pp. 377–383, 2021, [Online]. Available: https://ojs.serambimekkah.ac.id/index.php/jnkti/about/editorialPolicies#:~:text=Jurnal%20Nasional%20Komputasi%20dan%20Teknologi%20Informasi%20%28JNKTI%29%20merupakan,Bulan%20Februari%2C%20April%2C%20Juni%2C%20Agustus%2C%20Oktober%20dan%20Desember.

[10] M. R. Adnan and T. Fatimah, "PENGAMANAN DATA LAPORAN KEUANGAN MENGGUNAKAN METODE RC4 PADA REDDOG CABANG GADING SERPONG," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, vol. 1, no. 1, pp. 230–239, 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index