



UNIVERSITAS  
BUDI LUHUR



**SENAFTI**  
SEMINAR NASIONAL MAHASISWA  
FAKULTAS TEKNOLOGI INFORMASI  
VOL. 1 NO. 1 SEPTEMBER 2022  
E-ISSN: 2962-8628

# PROSIDING

SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI (SENAFTI)

PERANAN ARTIFICIAL INTELLIGENCE  
YANG CERDAS BERBUDI LUHUR  
DALAM MENGHADAPI ERA SOCIETY 5.0

# CYBER SECURITY



Supported by :

Ngampooz 

## **STEERING COMMITTEE**

### **Pelindung**

Dr. Ir. Wendi Usino, M.Sc., M.M

### **Penanggung Jawab**

Dr. Ir. Deni Mahdiana, S.Kom, M.M., M.Kom

### **Ketua Pelaksana**

Dr. Rusdah, M.Kom

### **Sekretaris**

Retno Wulandari, S.Kom., M.Kom.

### **Bendahara**

Noni Juliasari, S.Kom., M.Kom.

### **Acara**

Ratna Ujian Dari, S.Kom., M.M., M.Kom.

### **Pengelola Makalah dan Mitra Bestari**

1. Atik Ariesta, S.Kom., M.Kom.
2. Samsinar, S.Kom., M.Kom.

### **Pengelola Editor dan Jurnal**

1. Indah Puspasari Handayani, S.Kom., M.Kom.
2. Devit Setiono, S.Kom., M.Kom.
3. Anwar Rifa'i, S.Pd, M.Pd.
4. Reva Ragam Santika, S.Kom., M.Kom.
5. Kukuh Harsanto, S.Kom., M.Kom

### **Pengelola Teknologi Informasi**

1. Sovan Dianarto, S.Kom.
2. Dolly Virgian Shaka Yudha Shakti, S.Kom., M.Kom.

### **Pengelola Undangan dan Desain**

Wasiran

## **REDAKSI**

- Pelindung : Dr. Ir. Wendi Usino, M.Sc., M.M  
Penanggung Jawab : Dr. Ir. Deni Mahdiana, S.Kom, M.M., M.Kom  
Ketua Redaksi : Dr. Rusdah, M.Kom  
Wakil Ketua Redaksi :  
1. Atik Ariesta, M.Kom  
2. Samsinar, S.Kom, M.Kom
- Redaksi Pelaksana :  
1. Indah Puspasari Handayani, M.Kom  
2. Devit Setiono, M.Kom  
3. Anwar Rifa'I, S.Pd., M.Pd  
4. Reva Ragam Santika, M.Kom  
5. Kukuh Harsanto, S.Kom., M.Kom

## MITRA BESTARI

1. Dr. Ir. Achmad Solichin, S.Kom., M.T.I (Universitas Budi Luhur)
2. Anita Ratnasari, S.Kom, M.Kom (Universitas Mercu Buana)
3. Prof. Dr. Anton Satria Prabuwono, ST., SSi., M.M (Universitas Budi Luhur)
4. Dr. Ir. Arief Wibowo, S.Kom., M.Kom (Universitas Budi Luhur)
5. Arif Bramantoro, Ph.D (Universitas Budi Luhur)
6. Bima Cahya Putra, S.Kom., M.Kom. (Universitas Budi Luhur)
7. Prof. Ir. Dana Indra Sensuse, Ph.D (Universitas Indonesia)
8. Denni Kurniawan, S.T., M.T.I., Ph.D (Universitas Budi Luhur)
9. Dian Anubhakti, S.Kom., M.Kom. (Universitas Budi Luhur)
10. Dolly Virgian Shaka Yudha Sakti, S.Kom., M.Kom. (Universitas Budi Luhur)
11. Dwi Pebrianti, S.T., M.Eng., Ph.D (Universiti Budi Luhur)
12. Dr. Emy Setyaningsih, S.Si., M.Kom (Institut Sains dan Teknologi AKPRIND Yogyakarta)
13. Dr. Gandung Triyono, M.Kom (Universitas Budi Luhur)
14. Dr. Ir. Goenawan Brotosaputro, S.Kom., M.Sc (Universitas Budi Luhur)
15. Grace Gata, S.Kom., M.Kom. (Universitas Budi Luhur)
16. Dr. Ir. Hari Soetanto, S.Kom., M.Sc (Universitas Budi Luhur)
17. Hendra Cipta, M.Si (Universitas Islam Negeri Sumatera Utara Medan)
18. Hendri Irawan, S.Kom., M.T.I. (Universitas Budi Luhur)
19. Dr. Imelda, M.Kom (Universitas Budi Luhur)
20. Indra Nugraha Abdullah, Ph.D (Universitas Budi Luhur)
21. Dr. Indra, S.Kom., M.T.I (Universitas Budi Luhur)
22. Ita Novita, S.Kom., M.T.I. (Universitas Budi Luhur)
23. Dr. Ir. Iwan Setiawan, MT, MCSA, CRM. (Universitas Nusa Putra)
24. Dr. Ir. Jan Everhard Riwurohi, M.T (Universitas Budi Luhur)
25. Kelik Sussolaikah, S.Kom., M.Kom (Universitas PGRI Madiun)
26. Dr. Krisna Adiyarta M, S.Kom., M.Sc (Universitas Budi Luhur)
27. Luhur Bayuaji, S.T., M.Eng., Ph.D (Universiti Malaysia Pahang)
28. Dr. Ir. Mardi Hardjianto, M.Kom (Universitas Budi Luhur)
29. Mayanda Mega Santoni, S.Komp., M.Kom. (Universitas Pembangunan Nasional Veteran Jakarta)
30. Prof. Dr. Moedjiono, M.Sc (Universitas Budi Luhur)
31. Dr. Mohammad Syafrullah, M.Kom., M.Sc (Universitas Budi Luhur)
32. Dr. Ir. Nazori A. Z., M.T (Universitas Budi Luhur)
33. Noni Juliasari, S.Kom., M.Kom. (Universitas Budi Luhur)
34. Rizky Pradana, S.Kom., M.Kom. (Universitas Budi Luhur)
35. Rohmat Indra Borman, M.Kom. (Universitas Teknokrat Indonesia)
36. Safitri Juanita, S.Kom., M.T.I. (Universitas Budi Luhur)
37. Dr. Samidi, S.Kom., M.M., M.Kom (Universitas Budi Luhur)
38. Setyawan Widyarto, M.Sc., Ph.D (Universiti Selangor, Malaysia)
39. Dr. Sofian Lusa, S.E., M.Kom (Universitas Budi Luhur)
40. Dr. Tenia Wahyuningrum, S.Kom., M.T (Institut Teknologi Telkom Purwokerto)
41. Titin Fatimah, S.Kom., M.Kom. (Universitas Budi Luhur)
42. Dr. Ir. Utomo Budiyanto, M.Kom., M.Sc (Universitas Budi Luhur)
43. Windarto, S.Kom., M.Kom. (Universitas Budi Luhur)
44. Dr. Yan Rianto, M.Eng (Badan Riset dan Inovasi Nasional/BRIN)

## KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT dan hanya karena rahmat dan karunia-Nya, Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 2022 telah terselesaikan dengan baik. Prosiding seminar ini merupakan kumpulan makalah hasil penelitian para akademisi dan peneliti yang sebelumnya telah dipresentasikan pada SENAFIT tahun 2022 yang dilaksanakan secara daring (online) pada tanggal 6 September 2022. Tema SENAFIT Tahun 2022 adalah “Peranan Artificial Intelligence yang Cerdas Berbudi Luhur Dalam Menghadapi Era Society 5.0”

Penyusunan prosiding ini dimaksudkan untuk penyebarluasan hasil-hasil penelitian dan kajian dalam bidang teknologi informasi. Selain itu, penyusunan prosiding ini juga dimaksudkan agar masyarakat luas dapat mengetahui berbagai informasi terkait dengan penyelenggaraan SENAFIT. Penyusunan prosiding ini dibagi menjadi 4 (empat) buku yaitu:

1. Buku 1 - Cyber Security
2. Buku 2 – Artificial Intelligence
3. Buku 3 – Programming
4. Buku 4 – Information System

Pada kesempatan ini kami menyampaikan terima kasih yang sebesar-besarnya kepada para akademisi dan peneliti atas hasil karya dan sumbangan pemikiran yang dipresentasikan dalam bentuk makalah dan presentasi ilmiah. Juga kami sampaikan terima kasih kepada para mitra bestari yang telah mereview semua makalah sehingga kualitas isi dari makalah dapat terjaga dan dipertanggungjawabkan. Tak lupa kepada semua pihak yang telah memberikan dukungan bagi terselenggaranya SENAFIT dan atas tersusunnya prosiding ini. Harapan kita bersama, semoga prosiding ini dapat menambah khasanah pengembangan ilmu pengetahuan dan teknologi informasi di Indonesia.

Jakarta, September 2022

Tim Penyusun

## DAFTAR ISI

<b>Penerapan Aplikasi Kriptografi Dengan Algoritma Advanced Encryption Standard Pada Perusahaan PT Cahaya Televisi Indonesia</b>	
Hogan Prilandi, Dewi Kusumaningsih.....	1-9
<b>Pengamanan Database Sistem Pendaftaran Online Dengan Kriptografi AES-256-CCBC Pada TK Islam Baitul Khoir</b>	
Rizky Putra Mahendra, Hari Soetanto.....	10-19
<b>Penerapan Rivest Code 4 Pada Aplikasi Pengamanan File Berbasis Web Pada PT. Artindo Prima GrahaGuntur</b>	
Kevin Helbert Wattimena, Safrina Amini.....	20-28
<b>Penerapan Kriptografi Menggunakan Advanced Encryption Standard 128 Untuk Pengamanan File Pada SMK Muhammadiyah 4</b>	
Romi Ramadhan, Hari Soetanto .....	29-38
<b>Pengamanan Data Keuangan Menggunakan Algoritma Advanced Encryption Standard 128 Pada PT. Charise Deo Indonesia</b>	
Aif Ramadan, Painem Painem .....	49-57
<b>Penerapan Kriptografi Caesar Cipher Dan BASE64 Untuk Mengamankan Database Distributor Barang Pada PT. Sekawan</b>	
Kholik Nurzaman, Sri Mulyati.....	39-48
<b>Implementasi Algoritma Skipjack dan Rivest Shamir Adleman Pada File Dokumen Data Pegawai Shopee Express Hub Ciledug</b>	
Isnandar Kurniadi, Rizky Pradana .....	58-67
<b>Pengamanan Data Pasien Menggunakan Metode Rc-4 Berbasis Web Pada RSIA PKU Muhammadiyah Cipondoh</b>	
Fefi Casio, Dewi Kusumaningsih.....	68-75
<b>Penerapan Algoritma Rivest Code 4 (RC4) Untuk Keamanan File Pada SMPN 149 Jakarta</b>	
Fachrul Fatahillah, Hari Soetanto.....	76-83
<b>Klasifikasi Data Mining Untuk Memprediksi Status Penerimaan Di Perguruan Tinggi Negeri Bagi Lulusan Bimbel NF Dengan Algoritme Naive Bayes</b>	
Syafiq Abdurrohman, Arief Wibowo .....	84-92
<b>Implementasi Algoritma AES-128 Untuk Pengamanan Database Pada SMA Islamic Centre</b>	
Reyhan Davon Ardiya, Wahyu Pramusinto.....	93-102
<b>Optimasi Akses Internet Pengunjung Bubble Panjul Dengan Penerapan Voucher Berbasis Mikhmon dan Mikrotik</b>	
Sasi Kirana, Joko Christian Chandra.....	103-110
<b>Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security</b>	
Raudatul Firdaus, Reva Ragam Santika .....	111-120

<b>Implementasi Advanced Encryption Standard 128 Bit dan Shamir Secret Sharing Pada Website Data Ulang Pensiun Lembaga Dana Pensiun Pertamina</b>	
Ihvan Mulya Pradana, Rizky Pradana.....	121-129
<b>Implementasi Kriptografi File Ujian Siswa Dengan Metode Rsa Berbasis Website Di SMAN 84 Jakarta</b>	
I Gusti Ayu Yogie Andhika Putri, Noni Juliasari .....	130-139
<b>Penerapan Advanced Encryption Standard 128 Dan Rivest Code 4 Pada SMK Bakti Idhata</b>	
Alif Lathiif, Alexander Jp Sibarani.....	140-148
<b>Implementasi Kriptografi Dengan Menggunakan Metode RC4 Dan AES-256 Untuk Mengamankan File Dokumen Pada PT Varnion Technology Semesta</b>	
Arya Kusuma, Reva Ragam Santika .....	149-158
<b>Penerapan Advanced Encryption Standard-128 Dan Rivest Code4 Untuk Pengamanan Data Pada CV. Trista Jaya Abadi</b>	
Kamal Saputra, Alexander Sibarani .....	159-167
<b>Implementasi Pengamanan File Menggunakan Rivest Code 4 (RC4) Pada SMK Yadika 4 Tangerang</b>	
Junior Ceesar, Dolly Virgian Shaka Yudha Sakti .....	168-174
<b>Implementasi Algoritma Kriptografi Rivest Code 4 (RC4) Berbasis Web Pada PT. Putri Maharani Medikal</b>	
Daffa Arya, Dolly Virgian Shaka Yudha Sakti.....	175-181
<b>Penerapan Algoritme Rivest Code 4 Untuk Pengamanan Dokumen Di CV. Bintang Pratama Mandiri</b>	
Fauzan Ali Nurbi, Utomo Budiyanto .....	182-192
<b>Penerapan Algoritma RC4 Untuk Pengamanan File Berbasis Web Pada CV. Merpati Graphic Indonesia</b>	
Muhammad Daffa Hariyanto, Dolly Virgian Shaka Yudha Sakti .....	193-201
<b>Implementasi Algoritma Rivest Code 4 Untuk Pengamanan Dokumen Di Klinik First Health</b>	
Rahken Kapissa, Safrina Amini .....	202-212
<b>Prototipe Sistem Kendali Smart Home Dengan Menggunakan Mikrokontroler ESP8266 NODEMCU V3 CH340 Berbasis Web</b>	
Muhammad Alfian, Purwanto Purwanto .....	213-219
<b>Penerapan Algoritma AES128 Dan RC4 Untuk Pengamanan Database Dan File Pada PT. Mayaksa Mugi Mulia</b>	
Mila Rismaya, Dolly Virgian Shaka Yudha Sakti.....	220-229
<b>Pengamanan Data Laporan Keuangan Menggunakan Metode RC4 Pada Reddog Cabang Gading Serpong</b>	
Muhamad Rifki Adnan; Titin Fatimah .....	230-239
<b>Pengamanan File Ujian Menggunakan Algoritma Advanced Encryption Standard 128 Di SMP Negeri 22</b>	
Bonita Cerlia Ashari, Sejati Waluyo .....	240-247
<b>Pengamanan Database Perpustakaan Dengan Algoritma AES-128 Pada SMA Waskito</b>	
Muhammad Thoriq Ardian, Wahyu Pramusinto .....	248-257

<b>Implementasi Algoritma Elliptic Curve Cryptography (ECC) Untuk Pengamanan File Berbasis Web</b> Yoga Nugroho, Painem Painem.....	258-267
<b>Pengamanan File Rekam Medis Pada Puskesmas Larangan Utara Menggunakan Algoritma Kriptografi RSA Berbasis Web</b> Reychan Davia Al Hiday, Sejati Waluyo.....	277-286
<b>Aplikasi Pengamanan Surat Dengan Metode RC4 Berbasis Web Di Kelurahan Pakujaya Tangerang Selatan</b> Safwah Setiono Puteri, Sejati Waluyo.....	287-294
<b>Algoritme AES-256 Untuk Keamanan Basis Data Penilaian Pegawai Pada PT. Buana Jaya Korindo</b> Anggi Dwi Saputra, Mohammad Syafrullah .....	295-301
<b>Penerapan Algoritme Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung</b> Irfan Kumia Nurhareza, Siswanto Siswanto .....	302-309
<b>Implementasi Algoritma Rivest Code 4 (RC4) Untuk Pengamanan Dokumen Berbasis Web Pada PT. Tri Tunggal Multikreasi</b> Gilang Rassia Raudha, Safrina Amini.....	310-318
<b>Aplikasi Pengamanan Dokumen Menggunakan Metode Rivest Code 4 (RC4) Berbasis Web Pada Yayasan Berkembang Mandiri Indonesia</b> Muhammad Farhansyah, Utomo Budiyanto .....	319-326
<b>Aplikasi Pengamanan Dokumen Menggunakan Metode Rivest Code 4 (RC4) Berbasis Web Pada Yayasan Berkembang Mandiri Indonesia</b> Muhammad Farhansyah, Utomo Budiyanto .....	319-326
<b>Penerapan Algoritma AES-128 Untuk Pengamanan File Pada SMK PGRI 31 Legok</b> Kaliyana Tantri Rukmana, Pipin Farida Ariyani.....	327-336
<b>Implementasi Kriptografi Menggunakan Metode Advance Encryption Standart (AES 128) Pada Aplikasi Inisiasi Project Berbasis Web Di PT Pins Indonesia</b> Sandy Andreas, Purwanto Purwanto.....	337-343
<b>Implementasi Kriptografi Menggunakan Metode Rivest Shamir Adleman (RSA) Pada Perancangan Aplikasi Enkripsi &amp; Dekripsi Berbasis Java Desktop Pada Madrasah Tsanawiyah Daarul Falah</b> Muhammad Sugiarto, Purwanto Purwanto .....	344-350
<b>Implementasi Kriptografi Menggunakan Metode Algoritma RSA Pada Aplikasi Pengamanan Data Berbasis Java Desktop Untuk UD Tirta Soeper Teloer</b> Muhammad Zainal, Krisna Adiyarta M.....	351-359
<b>Implementasi Algoritma AES Dan RC4 Untuk Mengamankan File Data Customer Instalasi Baru</b> Andi Kumiawan, Rizky Pradana .....	360-367
<b>Implementasi Keamanan Database Menggunakan Kriptografi RC4 Pada Sistem Milik PT. Torop Sumber Makmur</b>	

Dadan Romadhan, Ferdiansyah Ferdiansyah.....	368-376
<b>Implementasi Algoritma RC4 Untuk Keamanan File Berbasis Web Pada SDIT Ar Rahman</b> Rahmat Awaludin Umar, Hari Soetanto.....	377-385
<b>Implementasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritme ElGamal Pada Dokumen Di Balai Pendidikan dan Pelatihan Penerbangan BP3 Curug Berbasis Web</b> Vicky Hemando Zulian, Purwanto Purwanto.....	386-393
<b>Pengamanan File Pendaftaran Siswa Baru Menggunakan Metode Algoritme RC4 Di TK Nurul Irfan</b> Muhammad Apriyanda Sutejo, Mardi Hardjianto.....	394-401
<b>Penerapan Kriptografi Caesar Cipher dan Vigenere Cipher Untuk Mengamankan Database Barang Belting Pada PT. Multi Mitra Usaha Bersama</b> Muhammad Rizki Zulfikar, Sri Mulyati.....	402-410
<b>Penerapan Algoritma AES-128 Untuk Aplikasi Pengarsipan Dokumen Berbasis Web Pada PT Studio Inovasi Teknologi</b> Re Riski Dwi Andika, Sri Mulyati.....	411-420

## IMPLEMENTASI ALGORITMA RC4 UNTUK KEAMANAN FILE BERBASIS WEB PADA SDIT AR RAHMAN

Rahmat Awaludin Umar<sup>1\*</sup>, Hari Soetanto<sup>2</sup>

<sup>1,2</sup>Fakultas Teknologi Informasi, Teknik Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: <sup>1</sup>Rahmatawal3@gmail.com , <sup>2</sup>hari.soetanto@budiluhur.ac.id

(\* : corresponding author)

**Abstrak**-Di setiap tahunnya, SDIT Ar-Rahman ini memiliki banyak sekali dokumen baik itu dokumen rekapan rapor, rekapan ujian, rekapan absen guru, dan lain lain yang bersifat penting. Diperlukan sebuah aplikasi untuk mengamankan dokumen tersebut. Sangat disayangkan jika dokumen dokumen tersebut jatuh ditangan yang salah dan disalah gunakan. Maka dari itu, untuk mencegah file dokumen tersebut menyebar dengan luas secara massal diperlukannya sebuah aplikasi dengan keamanan dan kerahasiaan yang dapat menjaga file dokumen tersebut. Dan aplikasi ini dapat dilakukan dengan salah satu kriptografi algoritma Rivest Code 4(RC4). Metode penelitian menggunakan model waterfall. Penerapan metode model waterfall ini terdiri dari beberapa tahapan, yaitu komunikasi, perencanaan, pemodelan, konstruksi, dan deployment. Ada beberapa rancangan hasil data yang dihasilkan dari penelitian ini, yaitu terdapat class diagram , logical record struktur (LRS), dan spesifikasi basis data yang menggunakan MySQL. Pembuatan aplikasi website ini menggunakan bahasa pemrograman, PHP, HTML5, dan untuk database menggunakan MySQL. Hasil dari pembuatan aplikasi yang menggunakan kriptografi algoritma Rivest Code 4(RC4) ini, yaitu sebuah website yang dapat mengamankan file dokumen berekstensi \*.docx, \*.pdf, \*.xls, \*.xlsx, \*.txt dengan menggunakan metode model waterfall. Pengujian ini dapat dilakukan dengan cara menggunakan uji blackbox untuk pengujian enkripsi dan dekripsi. Hasil dari pengujian menunjukkan sistem dapat berjalan dengan baik dan berhasil mengimplementasikan algoritma RC4.

**Kata Kunci:** Dokumen, Rivest Code 4 (RC4), Waterfall, Website, Kriptografi, Bahasa Pemrograman.

### IMPLEMENTATION OF THE RC4 ALGORITHM FOR WEB-BASED FILE SECURITY IN SDIT AR RAHMAN

**Abstract**-Every year, SDIT Ar-Rahman has a lot of documents, whether it's a report card summary, exam recap, teacher absence recap, and others that are important. An application is required to secure the document. It is unfortunate if these documents fall into the wrong hands and are misused. Therefore, to prevent these document files from spreading widely in bulk, an application with security and confidentiality is needed that can maintain the document files. And this application can be done with one of the cryptographic algorithms Rivest Code 4(RC4). The research method uses the waterfall model. The application of the waterfall model method consists of several stages, namely communication, planning, modeling, construction, and deployment. There are several designs of data results generated from this research, namely there are class diagrams, logical record structures (LRS), and database specifications that use MySQL. Making this website application using the programming language, PHP, HTML5, and for the database using MySQL. The result of making an application that uses Rivest Code 4(RC4) cryptography algorithm is a website that can secure document files with the extension \*.docx, \*.pdf, \*.xls, \*.xlsx, \*.txt using the waterfall model method. This test can be done by using the blackbox test for encryption and decryption testing. The results of the test show that the system can run well and successfully implement the RC4 algorithm.

**Keywords:** Document, Rivest Code 4 (RC4), Waterfall, Website, Cryptography, Programming Language.

## 1. PENDAHULUAN

Sekolah Dasar Islam Terpadu (SDIT) Ar-Rahman Bojonggede berada dibawah Yayasan Lembaga Pendidikan Pondok Pesantren (LP3) Ar-Rahman, yang dibentuk pada tahun 2009. Yayasan ini bergerak di bidang sosial yang diawali dengan mendirikan sekolah bernama SMAIT Ar-Rahman dan disusul dengan pendirian SMPIT Ar-Rahman, yang keduanya berlokasi di Kecamatan Bojonggrenteng Parungkuda Kabupaten Sukabumi.

Di setiap tahunnya, SDIT Ar-Rahman ini memiliki banyak sekali data dokumen. Data dokumen yang sekolah terima bisa berupa PPDB, dokumen rekapan rapor, rekapan ujian, rekapan absen guru, dan lain lain yang bersifat penting. Sangat disayangkan jika dokumen dokumen tersebut jatuh ditangan yang salah dan disalahgunakan. Oleh karena itu saya membuat sebuah website ini untuk mengamankan dokumen file.

Untuk menjaga keamanan data dan menghindari kebocoran data dapat dilakukan berbagai cara salah satunya yaitu dengan menggunakan kriptografi. Menurut pada ahli yang sudah mengambil sebuah kesimpulan tentang

kriptografi. Kriptografi merupakan ilmu yang menggunakan teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, authentication entity, dan authentication asal data. Dalam ilmu kriptografi terdapat berbagai macam algoritme salah satunya yaitu RC4.

## 2. METODE PENELITIAN

### 2.1 Kriptografi

Kriptografi awalnya digambarkan sebagai studi tentang bagaimana menyembunyikan pesan. Namun, dalam pengertian kriptografi saat ini, kriptografi adalah ilmu yang didasarkan pada teknik matematika untuk menangani keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi entitas. Jadi pengertian kriptografi saat ini, berarti tidak hanya berurusan dengan penyembunyian pesan tetapi lebih dari seperangkat teknik yang memberikan keamanan informasi. Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu *kryptos* berarti rahasia (*secret*) dan *graphein* artinya menulis (*writing*), jadi kriptografi artinya *secret writing* (tulisan rahasia). Dan ada beberapa definisi kriptografi yang telah dikemukakan oleh beberapa literatur, antara lain: Menurut Scheneier Bruce, Kriptografi berarti ilmu dan seni menjaga keamanan pesan (Kriptografi adalah seni dan ilmu menjaga keamanan pesan). Kata seni dalam definisi tersebut berasal dari informasi sejarah bahwa pada masa awal sejarah kriptografi, setiap orang mungkin memiliki cara unik untuk merahasiakan pesan. Cara-cara unik tersebut dapat berbeda untuk setiap pelaku kriptografi sehingga setiap cara penulisan pesan rahasia, pesan tersebut memiliki nilai keindahan tersendiri sehingga kriptografi berkembang sebagai seni menjaga kerahasiaan pesan.

### 2.2 Rivest Code 4 (RC4)

RC4 adalah jenis aliran kode yang berarti operasi enkripsi dilakukan per karakter 1 byte untuk satu operasi. Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris yang dirancang oleh RSADSI (RSA Data Security Inc) dalam bentuk *stream cipher*. RC4 menggunakan panjang kunci dari 1 hingga 256 byte yang digunakan untuk menginisialisasi tabel 256 byte.[4]

Algoritma RC4 menggunakan dua *Substitusi Box* (*S-Box*), yaitu array dengan panjang 256 yang berisi dari 0 sampai 255, dan *S-Box* kedua, berisi permutasi yang dimana memiliki fungsi dari kunci dengan panjang variabel. Cara kerja algoritma RC4 adalah dengan menginisialisasi *S-Box* pertama,  $S[0], S[1], \dots, S[255]$ , dengan angka 0 sampai 255. Langkah pertama berurutan  $S[0] = 0, S[1] = 1, \dots, S[255] = 255$ . Kemudian inisialisasi larik lain (*S-Box* lain), misal larik *K* dengan panjang 56. Isi larik *K* dengan kunci berulang-ulang sampai semua larik  $K[0], K[1], \dots, K[255]$  terisi penuh. Proses inisialisasi *S-Box* (Array *S*) dapat dilihat pada tabel 1 di bawah ini:

a. Proses Inisialisasi *S-Box*(Array *S*)

```
For i = 0 ; i < 256 ; i++;
```

```
S[i] = i
```

Proses inisialisasi *S-Box* (Array *K*) dapat dilihat pada tabel 2 berikut:

b. Proses Inisialisasi *S-Box*(Array *K*) array Kunci//Array dengan panjang kunci "length".

```
j = 0
```

```
for i = 0 ; I < 256 ; i++;
```

```
  j = (j + S[i] + (this -> key[i % strlen (this -> key)])) mod 256
```

```
  x = S[i]
```

```
  S[i] = S[j]
```

```
  S[j] = x
```

Kemudian pada lakukan pengacakan *S-Box* yang dapat dilihat pada tabel 3 sebagai berikut:

c. Proses Pengacakan *S-Box*

```
i = 0; j = 0; res = 0;
```

```
for y = 0; y < strlen (this -> str) ; y++;
```

Setelah itu, buat *pseudo random byte* pada tabel 4 dengan langkah sebagai berikut:

4. *Pseudo Random Byte*

```
I = (i + 1) mod 256;
```

```
J = (j + S[i]) mod 256;
```

```
x = S[i];
```

```
S[i] = S[j];
```

```
S[j] = x;
```

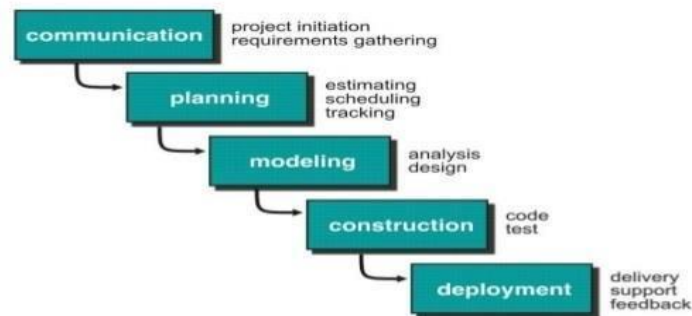
```
res = this ->str[y] ^ chr(S[(S[i] + S[j]) mod 256]);
```

### 2.3 Penerapan Metode

Desain atau metode penelitian yang digunakan pada penelitian ini adalah model waterfall. Model waterfall adalah model klasik yang bersifat sistematis, berurutan dalam membangun software [5]. Dalam penerapan metode ini menjelaskan bahwa dalam membangun sistem ini terdiri dari beberapa tahapan yaitu komunikasi, perencanaan, pemodelan, konstruksi, dan *deployment*.

#### a. Komunikasi

Pada Langkah pertama ini untuk membangun sebuah sistem adalah menganalisis dan mengkomunikasikan kebutuhan dalam sistem berdasarkan hasil dari pengumpulan data. Pada tahap komunikasi dapat disimpulkan bahwa diperlukan suatu sistem untuk pengamanan dokumen file di SDIT Ar Rahman.



**Gambar 1.** Penerapan Metode Waterfall

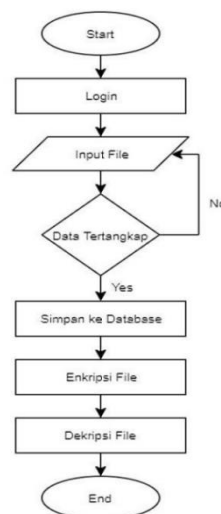
#### b. Perencanaan

Lalu pada tahap perencanaan ini menggambarkan sebuah tugas tugas teknik yang harus dilakukan oleh si pembuat program. Dimulai dari pengumpulan data hingga pengujian sistem, resiko yang mungkin terjadi pada saat melaksanakan tugas tersebut, dan hasil yang akan diperoleh untuk terciptanya sistem keamanan dokumen file yang berada di sekolah dengan menggunakan algoritma RC4

#### c. Pemodelan

Pada tahap pemodelan ini berfungsi untuk merancang sebuah skema sistem keamanan dokumen digital kemudian perancangan database dengan menggunakan MySQL sebagai sistem penyimpanan data. Selanjutnya adalah sebuah perancangan antarmuka sebuah sistem keamanan file dokumen. *System Flowchart* dapat dilihat pada Gambar 2.

Flowchart Sistem Pengamanan Data Digital



**Gambar 2.** Flowchart Sistem Pemodelan

Sistem dimulai dengan login. Dimana para pengguna (staff guru) dan admin, dapat memasukkan nama pengguna (*username*) dan kata sandi (*password*). Kemudian user dapat menginput file tersebut kedalam sistem, yang kemudian sistem akan menangkap file tersebut dan menyimpan kedalam *database*. Selanjutnya, file tersebut dapat di enkripsi dan di dekripsi lagi jika diperlukan oleh *user*.

d. Konstruksi

Pada tahap konstruksi ini, merupakan sebuah tahapan pembuatan kode, sehingga terciptanya suatu *system* yang telah dirancang sebelumnya. Pada pembuatan program ini, si pembuat menggunakan sebuah bahasa pemrograman HTML, PHP, dan untuk *database* menggunakan MySQL dalam membangun sistem tersebut.

Setelah proses coding selesai maka akan dilakukan pengujian pada sistem yang telah dibuat. Pengujian sistem tersebut dilakukan dengan menggunakan *blackbox*. Pengujian *blackbox* ini dilakukan untuk mengetahui apakah fungsi fungsi pada program dapat berjalan dengan baik, mulai dari login, input, proses, dan outputnya.

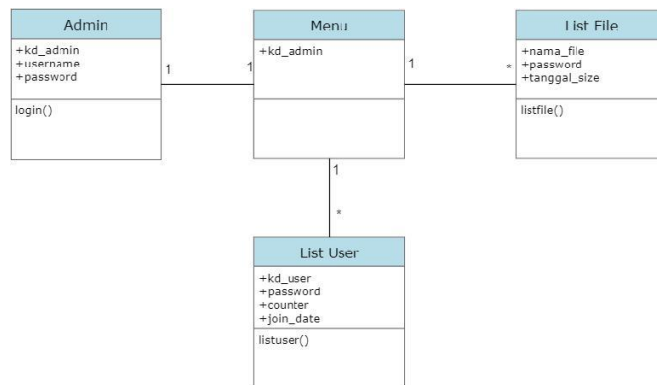
e. Deployment

Pada tahap terakhir ini, yaitu tahap *deployment*. Tahap *deployment* adalah sebuah tahap dimana sistem siap digunakan oleh *user*. Kemudian untuk menjaga agar sistem tetap berjalan dengan baik maka perlu dilakukan perawatan berkala sesuai dengan kebutuhan.

## 2.4 Rancangan Basis Data

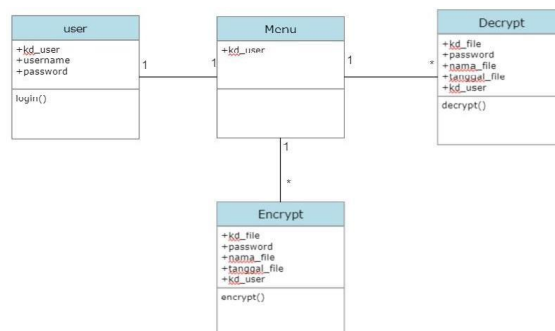
a. Class Diagram

Pada gambar 3 dibawah ini merupakan gambaran class diagram admin.



Gambar 3. Class Diagram Admin

Pada gambar 3 terdapat field admin yang berisikan, yaitu *kd\_admin* , *username*, *password*. Lalu ada *field* Menu yang berisikan, *kd\_admin*. Lalu terdapat *list file* dan *list user* yang berisi hampir sama diantaranya jika *list file* mempunyai , *nama\_file*, *password*, *tanggal\_file*. Maka *list user* itu ada *kd\_user*, *password*, *counter*, *join\_date*. Lalu setelah ditampilkannya *Class Diagram Admin*, maka kali ini akan menampilkan *Class Diagram User*.

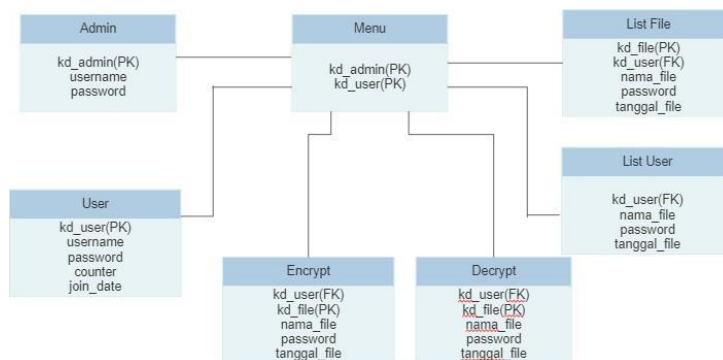


Gambar 4. Class Diagram User

Pada gambar 4 terdapat *field user* yang berisikan, yaitu *kd\_user*, *username*, *password*. Lalu ada *field Menu* yang berisikan, *kd\_user*. Lalu terdapat *Encrypt* dan *Decrypt* yang berisi hampir sama, yaitu *kd\_file*, *password*, *nama\_file*, *tanggal\_file*, dan *kd\_user*.

b. *Logical Record Structur (LRS)*

Pada gambar 5 dibawah ini merupakan gambaran LRS program ini.



**Gambar 5.** *Struktur Logical Record Structur (LRS)*

Pada gambar diatas tabel Admin yang berisi *kd\_admin* sebagai primary key, *username*, dan *password*. Tabel User yang berisi *kd\_user* sebagai primary key, *username*, dan *password*. Tabel Menu yang mempunyai *kd\_admin* sebagai primary key, dan *kd\_user* sebagai primary key. Tabel List File mempunyai *kd\_file* sebagai primary key, *nama\_file*, *password*, *tanggal\_file*, dan *kd\_user* sebagai foreign key. Tabel List User mempunyai *kd\_user* sebagai primary key, *username*, *password*, *counter*, dan *join\_date*. Tabel Encrypt dan Decrypt mempunyai isi yang sama, yaitu *kd\_user* sebagai foreign key, *kd\_file* sebagai primary key, *password*, dan *tanggal\_file*

**2.5 Spesifikasi Basis Data**

Dalam pembuatan aplikasi, terdapat juga rancangan basis data yang digunakan. Berikut spesifikasi basis data pada aplikasi ini :

**Tabel 1. Tabel Admin**

Nama	Jenis Data	Keterangan
Kd_admin	varchar (15)	Kode admin
Username	varchar (50)	Username admin
Password	varchar (50)	Password admin

**Tabel 2 Tabel File**

Nama	Jenis Data	Keterangan
Kd_file	int (5)	Kode File
Nama_file	text	Nama File
Password	Varchar(20)	Password File
Tanggal_file	timestamp	Tanggal User
Kd_User	Int(5)	Kode User

**Tabel 3 Tabel User**

Nama	Jenis Data	Keterangan
Kd_User	int (5)	Kode User
Username	Varchar(30)	Username
Password	Varchar(20)	Password
Tanggal_file	timestamp	Penanda
Join_Date	Timestamp	Tanggal Bergabung

Terdapat 3 tabel diantaranya pada tabel 1 Tabel Admin yang mempunyai field *kd\_admin* dengan jenis data varchar, *username* dengan jenis data varchar, dan *password* dengan jenis data varchar. Lalu pada tabel 2 Tabel File

ini mempunyai `kd_file` dengan jenis data int, `nama_file` dengan jenis data text, `password` dengan jenis data varchar, `tanggal_file` dengan jenis data timestamp, dan `kd_user` dengan jenis data int. Dan pada tabel terakhir yaitu Tabel Login mempunyai isi field `kd_user` dengan jenis data int, `username` dengan jenis data varchar, `password` dengan jenis data varchar, `counter` dengan jenis data char, dan `join_date` dengan jenis data timesamp.

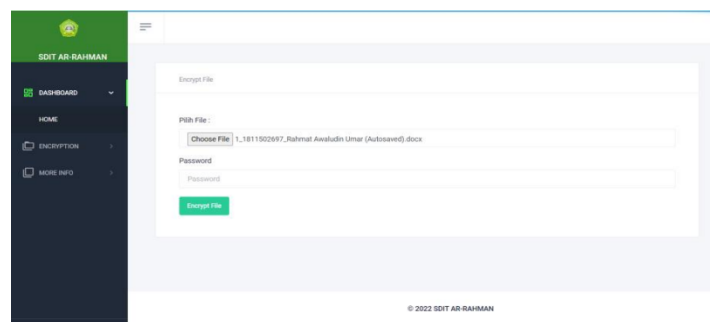
### 3. HASIL DAN PEMBAHASAN

#### 3.1 Implementasi Rivest Code 4 (RC4)

Berdasarkan penerapan metode yang diusulkan di bab sebelumnya maka berikut adalah hasil implementasi pada web yang dibuat.

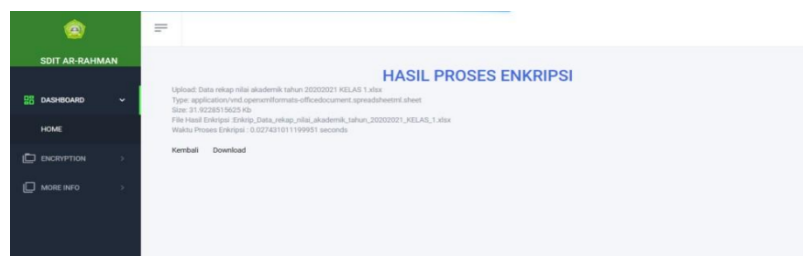
##### a. Implementasi Encrypt

Langkah pertama input file yang ingin di encrypt lalu masukan password yang hanya user dan admin saja yang mengetahuinya.



**Gambar 6.** Input Implementasi Encrypt

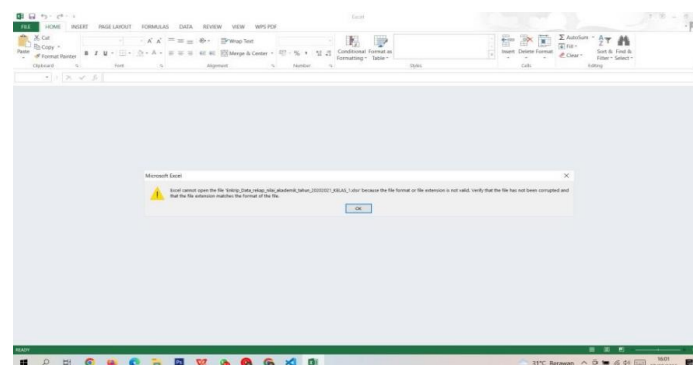
Pada Gambar 6 diatas klik encrypt untuk melanjutkan proses *encrypt* file tersebut. Jika sudah maka akan menampilkan hasil seperti gambar 7 dibawah ini



**Gambar 7.** Output Implementasi Encrypt

Pada bagian Encrypt ini telah berhasil mengamankan sebuah file dengan ukuran 31.9228515625 kb atau setara dengan 319228515,625 mb, dan mempunyai kecepatan Encrypt 0.027431011199951/detik

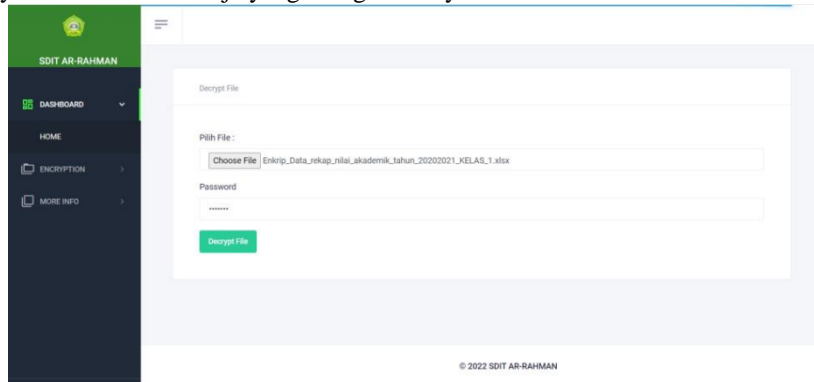
Pada gambar 7 klik download untuk melanjutkan menyimpan file tersebut, dan file tersebut yang akan di dekripsi. Dan pada gambar 8 adalah hasil dari implementasi encrypt.



**Gambar 8.** Hasil Implementasi *Encrypt*

b. Implementasi Decrypt

Langkah pertama input file encrypt yang sudah di download untuk di decrypt lalu masukan password file tersebut yang hanya user dan admin saja yang mengetahuinya.



Gambar 9. Input Implementasi Decrypt

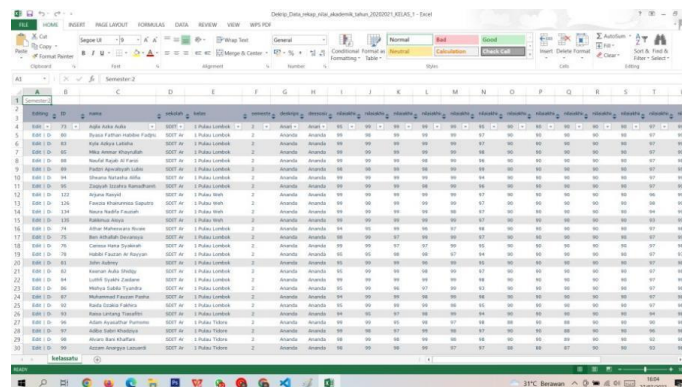
Pada gambar 9 diatas klik decrypt untuk melanjutkan proses decrypt file tersebut. Jika sudah maka akan menampilkan hasil seperti gambar 10 dibawah ini



Gambar 10. Output Implementasi Decrypt

Pada bagian Decrypt ini telah berhasil membuka keamanan sebuah file dengan ukuran 31.9228515625 kb atau setara dengan 319228515,625 mb, dan mempunyai kecepatan Decrypt 0.013211011886597/detik.

Download hasil file yang sudah didekrip, file sudah bisa digunakan kembali. Dan pada gambar selanjutnya, yaitu gambar 11 adalah hasil dari file yang sudah di dekrip.



Gambar 11. Hasil Implementasi Decrypt

Berikut adalah hasil dari implementasi Rivest Code 4 Berdasarkan bab sebelumnya tentang penerapan Rivest Code 4 yang akan dijabarkan melalui tabel 4 dan tabel 5 berikut.

**Tabel 4.** Implementasi Encrypt Rivest Code 4

Percobaan	Upload	Size (KB)	Hasil Encrypt	Waktu Proses (Secondh)
1	Data rekap nilai akademik tahun 20202021 KELAS 1.xlsx	31.9228515625	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_1.xlsx	0.0094840526580811/s
2	Data rekap nilai akademik tahun 20202021 KELAS 2.xlsx	24.431640625	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_2.xlsx	0.0065629482269287/s
3	Data rekap nilai akademik tahun 20202021 KELAS 3.xlsx	23.9873046875	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_3.xlsx	0.015224933624268/s
4	Data rekap nilai akademik tahun 20202021 KELAS 4.xlsx	23.33203125	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_4.xlsx	0.011126041412354/s
5	Data rekap nilai akademik tahun 20202021KELAS 5.xlsx	22.939453125	Enkrip_Data_rekap_nilai_akademik_tahun_20202021KELAS_5.xlsx	0.0059950351715088/s

**Tabel 5.** Implementasi Decrypt Rivest Code 4

Percobaan	Upload	Size (KB)	Hasil Encrypt	Waktu Proses (Secondh)
1	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_1.xlsx	31.9228515625	Dekrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_1.xlsx	0.038439989089966/s
2	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_2.xlsx	24.431640625	Dekrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_2.xlsx	0.014050006866455/s
3	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_3.xlsx	23.9873046875	Dekrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_3.xlsx	0.059432029724121/s
4	Enkrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_4.xlsx	23.33203125	Dekrip_Data_rekap_nilai_akademik_tahun_20202021_KELAS_4.xlsx	0.014281988143921/s
5	Enkrip_Data_rekap_nilai_akademik_tahun_20202021KELAS_5.xlsx	22.939453125	De_Data_rekap_nilai_akademik_tahun_20202021KELAS_5.xlsx	0.018555879592896/s

#### 4. KESIMPULAN

Setelah melakukan proses perancangan dan pembuatan website serta berdasarkan permasalahan yang telah disebutkan pada bab sebelumnya maka dapat disimpulkan sebagai berikut:

- a. Dengan membuat website dengan keamanan kriptografi yang menggunakan metode Rivest Code 4 (RC4) sebagai salah satu cara untuk mengamankan sebuah dokumen penting.

- b. Dengan Website yang dibuat pada penelitian ini dapat dijadikan salah satu contoh untuk mengamankan sebuah file, dan mengingatkan kepada seluruh masyarakat agar lebih berhati-hati dalam menyimpan sebuah dokumen penting.

## DAFTAR PUSTAKA

- [1] F. A. B. Purba, "Pengamanan File Teks Menggunakan Algoritma RC4," *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, pp. 420–425, 2020.
- [2] R. Damanik, "Sistem Enkripsi dan Dekripsi Serta Penyembunyian File Teks Menggunakan Algoritma RC4 dan End of File (Eof) Pada Citra Digital," *Jurnal ISD*, vol. 3, no. 1, pp. 50-56, 2018.
- [3] S. Darmawan, "Pengamanan Dokumen Menggunakan Kriptografi RC4 dan Steganografi EOF dengan Media VideoMP4 pada CV. Synergy Selaras," *Jurnal Teknologi Elektro*, vol. 8, no. 2, pp. 117-122, 2017.
- [4] K. Fahmi, "Pengamanan Data Arsip Pada Balai Desa Sidodadi Menggunakan Kriptografi Modern RC4," *RESOLUSI: Rekayasa Teknik Informatika dan Informasi*, vol. 2, no. 2, pp. 58-66, 2021.
- [5] F. S. Febriyani and A. Arfriandi, "Implementasi Algoritma RC4 Pada Sistem Pengamanan," *JISKA*, vol. 6, no. 3, pp. 171–177, 2021.
- [6] I. Anas, et al, "Perancangan Aplikasi Keamanan Data Dengan Kombinasi Algoritma Kriptografi RC4 dan One Time Pad," *JURIKOM (Jurnal Riset Komputer)*, vol. 8, pp. 20-27, 2021
- [7] D. Irwansyah, "Pengamanan Data Teks Dengan Algoritma Modifikasi RC4," *Pelita Informatika, Informasi dan Informatika* vol. 6, no. 3, pp. 309-312, 2018.
- [8] J. Prayudha, et al, "Implementasi Revest Code 4(RC4) Untuk Data Resep Obat Di RSUP H. Adam Malik," *KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)*, vol. 2, no. 3, pp. 174-181, 2021.
- [9] K. A. Seputra and G. A. J. Saskara, "Kriptografi Simetris RC4 Pada Transaksi Online Booking Engine System. *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 17, no. 2, pp. 286-295, 2020.
- [10] Rista, & A. S. Sitio, "Implementasi Keamanan Data Keuangan di smk swasta musda perbaungan menggunakan metode RC4," *JIKOMSI: Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 3, no. 1.1, pp. 60–66, 2021.
- [11] I. S. Sabana and L. Tanti, "Pengembangan Model Keamanan Data Inventory Dengan," *Jurnal FTIK*, vol. 1, no. 1, pp. 607–618, 2020.
- [12] N. Tanjung, "Perancangan Sistem Informasi Data Rekam Medis Pasien Rawat Jalan Pada Klinik Utama Al-Basyariah Citayam," *JITK: Jurnal Ilmu Pengetahuan dan Teknologi Komputer*, vol. 4, no. 1, pp. 119–124, 2018.
- [13] G. Ammary and S. Mulyati, "Aplikasi Kriptografi Untuk Keamanan Databse Dengan Metode RC4 dan Elgamal Berbasis Web Pada Jxl Design Co," *SKANIKA*, vol.11, no. 2, pp. 815–820, 2018.

ISSN 2962-8628



9

772962

862002

**FAKULTAS TEKNOLOGI INFORMASI**  
**UNIVERSITAS BUDI LUHUR**

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260

<https://senafti.budiluhur.ac.id/>