

Aplikasi Kerahasiaan Soal Uts Dan Uas Smp Al Washliyah 11 Percut Menggunakan Metode Feal

Confidential Application Of Al Washliyah Smp 11 Percut Uts And Uas Questions Using The Feal Method

Ricki Zulkarnaen¹, Sri Lestari Rahayu²

¹Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama

²Rekayasa Perangkat Lunak, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama

^{1,2}Jl.K.L. Yos Sudarso KM 6.5 Tanjung Mulia- Medan

E-mail: rickizulkarnaen99@gmail.com, aiyu.lestari13@gmail.com

ABSTRAK

Dalam proses sekolah maka setiap pelajar harus mengikuti prosedur mulai dari masuk kelas, belajar, mengerjakan tugas dan aktif di kegiatan lain di sekolah dan untuk dapat membuktikan hasil belajar yang di tempuh selama belajar maka seluruh pelajar wajib mengikuti ujian yaitu ujian tengah semester (UTS) dan ujian akhir semester (UAS) yang soalnya dibuat oleh para guru setiap mata pelajaran. Biasanya para guru menyerahkan Soal UTS atau UAS kepada Tata Usaha untuk dicetak ke kertas Ujian sehingga semua murid dapat memperoleh Soal Ujian ketika melaksanakan kegiatan Ujian. Masalah yang terjadi adalah tidak diterapkan kerahasiaan data Soal UTS dan UAS sehingga dapat disebarkan oleh pemegang soal UTS dan UAS untuk dijual ke para pelajar yang akan melaksanakan UTS atau UAS. Oleh sebab itu diperlukan sebuah cara agar Soal UTS dan UAS menjadi lebih aman. Penelitian ini menggunakan metode FEAL untuk mengatasi masalah kerahasiaan data soal UTS dan UAS. Dengan adanya metode FEAL maka SMP Al Washliyah 11 Percut mendapatkan kerahasiaan Soal UTS dan UAS.

Kata Kunci : Aplikasi, Kerahasiaan, Soal,Ujian, Metode FEAL.

ABSTRACT

In the school process, every student must follow the procedure starting from entering the class, studying, doing assignments and being active in other activities at school and to be able to prove the learning outcomes achieved during the study, all students are required to take exams, namely mid-semester exams (UTS) and final semester exams (UAS) whose questions are made by the teachers of each subject. Usually, teachers submit UTS or UAS questions to the Administration to be printed on exam paper so that all students can get exam questions when carrying out exam activities. The problem that occurs is that the confidentiality of UTS and UAS question data is not implemented so that it can be distributed by the holders of UTS and UAS questions to be sold to students who will take UTS or UAS. Therefore, a way is needed to make UTS and UAS questions more secure. This study uses the FEAL method to overcome the problem of confidentiality of UTS and UAS question data. With the FEAL method, SMP Al Washliyah 11 Percut gets the confidentiality of UTS and UAS questions.

Keywords: Application, Confidentiality, Questions, Exams, FEAL Method.

Keywords: Application, Confidentiality, Questions, Exams, FEAL Method.

Disubmit:05 Agustus 2024

Info Artikel :
Direview:07 September 2024

Diterima :08 Oktober 2024

Copyright © 2024 – senadimu. All rights reserved.

1. PENDAHULUAN

SMP Al Washliyah 11 Percut adalah sebuah instansi yang bergerak dalam bidang pendidikan yaitu sekolah menengah pertama. Sekolah Menengah Pertama merupakan jenjang pendidikan dasar pada pendidikan formal di Indonesia yang ditempuh dalam waktu 3 tahun. Pelajar sekolah atau siswa menengah pertama umumnya berusia 13-15 tahun. Sekolah Menengah Pertama merupakan masa transisi dari masa kanak-kanak ke dunia

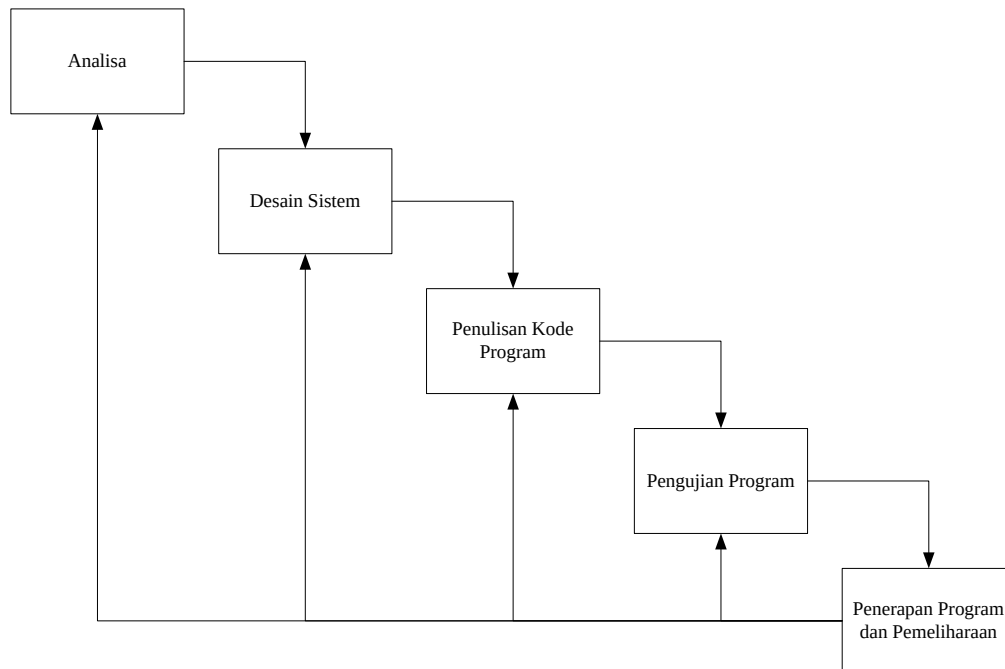
remaja. Masa SMP merupakan masa yang kritis bagi pendidikan siswa karena pada masa ini merupakan masa transisi dari kanak-kanak. (Yunus, 2020). Dalam proses sekolah maka setiap pelajar harus mengikuti prosedur mulai dari masuk kelas, belajar, mengerjakan tugas dan aktif di kegiatan lain di sekolah dan untuk dapat membuktikan hasil belajar yang di tempuh selama belajar maka seluruh pelajar wajib mengikuti ujian yaitu ujian tengah semester (UTS) dan ujian akhir semester (UAS) yang soalnya dibuat oleh para guru setiap mata pelajaran. Biasanya para guru menyerahkan Soal UTS atau UAS kepada Tata Usaha untuk dicetak ke kertas Ujian sehingga semua murid dapat memperoleh Soal Ujian ketika melaksanakan kegiatan Ujian. Masalah yang terjadi adalah tidak diterapkan kerahasiaan data Soal UTS dan UAS sehingga dapat disebarkan oleh pemegang soal UTS dan UAS untuk dijual ke para pelajar yang akan melaksanakan UTS atau UAS. Oleh sebab itu diperlukan sebuah cara agar Soal UTS dan UAS menjadi lebih aman.

Komputer telah banyak digunakan banyak orang sebagai pengelola data dan informasi, oleh karena itu peneliti menggunakan komputer untuk membuat sebuah aplikasi yang dapat merahasiakan isi data soal UTS dan UAS berbasis desktop menggunakan VB. Net dengan basis data SQL Server 2008, ilmu komputer yang dapat digunakan adalah kriptografi. Kriptografi merupakan seni yang dapat menghasilkan pesan rahasia. Ada dua proses dalam kriptografi diantaranya proses enkripsi dan dekripsi. Plaintext atau pesan asli yang dikodekan ke bentuk enkripsi dalam bentuk ciphertext disebut proses enkripsi. Proses dekripsi merupakan sebuah ciphertext atau pesan yang telah disandikan kemudian dipulihkan kembali menjadi plaintext. Kriptografi memiliki berbagai macam algoritma yang telah banyak digunakan sebagai pengamanan suatu informasi. Ada dua jenis pengelompokan Algoritma kriptografi, yaitu algoritma kriptografi modern dan algoritma kriptografi klasik. Algoritma kriptografi klasik bekerja menggunakan mode karakter dalam pengoprasian sedangkan pengoprasian algoritma kriptografi modern menggunakan mode bit. (Fadillah et al., 2022). Namun untuk dapat merahasiakan data soal UTS dan UAS menggunakan teknik kriptografi dibutuhkan metode yang tepat sehingga kerahasiaan data menjadi lebih baik. Berdasarkan penelitian yang dilakukan oleh Fadillah et al(2022) mengenai Implementasi Algoritma *Fast Encryption Algorithm* (FEAL) Dan Algoritma Fibonacci Mengamankan File Teks, Fadillah et al menggunakan metode *Fast Encryption Algorithm* (FEAL) untuk kerahasiaan file teks, sedangkan penelitian ini untuk kerahasiaan data soal UTS dan UAS SMP.

Berdasarkan penelitian yang dilakukan oleh Siregar (2020) mengenai Pengamanan Pesan Teks Menggunakan Algoritma FEAL dan RSA Pada Aplikasi *Android*, Siregar menggunakan metode *Fast Encryption Algorithm* (FEAL) untuk kerahasiaan pesanteks, sedangkan penelitian ini untuk kerahasiaan data soal UTS dan UAS SMP. Dari kedua penelitian terdahulu yang menggunakan metode FEAL dan telah berhasil mengatasi masalah kerahasiaan data maka peneliti menggunakan metode FEAL untuk mengatasi masalah kerahasiaan data soal UTS dan UAS. Dengan adanya metode FEAL maka SMP Al Washliyah 11 Percut mendapatkan kerahasiaan Soal UTS dan UAS. Pada proses enkripsi, pertama kali program akan memeriksa terlebih dahulu ada atau tidaknya teks pada kotak plaintext sebagai teks input proses enkripsi, jika teks belum dimasukkan maka akan ditampilkan pesan peringatan dan program akan dihentikan. Pada fungsi enkripsi, kemudian akan dicek jumlah karakter dari plaintextnya.

2. METODE

Metodologi penelitian merupakan tahapan penelitian yang dilakukan selama melakukan penelitian. Beberapa tahapan yang digunakan disajikan pada diagram *waterfall* pada gambar I.1.



Gambar I. Diagram *Waterfall* Metodologi Penelitian

Keterangan:

1. Analisa Kebutuhan
Pada tahapan ini peneliti melakukan analisa kebutuhan untuk penelitian yang berkaitan dengan data soal UTS dan UAS.
2. Perancangan
Pada tahapan ini model perancangan yang peneliti gunakan secara teori adalah pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.
3. Kode Program
Penulisan kode program menggunakan beberapa *platform* yaitu *Visual Basic.Net* dan menggunakan basis data *SQL server2008*.
4. Uji Coba
Uji coba dilakukan dengan dua cara yaitu *blackboxtesting* yaitu berupa tabel dan pengujian pada aplikasi menggunakan *Visual Basic.Net*. Apabila aplikasi masih terdapat kesalahan maka tahapan penelitian diperlukan peninjauan ulang.
5. Hasil
6. Hasil akhir tahapan penelitian ini yaitu menghasilkan Aplikasi kerahasiaan soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL.

3. HASIL DAN PEMBAHASAN

Metode yang digunakan untuk merahasiakan data Soal UTS dan UAS adalah FEAL. Berikut ini adalah rumus dan langkah dari metode FEAL beserta contoh perhitungannya :

1. Enkrip

Algoritma Enkrip FEAL:

$$C_i = (P_i + K_i) \bmod 256 \dots \dots \dots (1)$$

Dimana :

C : Ciphertext hasil proses enkrip

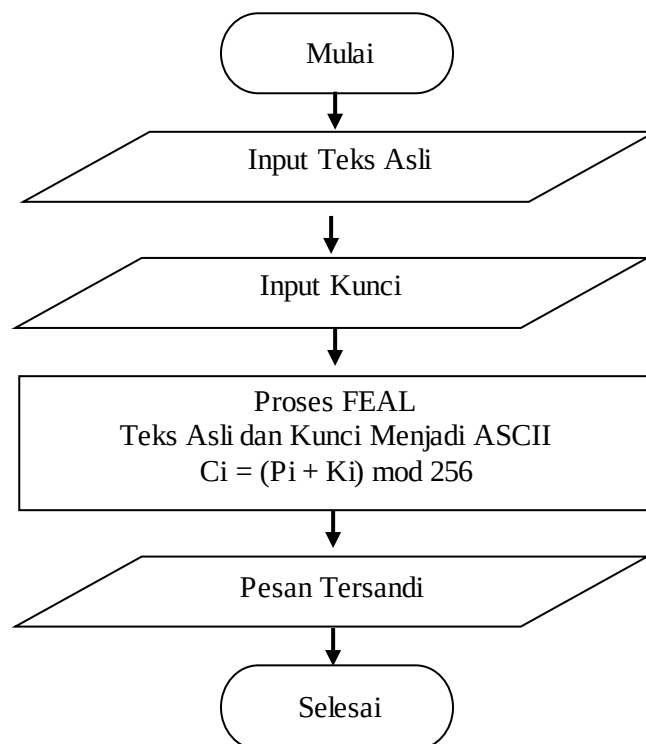
P : Plaintext untuk proses enkrip

K : Key untuk proses enkrip

mod : Sisa bagi

256 : Total ASCII pada keyboard

Flowchart enkripsi metode FEAL:



Gambar 2. Flowchart Enkripsi FEAL

Contoh Proses Enkrip :

Plaintext : SRIDINI AMANTA PUTRI SEMBIRING S.Pd

Key : 15 (ASCII: 49, 53)

Solusi :

Tabel 1. Enkrip FEAL SRIDINI

S	R	I	D	I	N	I	Plaintext
83	82	73	68	73	78	73	ASCII Plaintext
49	53	49	53	49	53	49	+
132	135	122	121	122	131	122	=
„	‡	z	Y	z	f	z	Ciphertext

Tabel 2. Enkrip FEAL PUTRI

P	U	T	R	I	Plaintext
80	85	84	82	73	ASCII Plaintext
49	53	49	53	49	+
129	138	133	135	122	=
•	Š	...	‡	z	Ciphertext

Tabel 3. Enkrip FEAL AMANTA

A	M	A	N	T	A	Plaintext
65	77	65	78	84	65	ASCII Plaintext
49	53	49	53	49	53	+
114	130	114	131	133	118	=
r	,	r	f	...	v	Ciphertext

Tabel 4. Enkrip FEAL SEMBIRING

S	E	M	B	I	R	I	N	G	Plaintext
83	69	77	66	73	82	73	78	71	ASCII Plaintext
49	53	49	53	49	53	49	53	49	+
132	122	126	119	122	135	122	131	120	=
„	z	~	w	Z	‡	z	f	x	Ciphertext

Tabel 5. Enkrip FEAL S.Pd

S	.	P	d	Plaintext
83	46	80	100	ASCII Plaintext
49	53	49	53	+
132	99	129	153	=
„	c	•	™	Ciphertext

Ciphertext:„‡zyzfzŠŠ...‡zr,rf...v,,z~wz‡zfx,,c™

2. Dekrip

Algoritma Dekrip FEAL:

$$P_i = (C_i - K_i) \bmod 256 \dots \dots \dots (2)$$

Dimana :

P : Plaintext hasil proses dekrip

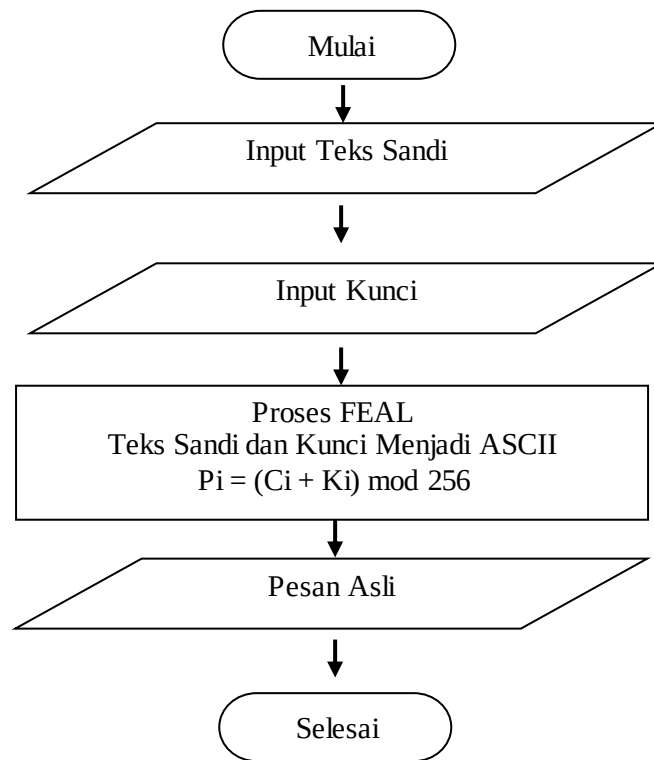
C : Ciphertext untuk proses dekrip

K : Key untuk proses dekrip

mod : Sisa bagi

256 : Total ASCII pada keyboard

Flowchart dekripsi metode FEAL:



Gambar 4. Flowchart Dekripsi FEAL

Contoh Proses Dekrip :

Tabel 6. Dekrip FEAL SRIDINI

„	‡	z	y	z	f	z	Ciphertext
132	135	122	121	122	131	122	ASCII Plaintext
49	53	49	53	49	53	49	-
83	82	73	68	73	78	73	=
S	R	I	D	I	N	I	Plaintext

Tabel 7. Dekrip FEAL PUTRI

•	Š	...	‡	z	Ciphertext
129	138	133	135	122	ASCII Plaintext
49	53	49	53	49	-
80	85	84	82	73	=
P	U	T	R	I	Plaintext

Tabel 8. Dekrip FEAL AMANTA

r	,	R	f	...	v	Ciphertext
114	130	114	131	133	118	ASCII Plaintext
49	53	49	53	49	53	-
65	77	65	78	84	65	=
A	M	A	N	T	A	Plaintext

Tabel 9. Dekrip FEAL SEMBIRING

„	z	~	w	z	‡	z	f	x	Ciphertext
132	122	126	119	122	135	122	131	120	ASCII Plaintext
49	53	49	53	49	53	49	53	49	-
83	69	77	66	73	82	73	78	71	=
S	E	M	B	I	R	I	N	G	Plaintext

Tabel 10. Dekrip FEAL S.Pd

„	c	•	™	Ciphertext
132	99	129	153	ASCII Plaintext
49	53	49	53	-
83	46	80	100	=
S	.	P	d	Plaintext

Plaintext: SRIDINI AMANTA PUTRI SEMBIRING S.Pd

Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL memiliki tampilan sebagai berikut:

1. Tampilan Halaman Utama

Tampilan Halaman Utama Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL memiliki tampilan sebagai berikut:



Gambar 4. Tampilan *Form* Halaman Utama

2. Tampilan Enkrip

Tampilan Enkrip Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL memiliki tampilan sebagai berikut:



Gambar 5. Tampilan *Form* Enkrip

3. Tampilan Dekrip

Tampilan Dekrip Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL memiliki tampilan sebagai berikut:

Gambar 5. Tampilan *Form* Dekrip

4. Pembahasan

Pembahasan mengenai perangkat keras dan perangkat lunak dalam pembuatan Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL dijabarkan sebagai berikut:

1. Perangkat keras laptop dengan spesifikasi sebagai berikut:
 - a. Processor Minimal Core 2 duo
 - b. RAMminimal 4 Gb
 - c. Hardisk minimal 80 Gb
2. Perangkat Lunak dengan spesifikasi sebagai berikut:
 - a. OS Windows
 - b. Visual Studio 2010

5. Uji Coba

Uji coba pada Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL menggunakan *blackbox testing* sebagai berikut:

Tabel 11. *Blackbox Testing Form* Halaman Utama

No	Form Halaman Utama	Hasil Uji	Validasi
1	Klik Mulai	Aplikasi akan menampilkan form enkrip/dekrip	Sesuai

Tabel 12. *Blackbox Testing Form* Enkrip

No	Form Enkrip	Hasil Uji	Validasi
1	Pilih File, Tulis Kunci, Klik Enkrip	Aplikasi akan mengenkrip file serta menyimpannya	Sesuai

Tabel 13. *Blackbox Testing Form* Dekrip

No	Form Dekrip	Hasil Uji	Validasi
1	Pilih File, Tulis Kunci, Klik Dekrip	Aplikasi akan mendekrip file serta menyimpannya	Sesuai

6. Hasil Uji Coba

Hasil uji coba terhadap sistem secara manual dan praktek memiliki hasil sebagai berikut:

1. Koneksi dari aplikasi ke basis data SQL Server berjalan dengan baik.
2. Proses dari Soal UTS teks telah berjalan dengan baik.
3. Proses dari Soal UAS teks telah berjalan dengan baik.
4. Perhitungan teori dengan perhitungan aplikasi telah sesuai.
5. Penggunaan aplikasi yang sederhana.

Tabel 14. Hasil Uji Coba Soal UTS

S	R	I	D	I	N	I	Plaintext
83	82	73	68	73	78	73	ASCII Plaintext
49	53	49	53	49	53	49	+
132	135	122	121	122	131	122	=
„	‡	z	y	z	f	z	Ciphertext

Tabel 15. Hasil Uji Coba Soal UTS

„	‡	z	y	z	f	z	Ciphertext
132	135	122	121	122	131	122	ASCII Plaintext
49	53	49	53	49	53	49	-
83	82	73	68	73	78	73	=
S	R	I	D	I	N	I	Plaintext

4.KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Dengan menggunakan Aplikasi Kerahasiaan Soal UTS dan UAS SMP Al Washliyah 11 Percut Menggunakan Metode FEAL maka Soal UTS dan UAS mendapatkan kerahasiaan sehingga tidak disebarkan.
2. Dengan menggunakan data UTS dan UAS serta langkah metode FEAL maka dapat menerapkan metode FEAL untuk kerahasiaan data soal UTS dan UAS

UCAPAN TERIMA KASIH

Penulis Sangat Berterima Kasih Kepada Universitas Potensi Utama yang telah memberikan banyak masukan dan saran berharga dalam penyelesaian penelitian ini. Kolaborasi dan dukungan dari universitas sangatlah berarti dalam mengembangkan penelitian ini. Terima kasih atas kontribusi yang luar biasa untuk keberhasilan penelitian ini.

REFERENSI

- [1] Aditya Fajar Ramadhan, Ade Dwi Putra, & Ade Surahman. (2021). Aplikasi Pengenalan Perangkat Keras Komputer Berbasis Android Menggunakan augmented Reality (Ar). *Jurnal Teknologi Dan Sistem Informasi (JTISI)*, 2(2), 24–31. <http://jim.teknokrat.ac.id/index.php/JTISI>
- [2] Aria, M., Widodo, A., Thasandra, M., Sutra, S. O., Nasution, A. B., Ikhwan, A., Negeri, U. I., Utara, S., William, J., Ps, I. V., Estate, M., Percut, K., Tuan, S., & Serdang, D. (2023). Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES. *Journal on Education*, 05(03), 6780–6787.
- [3] Fadillah, R., Idris, A. S., Marlina, D., Lubis, G., & Meisisri, R. (2022). *Implementasi Algoritma Fast Encryption Algorithm (FEAL) Dan Algoritma Fibonacci Mengamankan File Teks*. 295–300.
- [4] Indaryono, I., Yusuf, A. M., & Pebrianti, C. (2021). Sistem Informasi Akuntansi Pengelolaan Kas Kecil dengan Metode Fluktuatif Pada CV Focus Etania Zashika Karawang Menggunakan Visual Basic. Net. *Prosiding Seminar Nasional ...*, September, 45–54. <https://alumni.rosma.ac.id/index.php/inotek/article/view/113%0Ahttps://alumni.rosma.ac.id/index.php/inotek/article/download/113/118>
- [5] Jaya, R. M. (2023). 1, 2, 1, 2. 1(1), 21–27.
- [6] Khudzaifah, M. (2020). Implementasi Quasigroup Hybrid Encryption untuk Mengamankan Soal Ujian. *Prosiding SI MaNIs (Seminar ...)*, 3(1), 37–42. <http://conferences.uin-malang.ac.id/index.php/SIMANIS/article/view/1175>
- [7] Kudus, I. (2019). 4868-15130-1-Sm. *Jurnal Pendidikan Matematika*.
- [8] Meliasari, S., Astuti, S. W., Putri, T. Y., & Walid, A. (2022). ANALISIS SOAL UJIAN AKHIR SEMESTER (UAS) MATAPELAJARAN BIOLOGI di SEKOLAH MENENGAH ATAS (SMA) NEGERI 6 SELUMA TAHUN AJARAN 2018/2019. *EDUPROXIMA : Jurnal Ilmiah Pendidikan IPA*, 4(1), 37–43. <https://doi.org/10.29100/eduproxima.v4i1.2764>
- [9] Mirawati, & Purnia, D. S. (2015). Pada Sekolah Menengah Pertama. *Jurnal Informatika*, II(2), 385–394. <https://ejournal.bsi.ac.id/ejurnal/index.php/ji/article/view/115>
- [10] Pohan, M. I., Hariyanto, E., & Izhari, F. (2022). Pengacakan Soal Ujian Online Berbasis Web Menggunakan Algoritma Knuth Shuffle Pada SMK Gelora Jaya Nusantara Medan. *Bulletin of Information Technology (BIT)*, 3(4), 294–300.
- [11] Rachmawati, D., Budiman, M. A., & Siburian, W. S. E. (2018). Hybrid cryptosystem implementation using fast data encipherment algorithm (FEAL) and goldwasser-micali algorithm for file security. *Journal of Physics: Conference Series*, 1013(1). <https://doi.org/10.1088/1742-6596/1013/1/012159>
- [12] Sari, R. I. (2020). Analisis sikap toleransi belajar IPA siswa sekolah menengah pertama. *Jurnal Penelitian Ilmu Pendidikan*, 13(2), 120–128. <http://journal.uny.ac.id/index.php/jpiphttps://doi.org/10.21831/jpip.v13i2.35409>
- [13] Sativa, O. (2023). 9+Publish-+Oriza+Sativa+111-124. 02(01), 111–124.
- [14] Setiyadi, D., Arifin, R. ., & Henderi. (2020). Fungsi Date dalam Data Manipulation Language Menggunakan Bahasa Query dengan SQL Server. *Informatics for Educators and Professionals*, 4(2), 163–172.
- [15] Sihombing, V., & Yanris, G. J. (2020). Penerapan Aplikasi Dalam Mengolah Aset Desa (Studi Kasus : Kepenghuluan Sri Kayangan) 1). *Terakreditasi DIKTI*, 4(1), 12–15.

- [16] Siregar, S. N. (2020). Pengamanan Pesan Teks Menggunakan Algoritma FEAL dan RSA Pada Aplikasi Android. *Journal of Computer System and Informatics ...*, 1(4), 328–336. <https://ejurnal.seminar-id.com/index.php/josyc/article/view/351>
- [17] Wicaksana, B., & Setiawan, M. (2020). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Berkas Soal Ujian. *Teknois : Jurnal Ilmiah Teknologi Informasi Dan Sains*, 10(1), 25–34. <https://doi.org/10.36350/jbs.v10i1.74>