PENERAPAN SISTEM KEAMANAN DOKUMEN PENGARSIPAN MENGGUNAKAN *ALGORITMA RIVEST CODE 4* BERBASIS WEBSITE (STUDI KASUS: PRODI TEKNIK INFORMATIKA UKI PAULUS MAKASSAR)

Program Studi TeknikInformatika
Fakultas Informatika dan Komputer
Universitas Kristen Indonesia Paulus (UKI-Paulus)

Frederick Mangguali[1)], Hermin Arrang[2)],Erick Depthios[3)]
Program Studi Teknik Informatika
Fakultas Informatika dan Komputer
Universitas Kristen Indonesia Paulus
email : frederickmangguali0@gmail.com[1)], herminarrang12@gmail.com[2)],
erickdepthios@gmail.com[3)]

ABSTRACT

The University of UKI Paulus Makassar manages numerous documents that are still archived manually. To enhance efficiency and reduce the amount of physical documentation required, a document archiving website has been developed. However, the security of documents within this system must be ensured to provide adequate protection. One security method that can be applied is cryptography, particularly the Rivest Cipher 4 (RC4) algorithm. This research aims to implement document archiving security using the RC4 cryptographic algorithm. By employing the RC4 algorithm, it is expected that documents in the archiving system will be protected from external threats while achieving a higher efficiency level compared to other cryptographic algorithms.

The results of this study include the implementation of a website-based document archiving security system using the RC4 algorithm. This system enables users to upload, archive, access, and manage documents with a high level of security. Archived documents are encrypted using the RC4 algorithm before being stored on the server, and only users with the correct access credentials and keys can decrypt and access these documents. By adopting this system, the Informatics Engineering Program at UKI Paulus Makassar aims to enhance the security of document archiving and protect sensitive data. Furthermore, this research contributes to the development of information security and web-based archiving applications employing robust cryptographic algorithms.

Keywords: *Security, Cryptography, Documents, Archiving*

ABSTRAK

Universitas UKI Paulus Makassar memiliki banyak dokumen yang saat ini masih diarsipkan secara manual. Dalam rangka meningkatkan efisiensi dan mengurangi jumlah dokumen fisik yang perlu disimpan, dibangunlah sebuah website untuk pengarsipan dokumen. Namun, keamanan dokumen dalam sistem ini masih perlu diperhatikan agar dokumen-dokumen tersebut terlindungi dengan baik. Salah satu metode keamanan yang dapat diterapkan adalah dengan menggunakan kriptografi, khususnya algoritma *Rivest Code* 4 (RC4). Penelitian ini bertujuan untuk menerapkan sistem keamanan dokumen pengarsipan dengan menggunakan algoritma kriptografi RC4. Dengan menerapkan algoritma RC4, diharapkan dokumen-dokumen dalam sistem pengarsipan akan terlindungi dari serangan luar dan memiliki tingkat efisiensi yang baik dibandingkan dengan algoritma kriptografi lainnya.

Hasil dari penelitian ini adalah implementasi sistem keamanan dokumen pengarsipan berbasis website dengan menggunakan algoritma RC4. Sistem ini memungkinkan pengguna untuk mengunggah, mengarsipkan, mengakses, dan mengelola dokumen dengan tingkat keamanan yang tinggi. Dokumen-dokumen yang diarsipkan akan dienkripsi menggunakan algoritma RC4 sebelum disimpan di server, dan hanya pengguna yang memiliki akses dan kunci yang tepat yang dapat mendekripsi dan mengakses dokumen-dokumen tersebut. Dengan menerapkan sistem ini, diharapkan Program Studi Teknik Informatika UKI Paulus Makassar dapat meningkatkan keamanan dokumen pengarsipan dan melindungi data yang sensitif. Selain itu, penelitian ini juga memberikan kontribusi terhadap pengembangan keamanan informasi dan aplikasi pengarsipan berbasis web dengan menggunakan algoritma kriptografi yang kuat.

Kata Kunci: Keamanan, Kriptografi, Dokumen, Pengarsipan

I. PENDAHULUAN

Universitas Kristen Indonesia Paulus (UKI Paulus) Makassar memiliki banyak dokumen seperti biodata dan surat. Dokumen-dokumen digital ini seringkali berisi informasi penting dan rahasia yang perlu dijaga kerahasiannya. Aktivitas pada penyimpanan data secara *digital* mempunyai resiko hal ini terlihat apabila sebuah aktivitas tersebut dapat diakses oleh orang yang tidak bertanggung jawab dan orang yang tidak berkepentingan (*unauthorized person*) (Nathasia, 2012). Oleh karena itu, keamanan dokumen-dokumen digital menjadi sangat penting untuk memastikan kerahasiaan, integritas dan ketersediaanya.

Dalam menjaga keamanan dokumen-dokumen digital diperlukan sebuah keamanan yang sangat kuat. kriptografi merupakan salah satu cara yang efektif untuk keamanan dokumen digital. Kriptografi merupakan sebuah ilmu yang mempelajari tentang teknik matematis yang berkaitan dengan topik keamanan informasi (Munir,

2019). Dalam keamanan kriptografi data asli akan di ubah menjadi bentuk yang tidak bisa dibaca (*enkripsi*) dan kemudian mengembalikan data tersebut ke bentuk aslinya (*dekripsi*) dengan menggunakan kunci tertentu.

Salah satu jenis kriptografi yang digunakan adalah *algoritma rivest code 4. Algoritma Rivest Code 4 (RC4)* merupakan salah satu algoritma kriptografi jenis *stream cipher* dalam mengamankan data. Algoritma ini sendiri banyak digunakan pada berbagai aplikasi termasuk dalam sistem keamanan file. Selain itu perkembangan keamanan file berbasis web juga semakin meningkat karena memungkinkan adanya pengaksesan jarak jauh oleh *user* dan dalam penggunannya yang fleksibel. *Algoritma rivest code 4* mempunyai kelebihan pada data yang lebih panjang yang beragam, algoritma ini juga dinilai sangat cepat dalam pemrosesannya kurang lebih 10 kali lipat dari *DES* (Hakim et al., 2014).

Sehingga berdasarkan dari latar belakang diatas maka diangkat sebuah penelitian dengan judul "Penerapan Sistem Keamanan Dokumen Pengarsipan Menggunakan *algoritma rivest code 4* Berbasis Website (Studi Kasus: Prodi Teknik Informatika UKI Paulus Makassar)".

II. LANDASAN TEORI

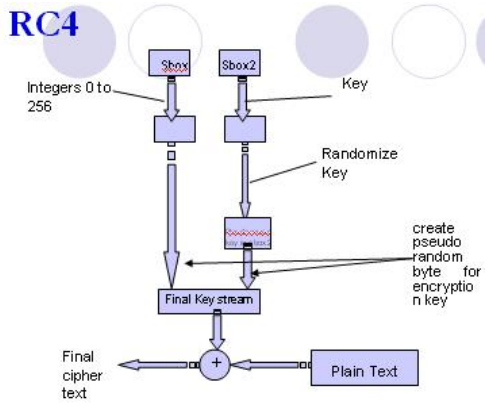
1.1 Kriptografi

Kriptografi mempunyai sejarah yang cukup panjang dan sangat menakjubkan. Informasi yang lengkap tentang sejarah kriptografi itu sendiri dapat kita temukan dalam sebuah buku david khan yang berjudul *The CodeBreakers*. Buku ini mempunyai tebal 1000 halaman ini menulis tentang rinci sejarah kriptografi. Kriptografi tidak menyembunyikan pesan tetapi mengubah pesan sehingga sulit untuk diperoleh pesan aslinya. Cara kerjanya pesan yang diubah dengan cara transposisi (mengubah letak huruf) dan subtitusi (mengantikan huruf/kata dengan huruf/kata lainnya) (Rahardjo, 2005).

1.2 Algoritma RC4

Algoritma Kriptografi Rivest Code 4 (RC4) adalah algoritma kunci *simetris* dibuat oleh *RSA Data Security Inc* (RSADI) berbentuk *stream cipher*. RC4 sendiri mempunyai panjang kunci 1 sampai 256 *Byte* yang digunakan untuk menginisialisasikan tabel sepanjang 256 *Byte*. Tabel ini digunakan untuk generasi yang berikutnya

dari *pseudorandom* yang memakai *XOR* dengan *plaintext* untuk menghasilkan *ciphertext* (Ariyus, 2006).



Gambar 2.2 Proses RC4 Stream Cipher (Ariyus, 2006)**.**

Metode RC4 stream cipher terbagi atas dua bagian yaitu *Key Setup* atau *Key Schedulling Algorithm* (KSA) dan *Stream Generation* atau *Pseudo Random Generation Algorithm* (PRGA) dan proses *XOR* dengan *Stream* data.

Pada sandi RC4 menggunakan *state*, yaitu larik *byte* berukuran 256 dan tercampur oleh kunci. Proses metode algoritma RC4.

1. Membuat inisalisasi variable S sepanjang 256.
2. Untuk i=0 hingga i=256 dilakukan perulangan untuk mengisi *array* S.
3. Isikan S dengan nilai i
4. Inisalisasi *array* K sepanjang *key* dan lakukan perulangan sepanjang *plainteks* dalam bentuk *ASCII.*
5. Proses *Key Schedulling Algorithm* (KSA)

a. Isi nilai i=0 sepanjang 256.
b. Inisalisasi J untuk penyimpanan sementara.
c. Lakukan proses j=nilai sebelumnya + nilai S pada *index* ke i + nilai K *index* ke i dalam bentuk *ASCII* (*Index modulus* jumlah *key* yang diinputkan) kemudian hasilnya dibagi 256.
d. Setelah melakukan proses diatas selanjutnya yaitu proses *Swap* yaitu proses pengacakan *plainteks* menjadi *ciphertext*.

6. Proses *Pseudo Random Generation Algorithm* (PRGA)

a. Lakukan pengisian pada *indeks* i dan j dengan nilai 0
b. Untuk i = 0 lakukan sepanjang i = panjang *plainteks*.
c. Isi nilai dengan hasil operasi (i+1) mod 256.
d. Isi nilai j dengan hasil operasi (j+s(i)) mod 256.
e. Tukar nilai s(i) dan s(j).
f. Isi nilai t dengan hasil operasi (s(i)+(s(j) mod 256))mod 256.
g. Isi nilai y dengan nilai s(t).
h. Nilai y dikenakan operasi *XOR* terhadap *plaintext.*

Dengan demikian akan dihasillkan *ciphertext* dengan hasil *XOR* antar *stream key* dari S-Box dan *plaintext* secara berurutan. Untuk menghasilkan *key stream, cipher* menggunakan *state internal* yaitu:

1. Tahap *key scheduling* dimana *state automaton* diberi nilai awal berdasarkan kunci *enkripsi, state* yang diberi awal berupa *array* yang merepresntasikan suatu permutasi dengan 256 elemen. Jadi hasil algoritma KSA adalah permutasi awal, *array* yang mempunyai 256 elemen ini namakan dengan S.

   for i = 0 to 256

   S[i] : = i

   j : = 0

   for i = 0 to 255

   j : = (j + S[i] + key [i mod *keylength*]) mod 256

   swap(S[i], S[j])
2. Tahap *pseudorandom generation* (PRGA) dimana *state automaton* beroperasi dan outputnya menghasilkan *keystream*. Setiap putaran bagian *keystream* sebesar 1 *byte* (nilai antara 0 sampai 255) di *output* oleh PRGA berdasarkan state S.

   i := 0

   j := 0

   loop

   I := (I + 1) mod 256

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

   Swap (S[i] , S[j])

Output S[(S[i] + S[j]) mod 256]

Setelah terbentuk *keystream* kemudian k*eystream* tersebut dimasukan dalam operasi *XOR* dengan *plaintext* yang ada dengan sebelumnya pesan dipotong-potong menjadi *byte-byte.*

1.3 Dokumen

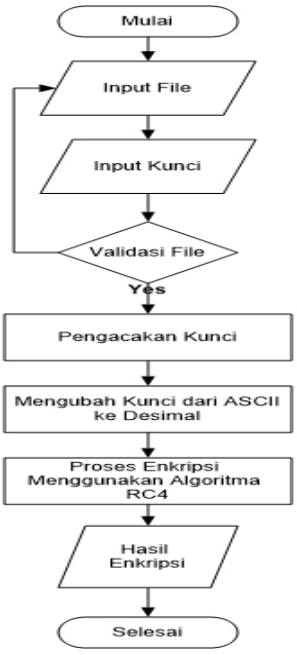
Dokumen merupakan informasi yang terstruktur yang bisa dari informasi terekam, diterbitkan atau tidak diterbitkan yang bisa dalam bentuk fisik juga digital dan dikelola sebagai unit distrik dalam sistem informasi (Basuki, 2003).

Menurut (Amin & Siahaan, 2016) dokumen adalah sumber tertulis dari informasi sejarah sebagai kebalikan dari pada kesaksian lisan, artetak. Pengertian dokumen dalam artian luas merupakan proses pembuktian yang didasarkan atas sumber jenis apapun, baik yang bersifat tulisan, lisan, gambaran atau arkeologis.

III. PERANCANGAN SISTEM

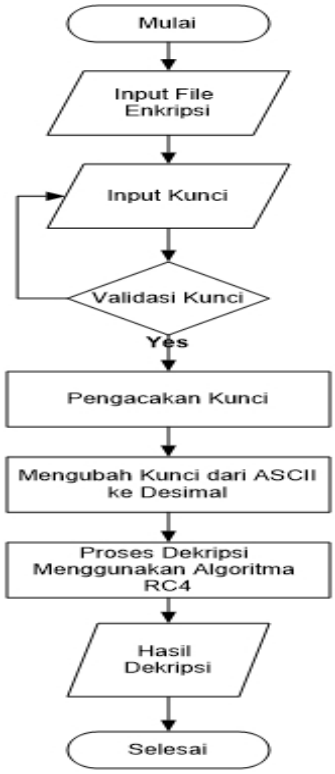
Keamanan terhadap dokumen merupakan suatu keharusan untuk menjaga validatas dan integritas data yang ada

didalamnya. Proses analisis sistem ini sangat diperlukan untuk meningkatkan keamanan pada dokumen serta mengetahui alur kerja sistem tersebut.



Gambar 3.1 Flowchart Enkripsi

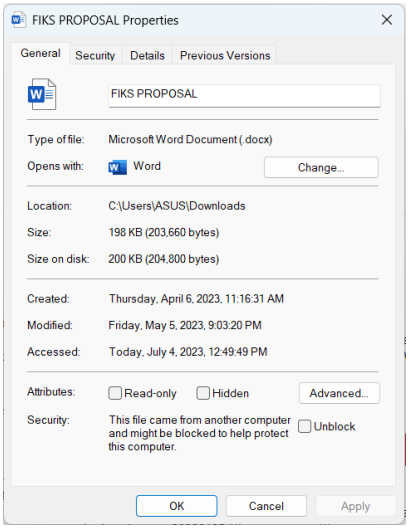
Gambar 3.2 Flowchart Dekripsi



Gambar 3.2 Flowchart Dekripsi

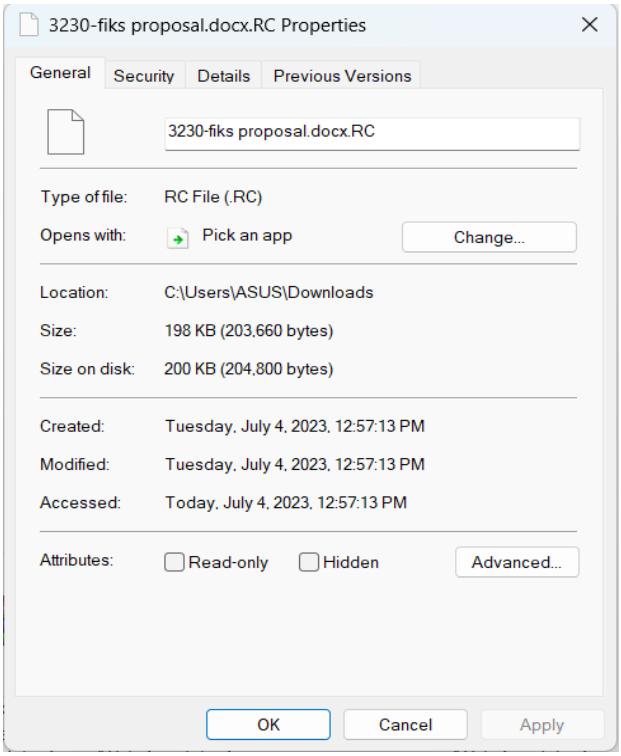
IV. HASIL DAN PEMBAHASAN

Pada hasil penelitian ini yang bertujuan untuk mengamankan dokumen pengarsipan dengan menggunakan algoritma *kriptografi rivest code* 4 (RC4) dalam mengamankan file dokumen agar file yang bersifat penting dan rahasia terjaga dari orang yang tidak bertanggung jawab. Penulis membuat *prototype* berupa *website* yang dapat digunakan untuk enkripsi dan dekripsi file dokumen. *Website* ini dapat di akses secara online via situs dan perancangan menggunakan *framework codeigniter* serta bahasa pemrograman php.



Gambar 4.1 Pengujian Enkripsi File D*ocx*

Pada gambar 4.1 digunakan file bertipe *docx* atau bisa menggunakan versi doc yang memiliki ukuran file 198 KB. File tersebut akan di enkripsi menggunakan *Rivest Code* 4 (RC4) dan setelah dilakukan enkripsi file akan berubah ke *extension .RC* serta ukuran file asli akan tetap sama setelah dilakukannya enkripsi.



Gambar 4.2 Hasil Dari Enkripsi

Pada gambar 4.2 diatas merupakan hasil dari proses enkripsi menggunakan algoritma *Rivest Code 4* (RC4). Hasil dari enkripsi nanti nya bertipe *extension .RC* yang merupakan extension dari enkripsi *Rivest Code 4.*

1.4 Pengujian Kecepatan Enkripsi

Tabel 1 Pengujian Kecepatan Enkripsi.

No	Nama File	Ukuran	kecepatan
1	Sk pa awal 20211.pdf	1.42 MB	0.25243616104126/s
2	137 sk mengajar semester akhir 2022-2023 prodi teknik informatika.pdf	0.21MB	0.0592360496521/s
3	lulusan.xls	0.18MB	0.027866125106812/s

No	Nama File	Ukuran	kecepatan
4	undangan.jpg	0.15MB	0.032846927642822/s
5	sk pa 2019.docx	0.01MB	0.002362012863159 2/s
6	sk pa awal 20202021.pdf	1.34MB	0.221139907836 91/s
7	sk mengajar semester awal 2021-2022 prodi teknik informatika.pdf	0.35MB	0.046556949615479/s
8	disatukan (1).docx	8.02MB	1.495236158371/s

1.5 Pengujian Kecepatan Dekripsi.

Tabel 2 Pengujian Kecepatan Dekripsi.

No	Nama File	Ukuran	Kecepatan
1.	Sk pa awal 20211.pdf.RC	1.42 MB	0.24300718307495/s
2.	137 mengajar semester akhir 2022-2023 prodi teknik informatika.pdf.RC	0.21 MB	0.055736064910889/s
3.	lulusan.xls.RC	0.18 MB	0.030760049819946/s
4.	undangan.jpg.RC	0.15 MB	0.025964021682739 /s
5.	sk pa 2019.docx.RC	0.01 MB	0.0021021366119385/s
6.	sk pa awal 20202021.pdf.RC	1.34 MB	0.19176697731018/s
7.	sk mengajar semester awal 2021-2022 prodi teknik informatika.pdf.RC	0.35 MB	0.058746814727783/s
8.	disatukan (1).docx.RC	8.02 MB	1.4792861938477/s

V KESIMPULAN

1.5 Kesimpulan

Berdasarkan dari penelitian "Penerapan sistem keamanan dokumen pengarsipan menggunakan *algoritma rivest code* 4 berbasis website (studi kasus: Prodi Teknik Informatika UKI Paulus Makassar)" dalam pengamanan dokumen arsip dapat disimpulkan beberapa hal diantaranya:

1. Melalui penelitian ini, diharapkan dapat merancang sebuah website yang memiliki sistem keamanan dokumen pengarsipan menggunakan algoritma *rivest code* 4. Dengan adanya website ini, diharapkan dapat meningkatkan keamanan dokumen pengarsipan, sehingga hanya orang yang memiliki *otorisasi* yang sah yang dapat mengakses dan mengelola dokumen-dokumen tersebut.
2. Dalam upaya menguji sistem keamanan dokumen pengarsipan yang menggunakan algoritma *rivest code* 4 berbasis website metode *Black* Boix. Metode *Black Box* menguji sistem tanpa memperhatikan implementasi internalnya, melainkan fokus pada *fungsionalitas* dan *respons* sistem terhadap input tertentu. Dengan metode ini, diharapkan dapat mengetahui sejauh mana tingkat keamanan sistem dalam melindungi dokumen-dokumen pengarsipan.

1.6 Saran

Untuk kedepannya dapat dikembangkan dengan mengkombinasikan algoritma yang

baru dengan tingkat keamanan tinggi sehingga aplikasi yang dihasilkan akan jauh lebih aman serta untuk keamanan dalam pengamanan kunci untuk menggunakan hashing yang mempunyai tingkat keamanan yang relatif sulit dibobol.

DAFTAR PUSTAKA

Amin, S., & Siahaan, K. (2016). Arsip Berbasis Web Pada Sekolah Tinggi Ilmu Tarbiyah. *Jurnal Manajemen Sistem Informasi*, *1*(1), 1–10.

Apdilah, D., & Swanda, H. (2018). Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP. *Jurnal Teknologi Informasi*, *2*(1), 45. https://doi.org/10.36294/jurti.v2i1.407

Ariyus, D. (2006). Kriptografi keamanan data dan komunikasi. *Graha Ilmu, Yogyakarta*.

Basuki, S. (2003). *Manajemen Arsip Dinamis*. Gramedia Pustaka Utama.

Dharwiyanti, S., & Wahono, R. S. (2003). Pengantar Unified Modeling Language (UML). *Ilmu Komputer*, 1–13.

Febriyani, F. S., & Arfriandi, A. (2021). *Implementasi Algoritma RC4 pada Sistem Pengamanan Dokumen Digital Soal Ujian*. *6*(3), 171–177.

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *TECHSI - Jurnal Teknik Informatika*, *13*(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Haji, W. H., Mulyono, S., Informasi, J. S., Komputer, F. I., Mercu, U., & Jakarta, B. (2012). *IMPLEMENTASI RC4 STREAM CIPHER UNTUK KEAMANAN BASIS DATA*. *2012*(Snati), 15–16.

Hakim, E. L., Khairil, K., & Utami, F. H. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php. *Jurnal Media Infotama*, *10*(1).

Harold F. Tipton, M. K. (2007). *Information Security Management Handbook* (6th Editio). CRC Press. https://doi.org/https://doi.org/10.1201/9781439833032

Intani, S. M. (2019). *Implementasi Kriptografi AES pada File Word*. *December*.

Munandar, A., Of, D., Data, T., Applications, S., Stream, U., Algorithm, C., Munandar, A., Rosnelly, R., Jhony, C., Sianturi, M., Teknik, J., Potensi, I., Jurusan, D., Informatikauniversitas, T., Utama, P., Utama, U. P., & Cipher, M. S. (n.d.). *TEKS MENGGUNAKAN ALGORITMA STREAM*. 407–416.

Munir, R. (2019). Kriptografi Edisi Kedua. *Bandung. Penerbit Informatika*.

Nathasia, N. D. (2012). Penerapan teknik Kriptografi stream cipher untuk pengaman basis data. *Basis Data*, *6*(1).

Rahardjo, B. (2005). Keamanan sistem informasi berbasis internet. *Bandung: PT. Insan Indonesia*.

Raharjo, B. (2021). Keamanan Sistem Informasi. *Penerbit Yayasan Prima Agus Teknik*, 1–429.

Ramadhan, R., & Soetanto, H. (2022). Penerapan Kriptografi Menggunakan Advanced Encryption Standard 128 Untuk Pengamanan File Pada SMK Muhammadiyah 4. *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, *1*(1), 29–38.

Rosa, A. S. (2016). *Rekayasa perangkat lunak terstruktur dan berorientasi objek*.

Silalahi, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *J. Nas. Komputasi Dan Teknol. Inf*, *3*(2).

Suryadi, E., Nurwijayanti, K., & Mataram, U. T. (2022). *Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris*. *9*(3).