Jurnal Sistem Informasi ISSN P : 2598-599X; E: 2599-0330

Sistem Informasi Manajemen Data Surat Dengan Algoritma *Blowfish*

Essay Puspita Sitopu [1], Nurul Khairina [2*], Rizki Muliono [3], Muhathir [4]
Teknik Informatika Universitas Medan Area
Jl. Kolam Nomor 1 Medan Estate
Email : essaypuspita@gmail.com, nurulkhairina27@gmail.com, rizkimuliono@gmail.com, muhathir@staff.uma.ac.id
*corresponding author : Nurul Khairina

Abstrak

Perkembangan teknologi informasi yang semakin pesat saat ini menuntut kita untuk mampu mengikuti perkembangannya. Komunikasi secara digital di era modern dapat menjadi salah satu ancaman akan adanya penyadapan, penyalahgunaan informasi, dan pencurian data penting yang tidak diinginkan oleh pihak yang tidak berwenang. Apalagi jika informasi tersebut bersifat rahasia dan memliki ruang lingkup yang luas dalam kenegaraan. Oleh karena itu, keamanan penyimpanan data menjadi sangat penting. Data yang terdapat pada surat masuk ataupun surat keluar dalam satu sekolah juga memliki kerahasiaan yang harus dijaga, kemana surat dikirimkan dan dari mana surat berasal juga menjadi salah satu hal yang perlu dijaga kerahasiannya. Atas dasar inilah peneliti ingin membangun sistem informasi manajemen surat yang berfokus pada penyimpanan data surat atau database surat. Dari berbagai metode penyandian yang ada hingga saat ini, salah satunya adalah metode Kriptografi Blowfish yang menggunakan blok cipher 64-bit dengan panjang kunci variabel. Proses enkripsi pada penelitian ini merupakan proses memberikan kunci rahasia pada surat tersebut agar surat tersebut berubah menjadi tulisan sandi yang tidak dapat dipahami oleh pihak yang tidak berwenang. Proses deskripsi merupakan proses menterjemahkan kembali surat yang telah terahasia agar pihak sekolah dapat membaca surat yang dimaksud. Dari hasil pengujian sistem informasi, sistem informasi manajemen surat dapat menerapkan Algoritma Blowfish dengan baik, hal ini ditandai dengan adanya perubahan nomor surat, tanggal pengiriman surat serta tujuan pengiriman surat pada saat proses enkripsi maupun pada saat proses dekripsi.

Kata Kunci : Keamanan Data, Surat, Blowfish, Sistem Informasi

Abstract

The rapid development of information technology today requires us to be able to follow its development. Digital communication in the modern era can be a threat to eavesdropping, misuse of information, and theft of important data that is not wanted by unauthorized parties. Especially if the information is confidential and has a wide scope in the state. Therefore, the security of data storage becomes very important. The data contained in incoming and outgoing letters in one school also has confidentiality that must be maintained, where the letter is sent and where the letter comes from is also one of the things that needs to be kept confidential. On

this basis, the researcher wants to build a mail management information system that focuses on storing mail data or mail databases. Of the various encoding methods that exist to date, one of them is the Blowfish Cryptography method which uses a 64-bit block cipher with a variable key length. The encryption process in this study is the process of giving the secret key to the letter so that the letter turns into a cipher that cannot be understood by unauthorized parties. The description process is the process of translating a letter that has been kept secret so that the school can read the letter in question. From the results of testing the information system, the mail management information system can apply the Blowfish Algorithm well, this is indicated by changes in the letter number, the date of sending the letter and the purpose of sending the letter during the encryption process and during the decryption process.

Keywords: Data Security, Letters, Blowfish, Information Systems

1. Pendahuluan

Perkembangan teknologi semakin pesat dan cepat berkembang. Teknologi diciptakan untuk mempermudah pekerjaan di berbagai aspek kehidupan, baik untuk kebutuhan operasional, manajemen, maupun pengambilan keputusan. Teknologi sangat mendukung proses komunikasi antar satu dengan lainnya, namun teknologi tidak selalu digunakan dengan tepat, adakalanya teknologi juga sering disalahgunakan untuk kepentingan oknum-oknum tertentu.

Algoritma *Blowfish* merupakan salah satu penerapan bidang ilmu teknik informatika kususnya Kriptografi (Maradona & Basorudin, 2017). Metode ini dikenalkan oleh seorang peneliti bernama Bruce Schneier. Algoritma *Blowfish* merupakan salah satu algoritma yang digunakan untuk proses enkripsi tanpa merubah kunci (Simanullang & Silalah, 2018).

Pada penelitian ini, peneliti akan melakukan penelitian tentang keamanan data surat, yang nantinya akan diimplementasikan dalam bentuk sistem informasi manajemen surat, kususnya dalam pengarsipan surat atau database surat (Farell, Saputra, & Novid, 2018).

Pada penelitian ini, peneliti akan melakukan penelitian tentang keamanan data surat, yang nantinya akan diimplementasikan dalam bentuk sistem informasi manajemen surat, kususnya dalam pengarsipan surat atau database surat (Faisal & Khairina, 2020) (Farell, Saputra, & Novid, 2018). Peneliti akan menerapkan pengamanan data surat ini pada SMK Negeri 1 Percut Sei Tuan karena data surat masuk dan data surat keluar yang terdapat di sekolah merupakan data yang bersifat rahasia. Hal ini juga bertujuan untuk memberikan batasan terhadap hak akses orang lain yang tidak berwenang terhadap sistem tersebut.

2. Tinjauan Pustaka

2.1 Surat

Surat merupakan alat komunikasi yang dilakukan secara tertulis, komunikasi ini berasal dari salah satu pihak ke pihak lain dengan tujuan tertentu (Marthasari, Risqiwati, & Wibowo, 2016). Surat merupakan pernyataan tertulis dari satu pihak ke pihak yang lain, atas nama perseorangan maupun atas nama jabatan. Sedangkan menurut yaitu satu kertas ataupun lebih yang dipergunakan sebagai alat komunikasi dengan tertulis.

Berdasarkan beberapa pendapat diatas sehngga dapat ditarik kesimpulan arti surat adalah wahana/srana komunikasi tertulis yang diberikan kepada orang lain maupun suatu instansi yang memiliki tujuan agar menyampaikan suatu informasi, perintah maupun sebuah pemberitahuan.

2.2 Arsip

Arsip merupakan salah satu kegiatan untuk mengumpulkan data dan informasi yang berbentuk surat atau dokumen tertentu (Santi & Tongkuru, 2020). Arsip sangat penting dalam setiap lembaga/organisasi dalam menjalankan kegiatan administrasi. Arsip akan disimpan dalam waktu yang lama dan tercatat dengan rapi dan baik. Arsip sangat berguna apabila suatu lembaga/organisasi ingin melakukan perencanaan dalam beberapa waktu kedepan, analisa terhadap sebuah permasalahan, pengambilan keputusan terhadap hasil analisis permasalahan, dan sebagainya (Wedyawati, Elmawati, & Akhir, 2018).

2.3 Algoritma *Blowfish*

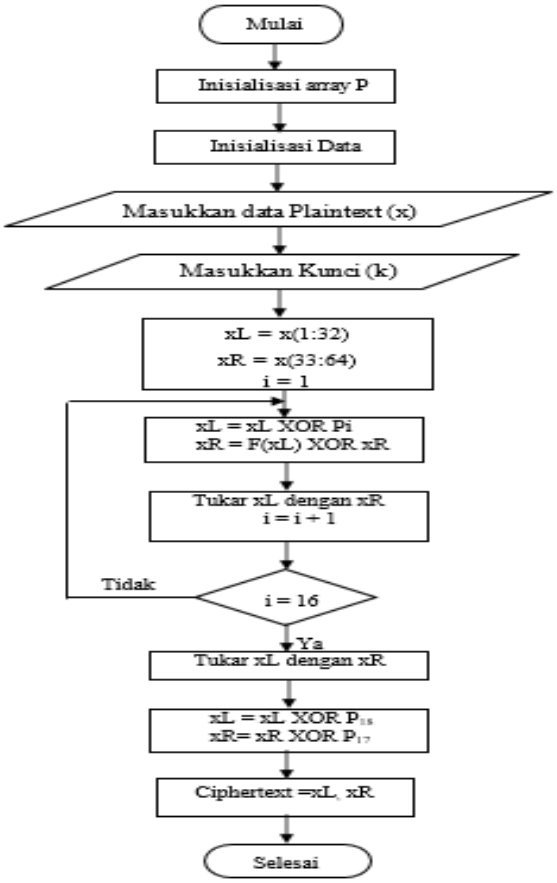
Algoritma *Blowfish* merupakan salah satu algoritma kriptografi kunci simetris (Almuwaffaq, Hadiana, & Sabrina, 2022). Algoritma *Blowfish* memiliki keunikan yang terletak pada panjang blok nya yang mencapai 64 bit (Mujito & Susilo, 2016). Berikut proses enkripsi algoritma *Blowfish* (Meko, 2018) (Suhandinata, Rizal, Wijaya, Warren, & Srinjiwi, 2019):

1. P-array diinisialisasi sebanyak 18 buah
2. S-box diinisialisasi sebanyak 4 buah, dimana masing-masing bernilai 32 bit yang memiliki masukan 255.
3. Ambil *Plaintext* sebanyak 64 bit
4. *Plaintext* yang terdiri dari 64 bit selanjutnya dibagi 2, 32 bit pertama dimasukkan ke XL, dan 32 bit yang kedua dimasukkan ke XR.
5. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR
6. Dari hasil tahap 6, tukar XL menjadi XR dan tukar XR menjadi XL.

7. Lakukan proses tahap 6 sebanyak 16 kali
8. Setelah proses yang ke 16, pada proses ke 17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
9. Proses terakhir, satukan hasil XL dan XR sehingga menjadi 64bit kembali.

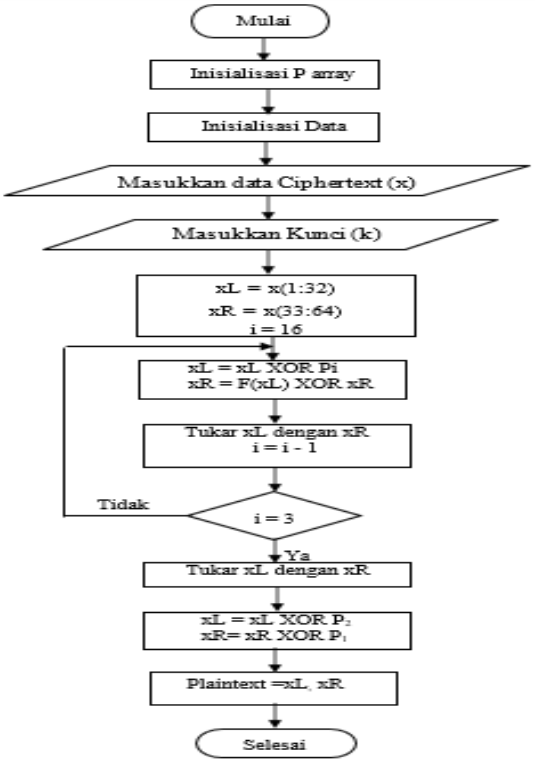
3. METODE PENELITIAN

Adapun *flowchart* proses Enkripsi algoritma *Blowfish* adalah seperti pada Gambar 1 berikut ini :



Gambar 1. *Flowchart* Proses Enkripsi

Adapun *flowchart* proses Dekripsi algoritma *Blowfish* adalah seperti pada Gambar 2 berikut ini :



Gambar 2. *Flowchart* Proses Dekripsi

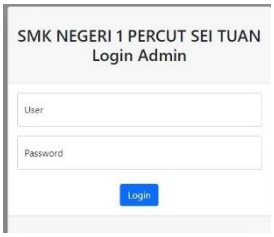
4. HASIL DAN PEMBAHASAN

4.1 Tampilan Hasil

Pada bab ini peneliti akan menjelaskan dan menampilkan poin hasil dan uji coba dari aplikasi enkrpsi dan dekripsi yang tersedia pada aplikasi yang telah dibangun.

1. Form *Login*

Pada halaman *login* terdapat halaman awal sistem informasi manajemen surat di sekolah, pada halaman ini terdapat tiga tombol yaitu *user, password* dan *login*. Dimana jika admin ingin *login* ke sistem maka admin akan memasukkan *user* dan *password* yang dimana *user* dan *password* tersebut merupakan data yang rahasia untuk dapat menggunakan sistem, setelah memasukkan *user* dan *password* klik tombol *login* maka admin akan masuk ke menu selanjutnya atau menu utama (*Dashboard*).



Gambar 3. Login Admin

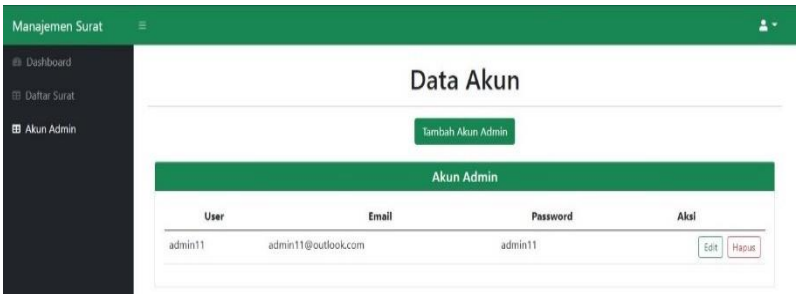
2. Form Dashboard

Pada halaman menu utama (*Dashboard*) tampilan awal dari aplikasi yang menunjukan data surat serta akun admin yang terdaftar pada aplikasi dimana jika kita menekan salah satu menu maka akan tampil menu yang terkait pada sistem yang di bangun.

Gambar 4. Form Dashboard

3. Form Data Akun

Pada halaman ini berisi tentang data akun yang digunakan admin seperti *user*, *email,* dan *password* yang di simpan ke *database*. Kita juga dapat menghapus akun yang lama jika sudah tidak digunakan lagi.



Gambar 5. Data akun

4. Form Tambah Akun

Pada halaman ini terdapat halaman tambah akun admin dimana jika kita ingin menambahkan akun admin maka akan memasukkan *user, email,* dan *password* lalu klik tombol simpan, maka akun yang di tambahkan akan tersimpan ke *database*. Jika tidak jadi menambahkan akun admin mak klik tombol batal.

Gambar 6. Tambah akun

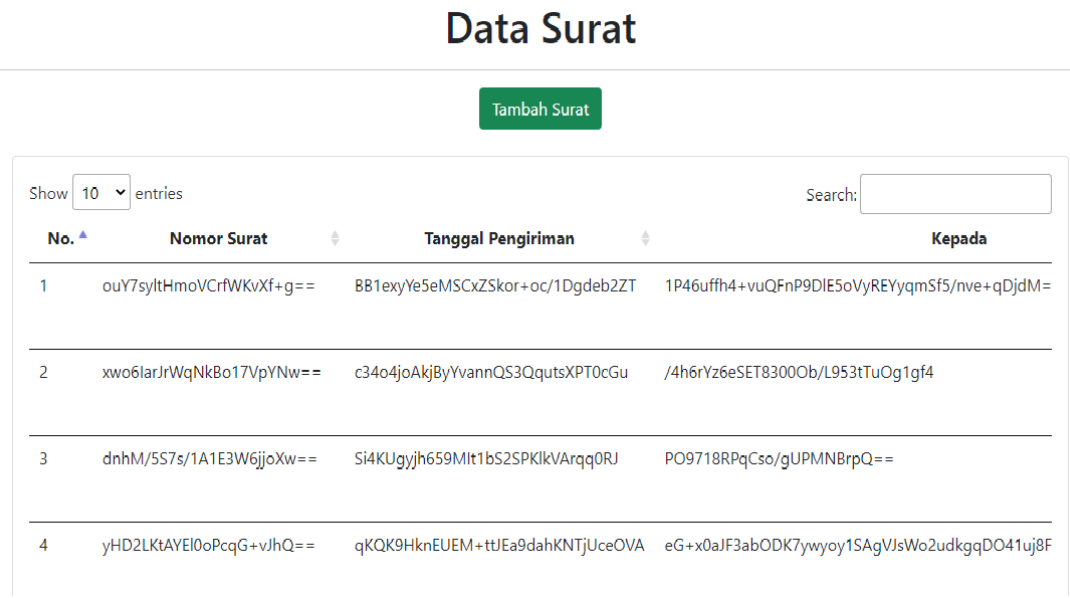
5. Form Tambah Surat

Pada halaman ini terdapat halaman tambah surat yang berisi menu kunci surat, nomor surat, tanggal pengiriman, dikirim kepada, isi pokok surat, hubungan dengan surat lain, dan simpan. Dimana jika kita ingin menambahkan surat maka kita kan mengisi semua menu yang ada pada system dan klik tombol simpan maka surat yang di tambhakan akan tersimpan dan terenkripsi di sistem dan di *database*.

Gambar 7. Form Tambah Surat

6. Form Data Surat Enkripsi

Pada halaman ini terdapat data surat-surat yang sudah terenkripsi dimana surat yang di simpan ke sistem sudah tidak dapat di baca lagi oleh siapa pun selain admin.



Data Surat

Tambah Surat

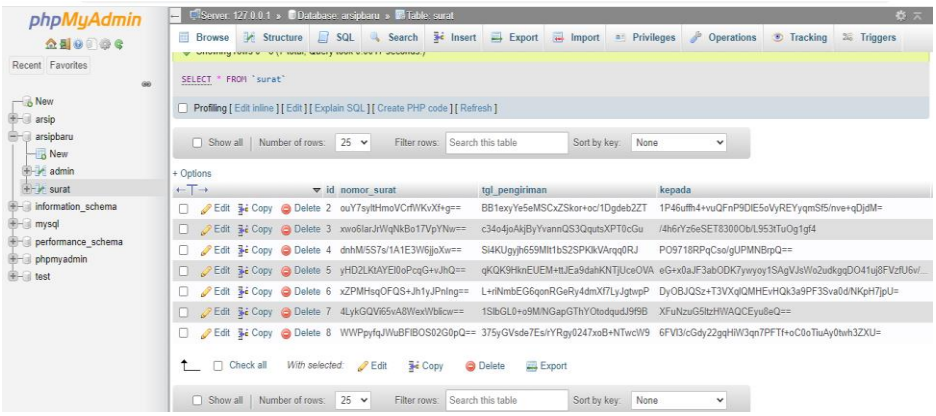
Show 10 entries Search:

No.	Nomor Surat	Tanggal Pengiriman	Kepada
1	ouY7syltHmoVCrfWKvXf+g==	BB1exyYe5eMSCxZSkor+oc/1Dgdeb2ZT	1P46uffh4+vuQFnP9DlE5oVyREYyqmSf5/nve+qDjdM=
2	xwo6larJrWqNkBo17VpYNw==	c34o4joAkjByYvannQS3QqutsXPT0cGu	/4h6rYz6eSET8300Ob/L953tTuOg1gf4
3	dnhM/5S7s/1A1E3W6jjoXw==	Si4KUgyjh659MIt1bS2SPKlkVArqq0RJ	PO9718RPqCso/gUPMNBrpQ==
4	yHD2LKtAYEl0oPcqG+vJhQ==	qKQK9HknEUEM+ttJEa9dahKNTjUceOVA	eG+x0aJF3abODK7ywyoy1SAgVJsWo2udkgqDO41uj8F

Gambar 8. Data Surat Enkripsi

7. Form Enkripsi Database

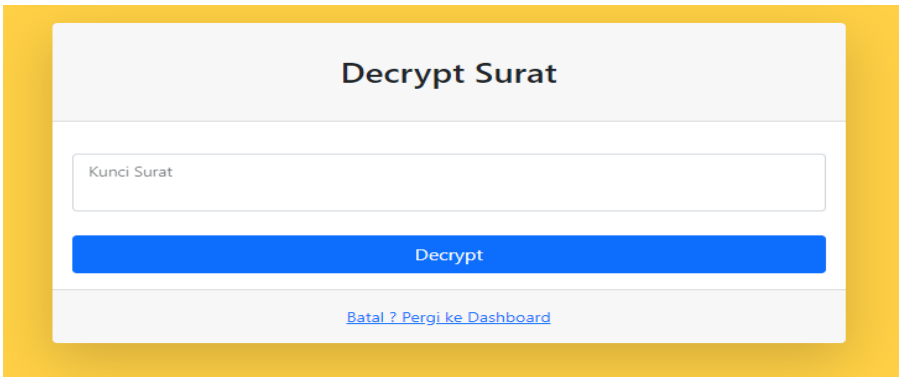
Pada halaman ini terdapat tampilan hasil enkripsi data surat yang ada pada database sistem.



Gambar 9. Hasil Enkripsi Database

8. Form Dekrispsi Surat

Pada halaman ini adalah proses dekripsi surat yang dimana admin akan memasukkan kunci surat dari setiap surat yang akan di dekripsi.



Gambar 10. Dekripsi Surat

9. Form Data Surat Hasil Enkripsi

Pada halaman ini adalah hasil data –data surat yang sudah di dekripsi oleh admin menggunakan kunci yang sama pada saat pengenkripsian surat. Pada halaman ini surat sudah dapat di baca.

Gambar 11. Data Surat Hasil Dekripsi

5. KESIMPULAN DAN SARAN

A. Kesimpulan

Penelitian yang berfokus pada pengamanan data surat ini memiliki dua proses yaitu proses enkripsi dan proses dekripsi. Proses enkripsi menambahkan surat ke dalam sistem informasi manajemen surat dan merubah isi surat menjadi kata-kata sandi sesuai dengan aturan yang ada pada Algoritma *Blowfish*. Hasil enkripsi ditandai dengan perubahan nomor surat, tanggal pengiriman dan tujuan pengiriman surat yang berupa kata sandi yang tidak dapat dimengerti. Proses selanjutnya adalah proses dekripsi, pada tahapan ini, surat yang telah dirahasiakan akan diubah kembali menjadi surat yang dapat dibaca dan dipahami. Hasil dekripsi ditandi dengan prubahan nomor surat, tanggal pengiriman dan tujuan pengiriman surat yang berupa kata sandi yang tidak dapat dimengerti menjadi tulisan normal yang dapat dipahami.

B. Saran

Adapun saran untuk pengembangan penelitian ini adalah dengan melakukan penelitian lanjutan menggunakan algoritma kriptografi lainnya yang sejenis dengan algoritma *Blowfish* dan juga melakukan modifikasi terhadap tabel kebenaran XOR.

DAFTAR PUSTAKA

Almuwaffaq, M. H., Hadiana, A. I., & Sabrina, P. N. (2022). Data Encryption Pada File Video Menggunakan Algoritma Blowfish Berbasis Android. *Informatics and Digital Expert (INDEX)* , 33-39.

Farell, G., Saputra, H. K., & Novid, I. (2018). Rancang Bangun Sistem Informasi Pengarsipan Surat Menyusur (Studi Kasus Fakultas Teknik UNP) . *Jurnal Teknologi Informasi dan Pendidikan* , 55-62.

Faisal, A., & Khairina, N. (2020). Sistem Informasi Administrasi Surat Masuk Dan Surat Keluar Pada Dinas Pendidikan Kota Medan. REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer, 267-275.

Maradona, H., & Basorudin. (2017). Analisis Algoritma Blowfish Pada Proses Enkripsi Dan Dekripsi File . *Riau Journal Of Computer Science* , 156-168.

Marthasari, G. I., Risqiwati, D., & Wibowo, H. (2016). Aplikasi Berbasis Web untuk Mempermudah Pengarsipan Surat. *Seminar Nasional Teknologi dan Rekayasa (SENTRA)* , (pp. 57-60).

Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data . *Jurnal Teknologi Terpadu* , 8-15.

Mujito, M., & Susilo, A. B. (2016). Aplikasi Kriptografi File Menggunakan Metode Blowfish dan Metode Base64 pada Dinas Kependudukan dan Pencatatan Sipil Kota Tangerang Selatan . *Jurnal SISFOKOM*, 54-60.

Santi, D., & Tongkuru, M. K. (2020). Sistem Informasi Pengarsipan Surat- Surat pada PT Sinergi Perkebunan Nusantara. *Jurnal Ilmiah Intech : Information Technology Journal of UMUS* , 51-60.

Simanullang, H. G., & Silalah, A. P. (2018). Algorithmv Blowfish untuk Meningkatkan Keamanan Database MYSQL. *Harlen Gilbert Simanullang; Arina Prima Silalah*, 10-14.

Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA . *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)* , 1-10.

Wedyawati, V., Elmawati, & Akhir, K. I. (2018). Perancangan Aplikasi Pengarsipan Surat Program Studi Sistem Informasi pada Sekolah Tinggi Teknologi Industri Padang Menggunakan VB NET 2010 . *Jurnal Sains dan Teknologi*, 1-9.