Implementasi Kriptografi untuk Keamanan Data dan Jaringan menggunakan Algoritma DES

Annisa Thahara*[1], Ina Tia Siregar[2]
[1,2] Teknik Informatika STIKOM,Pematang Siantar.
e-mail: *[1]**annisathahara80@gmail.com,** [2]inatiasiregar012@gmail.com

Abstrak

Komputer semakin hari semakin berkembang dan dizaman 4.0 ini komputer mulai digandrungi oleh masyarakat milenial untuk membantu dalam proses berkerja maupun belajar dengan komputer membuat perkerjaan lebih mudah. Umumnya komputer sangat diminati oleh masyarakat melenial, semua aktivitas baik sekolah, belajar maupun berkerja dapat dilakukan dengan mudah oleh komputer. Namun dibalik kecanggihan dan banyak lagi kelebihan komputer baik dalam menyimpan data. Kita juga harus dapat merawat komputer dan menjaga keamanan komputer terutama data, karena ditangan orang yang tidak baik data yang ada didalam komputer kita dapat dicuri selain itu data yang ada didalam komputer kita juga dapat mengalami kerusakan baik dari virus ataupun dari orang yang tidak berniat baik contohnya seperti hacker. Namun adapun salah satu cara untuk meningkatkan atau menjaga keamanan komputer yang kita miliki terutama keamanan data dengan menerapkan kriptografi dengan mengunakan Algoritma DES dalam menjaga data atau dapat meningkatan pengamanan data kita yang ada didalam komputer. Diharapkan dengan kita mengetahui cara dalam mengimplementasikan kriptografi dengan menggunakan algoritma DES dalam keamanan data dapat meningkatan atau menjaga agar data kita yang ada dikomputer agar tetap aman dan tidak dicuri atau mengalami gangguan baik dari virus maupun hacker.

Kata kunci*— Keamanan komputer, Kriptografi, Serangan keamanan, Algoritma DES.*

1. PENDAHULUAN

Zaman indrustri 4.0 ini merupakan zaman dimana terjadinya perkembangan teknologi dan informasi yang sangat cepat dan pesat. Dimana perkembangan tersebut dapat dipanggaruhi oleh globalisasai ,seiring perkembangan zaman dari tahun ke tahun teknologi makin hari makin berkembang salah satunya adalah komputer. Komputer adalah sebuah alat yang dapat membantu dan memudahkan manusia dalam mengelolah data menurut prosedur yang telah dirumuskan. komputer juga dapat digunakan bagi semua kalangan baik muda maupun tua yang memahami teknologi yang satu ini [1].

Namun dibalik dari kelebihan komputer ini komputer juga memiliki kekurangan salah satunya dalam hal masalah keamanan komputer. Keamanan komputer merupakan salah satu bagian yang penting dari sebuah sistem informasi namun tak jarang keamanan dari sebuah komputer dapat diserang atau mengalami ancaman yang mengakibatkan misalnya menjadikan data - data penting yang ada di si pengguna komputer sendiri menjadi rusak atau dicuri dan membuat pengguna mengalami kerugian [2].

Serangan keamanan pada komputer dapat terjadi dari berbagai sumber, Contohnya seperti adanya kerusakan yang disebabkan oleh virus komputer yang dapat merusak data atau adanya orang yang berniat kurang baik namun memahami kecangihan komputer sehingga dapat mencuri data yang ada di komputer anda salah satunya adalah yang dilakukan oleh seorang hacker .seorang hacker dapat mencuri sebuah data yang dibutuhkannya. Tentu hal ini sangat tidak menguntungkan bagi penguna apalagi bagi pengguna yang menggunakan komputer untuk membantunnya dalam urusan mengenai data perusahan yang disimpan didalam komputer.

Namun sekarang user janganlah terlalu risau ada beberapa cara yang dapat digunakan oleh user agar komputernya aman dari pencurian data atau kerusakan yang mengakibatkan data

yang ada dikomputer salah satunya dengan metode menerapkan kriptografi mengunakan algoritma DES dalam usaha meningkatkan keamanan data pada komputer [3]. Penulisan ini dilakukan agar masyarakat atau cara mengimplementasikan kriptografi menggunakan algoritma DES dalam meningkatkan kemanan komputer terkususnya data.

2. METODE PENELITIAN

Pada penelitan kali ini saya akan menggunakan metode implimentasikan kriptorafi menggunakan metode algoritma DES dalam keamanan data komputer. Implementasi menurut KBBI memiliki arti pelaksanaan atau penerapan, oleh karena itu pada materi penelitian kali ini saya akan menulis tentang cara penerapan algoritma des dalam keamanan data dan jaringan.

3. HASIL DAN PEMBAHASAN

3.1. Keamanan Komputer

Dengan perkembanganan sistem informasi yang pesat dan kecanggihan teknologi yang ada sangat membantu dan memberikan dampak positif juga bagi masyakat karena dapat memudahkan perkerjaan si pengguna namun dibalik dampak positif dari kecangihan teknologi dan berkembangnya sistem informasi perlunyaadanya upaya meningkatkan keamanan komputer misalnya sebagai contoh dari perkembangan teknologi. Meski banyak dampak postif yang dirasakan masyarakat dari perkembangan teknologi tidak dapat di pungkirin bahwa juga mengakibatkan dampak yang negatif salah satunya adalah adanya pencurian data yang ada di komputer anda atau adanya penipuan–penipuan yang berbasis komputer oleh sebab itu kita harus meningkatkan lagi keamanan komputer agar data yang ada dikomputer kita tidak dapat di curi atau rusak [4].

Salah satu cara untuk meningkatkan keamanan komputer adalah dengan cara mengunakan metode mengimplementasikan kriptografi dengan mengunakan algoritma DES agar data pada komputer kita dapat aman khususnya dari hal–hal yang dapat mengancam keamanan komputer.

3.2. Serangan Keamanan Jaringan

Sistem keamanan jaringan yang biasanya digunakan pada jaringan publik secara umum sangat mudah terkena serangan oleh siapapun termasuk orang yang suka menyerang jaringan disebut penyerang. Seorang penyerang biasanya menyerang sistem keamanan jaringan bertujuan untuk mengalahkan tujuan layanan keamanan jaringan [5]. Misalnya menyerang kerahasianaan data. Secara umum serangan pada sistem keamanan jaringan dibagi menjadi 2 jenis yaitu :

3.2.1. Passive attack

Merupakan serangan yang terjadi pada data yang melintas pada jaringan yang bisa diakses oleh penyerang. Berikut adalah beberapa jenis serangan yang digolongan sebagai serangan pasif, Snooping merujuk pada kegiatan yang bermaksud mendapatkan data yang terkirim pada jaringan biasanya melalui akses yang tidak berwewenang. contohnya adalah saat sebuah e–mail disadap oleh penyerang. Sehingga data yang terkirim dibuat tidak tampak mata oleh penyerang kagiatan tersebut aktivitas snooping.

Traffic analysis adalah serangan dimana penyerang melakukan monitoring terhadap lalu lintas data pada jaringan. Data–data lalu lintas jaringan dikumpulkan dan kemudian dianalisis oleh penyerang agar penyerang dapat mengetahui maksud dari data–data tersebut.

3.2.2. Active attack

Active attack merupakan serangan yang menyebabkan perubahan data yang terkirim dan jalannya sistem terganggu. Jenis–jenis serangan active antara lain, masquerade merupakan serangan aktif yang dilakukan oleh penyerang dengan cara mengambil alih (menirukan) perilaku pengirim atau penerima. Modification merupakan serangan aktif yang dilakukan penyerang dengan cara penyerang mengambil alih jalur komunikasi untuk mengubah atau menghapus atau menunda pesan yang sendang terkirim untuk keuntungan penyerang. Replay merupakn penyerangan atas pencatatan secara pasif data unit dan tarnmisi ulang untuk menimbulkan efek yang diinginkan penyerang. Denial of service merupakan serangan yang memiliki tujuan agar sistem menjadi collapse sehingga tidak dapat memberikan respon dan layanan yang semestinya di berikan ke pengguna.

3.3. Kriptografi

Kriptografi adalah suatu cara bagi seseorang agar dapat mengirim pesan rahasia ke pada orang lain atau bisa dibilang si penerima pesannya dengan cara menggunakan sistem kode agar tidak dapat di mengerti oleh orang ketiga atau orang yang berniat tidak baik seperti hacker misalnya walaupun pihak ketiga itu sendiri dapat menginterupsi tranmisi dari sistem mengirim pesan. Alangkah baiknya jika pesan tersebut tidak jatuh kepihak ketiga sebelum terjadinya tranmisi agar bisa dapat dicegah untuk mengira–ngira pesan tersebut, oleh karena itu dibutuhkannya adanya algoritma. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan [6].

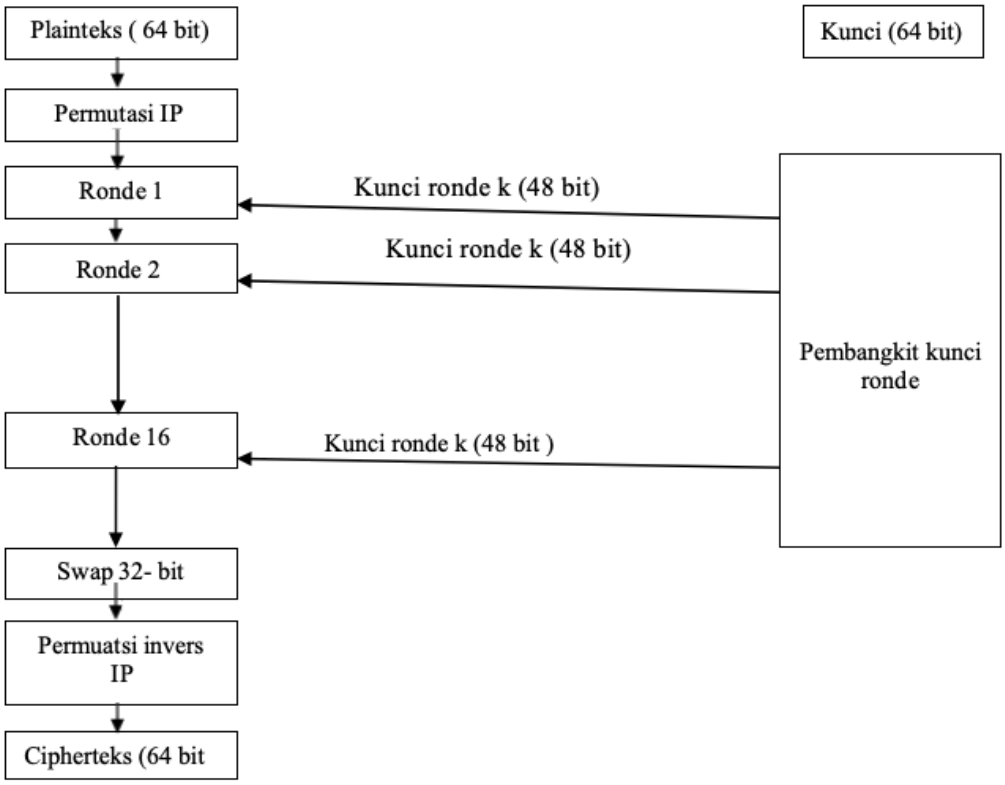
3.4. Algoritma Des

Algoritma DES termasuk kedalam sistem kriptografi simetri yang termasuk dalam blok code.algoritma DES merupakan termasuk kedalam algoritma chiper blok yang lumayan sangat populer karena dijadikan standar algoritma kunci simetri walaupun sekarang telah diganti oleh algoritma baru karean des sudah mulai dianggap tidak aman lagi [7]. DES berkerja pada blok 64 bit. DES mengenkripsikan 64 bit teks asli menjadi 64 teks kode dengan menggunakan 56 bit kunci internal atau subkey [8]. Algoritma DES merupakan standar sandi blok dengan kunci simetri yang cukup tua, namun walaupun sudah lama, DES masih digunakan karena cepat dan cukup aman walaupun ada beberapa DES yang tidak cukup aman untuk beberapa jarigan [9].

DES adalah algoritma block cipher yang populer meskipun telah digantikan menjadi AES, algoritma DES memiliki kelebihan dimana algoritma ini lebih baik dibandingkan algoritma XOR yang lain [10]. Algoritma DES tidak digunakan lagi karena dengan serangan brute force pada sistem parallel computing telah berhasil memecahkan algoritma ini dengan mudah [11].

3.4.1 Struktur DES

DES merupakan salah satu sandi Feistel , sehingga struktur sandinya sama dengan sandi feistel dengan penghususan : panjang blok DES adalah 64 bit, ukuran teks sandi dan tek asli sama 64 bit ,ukuran kunci DES dalah 64 bit dan ukuran kunci ronde adalah 48 bit dan jumlah ronde yang dimiliki adalah 16 ronde.



Gambar 1. Struktur Sistem sandi DES

Pada gambar diatas merupakan proses teks asli berukuran 64 bit melalui 3 tahapan yaitu :tahapan pertama adalah painteks dikenakan book permutasi IP sebesar 64 bit, setelah itu tahap kedua terdiri 16 ronde percampuran kunci ronde dan hasil sementara pada fungsi sandi produk .pada akhirnya 16 ronde keluar di swap dan pada tahap terakhir dikenakan boks permutasi invers (kebalikan boks permutasi IP) untuk menghasilkan 64 bit teks sandi.

3.5. Cara Kerja Algoritma Des

Skema global algoritma DES adalah sebagai berikut :

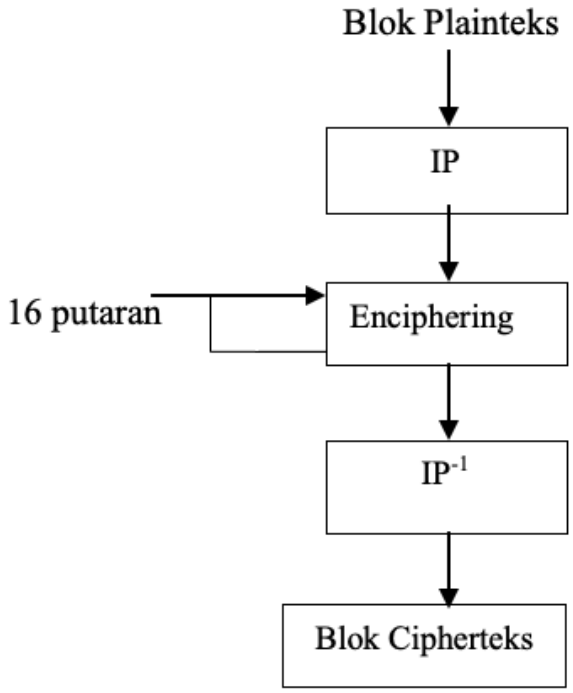
1) Blok plainteks dipermutasi dengan matriks permutasi awal, Contoh tahapan plainteks dipermutasi dengan matriks permutasi awal :

a) Contoh plaintext :annisaceam
binary
: 01100010011000010111100101110101011000110110000101100101011011 01

b) Setelah itu binary-nya diacak oleh matriks IP setelah itu binary dibagi 64 bit maka dipermutasi dengan matiks IP setelah tahap permutasi selesai dilakukan maka sekarang menuju ke tahap enchipering. Butuh yang namanya kunci eksternal yang akan membentuk kunci internal. jadi gambarannya sang user jika ingin mengenkripsi maka ada dua yang harus diinputkan yaitu plaintextnya dan kuncinya sepanjang 16 digit hexadesimal. kunci ini juga (selanjutnya disebut kunci eksternal) akan digunakan pada saat mendekripsi DES.

2) Hasil permutasi awal kemudian di enciphering – sebanyak 16 putaran .setiap putaran menggunakan kunci internal yang berbeda.

3) Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP -1) menjadi blok cipherteks.

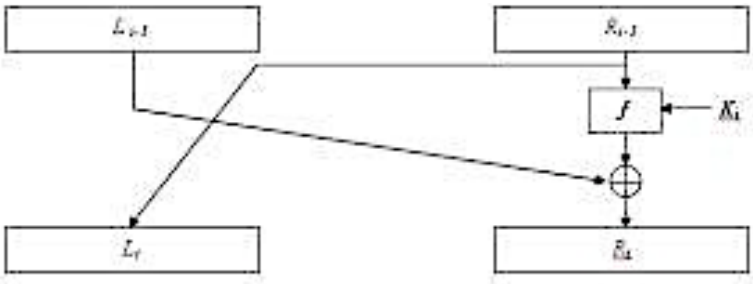


Gambar 2. Skema global algoritma des

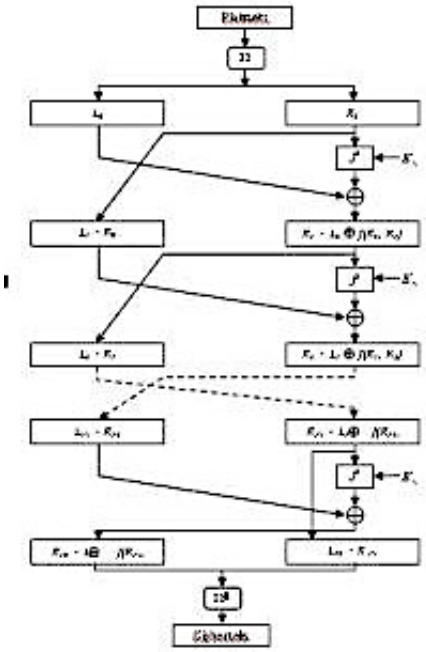
Di dalam proses enciphering, blok plainteks terbagi menjadi dua bagian, kiri (L) dan kanan R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang disebut f. Pada fungsi f, blok R di kombinasikan dengan yang namanya kunci internal.

Li=Ri-1 (6.1)
R i=L i-1 f(Ri-1, K i) (6.2)

Gambar 3 memperlihatkan skema algoritma DES yang lebih rinci. Satu putaran DES merupakan model jaringan Feistel (lihat Gambar 6.2). Perlu dicatat dari Gambar 6.2 bahwa ika (L,6, R,6) merupakan keluaran dari putaran ke-16, maka (R,6, L,s) merupakan pra:ipherteks (pre-ciphertext) dari enciphering ini. Cipherteks yang sebenarnya diperoleh dengan melakukan permutasi awal balikan, IP-1, terhadap blok pra-cipherteks.



Gambar 3. Jaringan Feistel untuk satu putaran DES



Gambar 4 Algoritma Enkripsi dengan DES Permutasi Awal

Sebelum putaran pertama, terhadap blok plainteks dilakukan permutasi awal (initial-permutation atau IP). Tujuan permutasi awal adalah mengacak plainteks sehingga urutan bit-bit di dalamnya berubah. Pengacakan dilakukan dengan menggunakan matriks permutasi awal berikut ini:

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Gambar 5. Matriks Permutasi Awal

Cara membaca tabel/matriks: dua entry ujung kiri atas (58 dan 50) artinya: "pindahkan bit ke-58 ke posisi bit 1"

"pindahkan bit ke-50 ke posisi bit 2", dan seterusnya

Pembangkitan Kunci Internal

Ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K,, Kz, ...,K16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter.

Misalkan kunci eksternal yang tersusun dari 64 bit adalah K. Kunci eksternal ini menjadi masukan untuk permutasi dengan menggunakan matriks permutasi kompresi PC- 1 sebagai berikut:

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Gambar 6. Matriks Permutasi kompresi PC-1

Dalam permutasi ini, tiap bit kedelapan (parity bit) dari delapan byte kunci diabaikan. Hasil 7-permutasinya adalah sepanjang 56 bit, sehingga dapat dikatakan panjang kunci DES adalah 56 bit. Selanjutnya, 56 bit ini dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing nanjangnya 28 bit, yang masing-masing disimpan di dalam Co dan DO:

CO: berisi bit-bit dari K pada posisi
57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18
10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36

Do: berisi bit-bit dari K pada posisi
63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22
14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4

Selanjutnya, kedua bagian digeser ke kiri (left shift) sepanjang satu atau dua bit bergantung pada tiap putaran.

4. KESIMPULAN

Dari hasil penelitian mengemukakan bahwa algoritma DES dapat menjaga keamanan data maupun jaringan dengan melewati beberapa tahap dalam proses kerjanya baru bisa membuat data anda aman dari penyerang dengan mengubah blok teks ke blok sandi sebelum dibaca oleh penerima. Penerima harus membaca dan mengubah kembali dari blok sandi ke blok teks menggunakan aplikasi tertentu.

DAFTAR PUSTAKA

[1] M. B. Firdaus, E. Budiman, Haviluddin, M. Wati, H. J. Setyadi, and H. S. Pakpahan, "An openness of government website content using text analysis method," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 5, pp. 1461–1466, 2019, doi: 10.35940/ijeat.E1214.0585C19.

[2] M. S. Rahmawati and R. Soekarta, "Teori Grup Pada Algoritma DES Dan Transformasi Wavelet Diskrit Dalam Program Aplikasi Keamanan Citra Digital," *Insect (Informatics …*, vol. 4, no. 1, 2019, [Online]. Available: http://ejournal.um-sorong.ac.id/index.php/insect/article/view/281.

[3] G. Putrodjojo, J. H. Purba, and J. Candra, "Aplikasi Algoritma Des (Data Encryption Standard) Untuk Pengaman Data," *CCIT J.*, vol. 10, no. 1, pp. 62–74, 2017, doi: 10.33050/ccit.v10i1.518.

[4] N. Syahputri, "Rancang Bangun Aplikasi Kriptografi Pengamanan Transmisi Data Multimedia Menggunakan Algoritma Data Encryption Standard …," *Maj. Ilm. Methoda*, vol. 9, no. 2, pp. 57–63, 2019.

[5] A. Baby and A. Kannammal, "Network Path Analysis for developing an enhanced TAM model: A user-centric e-learning perspective," *Comput. Human Behav.*, vol. 107, no. September 2018, p. 106081, 2020, doi: 10.1016/j.chb.2019.07.024.

[6] A. Priatmoko and E. Harahap, "Implementasi Algoritma DES Menggunakan MATLAB," *Matematika*, vol. 16, no. 1, pp. 11–19, 2017, doi: 10.29313/jmtm.v16i1.3360.

[7] A. Pangestu, L. Fitriani, and D. D. S. Fatimah, “Rancang Bangun Sistem Multimedia Kegiatan Keagamaan Masyarakat Indonesia Berbasis Android,” *J. Algoritm.*, vol. 17, no. 1, pp. 68–74, 2020, doi: 10.33364/algoritma/v.17-1.68.

[8] B. Fachri and R. M. Sembiring, “Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android,” *J. Media Inform. Budidarma*, vol. 4, no. 1, p. 110, 2020, doi: 10.30865/mib.v4i1.1700.

[9] A. D. Depayusa, “Perbandingan Algoritma Des Dan Algoritma Aes Pada Teknologi Qr-Code,” *SHaP SITI*, no. September, 2016.

[10] M. Satria *et al.*, “Perancangan Aplikasi Keamanan Data Dokumen Word dengan Menggunakan Algoritma Triple DES,” *J. FTIK*, vol. 1, no. 1, pp. 463–475, 2020.

[11] D. Adhar, “Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android,” *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 53–60, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/185.