Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi
Penerbit ADM RUMAH PENGETAHUAN

Network-Based Text Message Security System Using the Data Encryption Standard (DES) Algorithm

Sistem Keamanan Pesan Teks Berbasis Jaringan Menggunakan Algoritma Data Encryption Standard (DES)

Horas Aryanto Simanjuntak [1)]; Hari Aspriyono [2)]; Eko Prasetiyo Rohmawan [3)]
[1,2,3)] Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Email: [1)] Horasaryanto@gmail.com

How to Cite :
Simanjuntak, H. A., Aspriyono, H., Rohmawan, E. P. (2022). Network-Based Text Message Security System Using the Data Encryption Standard (DES) Algorithm. Jurnal Komitek, 2 (2). DOI: https://doi.org/10.53697/jkomitek.v2i2

ARTICLE HISTORY
Received [08 November 2022]
Revised [2 Desember 2022]
Accepted [09 Desember 2022]

Keywords :
Sistem Keamanan, Pesan Teks, Berbasis Jaringan, Algoritma Data Encryption Standard

ABSTRAK

UPT. Puskom sebagai pengelola praktikum memiliki tanggung jawab untuk menyediakan fasilitas termasuk aplikasi-aplikasi yang dibutuhkan setiap mata kuliah. Dalam penelitian ini dilakukan pengembangan sistem keamanan teks berbasis jaringan dengan mengimplementasikan salah satu algoritma kriptografi yang sudah dikemas ke dalam bentuk aplikasi sehingga mahasiswa dapat mengetahui proses enkripsi dan dekripsi dari algoritma Kriptografi yaitu Algoritma Data Encryption Standard (DES). Sistem keamanan pesan teks berbasis jaringan menggunakan Algoritma Data Encryption Standard (DES) dibuat menggunakan Bahasa Pemrograman Visual Basic .Net dan database SQL Server. Sistem keamanan yang dibangun dapat membantu merahasiakan pesan yang akan dikirim dari pengirim ke penerima pesan melalui algoritma DES. Proses Enkripsi dapat dilakukan oleh user yang akan mengirim pesan teks ke user yang dituju dapat membuka form enkripsi dan memilih user yang akan dituju, pesan yang telah terenkripsi akan tersimpan ke dalam database. Sedangkan dekripsi dapat dilakukan oleh user yang menerima pesan teks dengan membuka form dekripsi dan menampilkan pesan-pesan yang telah dikirim oleh pengirim pesan. Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi mampu melakukan enkripsi dan dekripsi pesan teks menggunakan algoritma DES.

ABSTRACT

UPT. Puskom as practicum manager has the responsibility to provide facilities including applications needed for each course. In this research, the development of a network-based text security system was carried out by implementing one of the cryptographic algorithms that had been packaged into an application so that students could find out the encryption and decryption processes of the Cryptographic algorithm, namely the Data Encryption Standard (DES) Algorithm. A network-based text message security system using the Data Encryption Standard (DES) Algorithm was built using the Visual Basic .Net Programming Language and SQL Server database. The security system built can help keep messages sent secret from the sender to the recipient of the message through the DES algorithm. The encryption process can be carried out by the user who will send a text message to the intended user, who can open the encryption form and select the intended user, the encrypted message will be stored in the database. Meanwhile, decryption can be done by users who receive text messages by opening the decryption form and displaying the messages sent by the message sender. Based on the tests that have been

carried out, it can be concluded that the application is capable of encrypting and decrypting text messages using the DES algorithm.

PENDAHULUAN

Dunia teknologi informasi sekarang ini berkembang sangat pesat dan mempengaruhi hampir seluruh aspek kehidupan manusia. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi semua sistem yang berhubungan ataupun tidak dengan sistem informasi itu sendiri seperti perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan.

Keamanan merupakan aspek yang sangat penting dalam proses pengiriman pesan teks yang sifatnya rahasia. Karena pesan teks sangat rentan terhadap pencurian ataupun penyadapan. Oleh karena itu, keamanan sangat penting untuk mencegah informasi tersebut sampai pada pihak-pihak lain yang tidak berkepentingan yang mengakibatkan terjadinya kebocoran atau penyalahgunaan data dan informasi.

PUSKOM Universitas Dehasen Bengkulu merupakan unit pelaksana perkuliahan komputer dan pelaksana teknis yang berfungsi di bidang teknologi pengelolaan data dan pelayanan teknologi sistem informasi pendidikan, penelitian, pengabdian kepada masyarakat serta pengolahan data kepegawaian, dan sarana/prasarana dan seluruh Manajemen Sistem Informasi Universitas.

Salah satu mata kuliah pokok pada konsentrasi jaringan pada Program Studi Informatika yaitu kriptografi. Kriptografi digunakan sebagai keamanan data untuk mencegah data tersebut dapat diakses oleh pihak-pihak lain yang tidak berkepentingan. Selama ini beberapa mahasiswa masih sulit memahami konsep dari kriptografi, hal ini dikarenakan belum tersedianya fasilitas pada praktikum di laboratorium komputer. Oleh karena itu, UPT. Puskom sebagai pengelola praktikum memiliki tanggung jawab untuk menyediakan fasilitas termasuk aplikasi-aplikasi yang dibutuhkan setiap mata kuliah. Dalam penelitian ini dilakukan pengembangan sistem keamanan teks berbasis jaringan dengan mengimplementasikan salah satu algoritma kriptografi yang sudah dikemas ke dalam bentuk aplikasi sehingga mahasiswa dapat mengetahui proses enkripsi dan dekripsi dari algoritma Kriptografi yaitu Algoritma Data Encryption Standard (DES).

Algoritma DES (Data Encryption Standard) merupakan algoritma kriptografi modern yang paling bayak digunakan di dunia yang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolahan informasi federal AS. Plain di enkrip dalam blok-blok bid menjadi 64 bit data ciphertext menggunakan kunci 56bit kunci internal. Dalam mengimplementasikan algoritma DES tersebut, maka dibangun suatu aplikasi berbasis web yang berjalan di jaringan LAN dimana memiliki database server menggunakan MySQL, sehingga proses pengiriman pesan teks dilakukan melalui interface aplikasi tersebut.

LANDASAN TEORI

Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Kriptografi menurut terminologinya adalah sebuah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara istilah kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan baik berupa data maupun informasi yang mempunyai arti atau nilai dengan cara menyamarkan (mengacak) menjadi bentuk yang tidak dapat dimengerti dan hanya penerima yang dapat mengubah kode-kode tersebut menjadi pesan asli yang dapat dimengerti (Jamaludin, 2020:7).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data dan otentikasi. Jadi dapat disimpulkan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika untuk menjaga keamanan informasi. Cara melakukan teknik ini mulainya pengirim pesan akan melakukan

penyandian pesan awal yang menjadi kode-kode yang hanya dapat dibaca oleh penerima tersebut. Selanjutnya, penerima pesan mengembalikan kode-kode yang telah diterima menjadi pesan asli dengan menggunakan kunci yang dikirimkan oleh pengirim pesan (Jamaludin, 2020:7).

Jaringan Komputer

Jaringan komputer merupakan suatu sistem yang terdiri dari komputer-komputer dan perangkat-perangkat jaringan lainnya yang terhubung satu sama lain, bekerja sama untuk mencapai suatu tujuan. Perangkat jaringan sangat penting untuk berlangsungnya hubungan atau komunikasi antar komputer. Informasi berpindah dari komputer ke komputer lainnya dengan menggunakan jaringan daripada melalui perantara manusia, sehingga membuat pertukaran informasi menjadi lebih cepat dan mudah (Simargolang, et al, 2021:1).

Sebuah jaringan komputer terdiri dari dua atau lebih perangkat komputasi yang terhubung untuk berbagi komponen dari jaringan berupa sumber daya dan informasi yang disimpan jaringan tersebut. Komputer lokal adalah komputer dekstop yang biasa digunakan, perlu terhubung ke jaringan workstation dan server sebagai tempat penyimpanan dan pengendali komputer client sehingga setiap client dapat berbagi sumber daya, informasi, komunikasi satu sama lainnya. Jika satu jaringan workstation terhubung dengan jaringan workstation jaringan lainnya akan menjadi jaringan yang lebih besar dan membutuhkan dukungan hardware yang baik untuk firewall yang lebih kuat (Hendry, 2018:26).

Algoritma DES

Algoritma DES adalah metode kunci simetris lama untuk mengenkripsi data. Algoritma DES bekerja dengan menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi pesan, sehingga pengirimdan penerima harus mengetahui dan menggunakan kunci privat yang sama (Simarmata, et al, 2021:122).

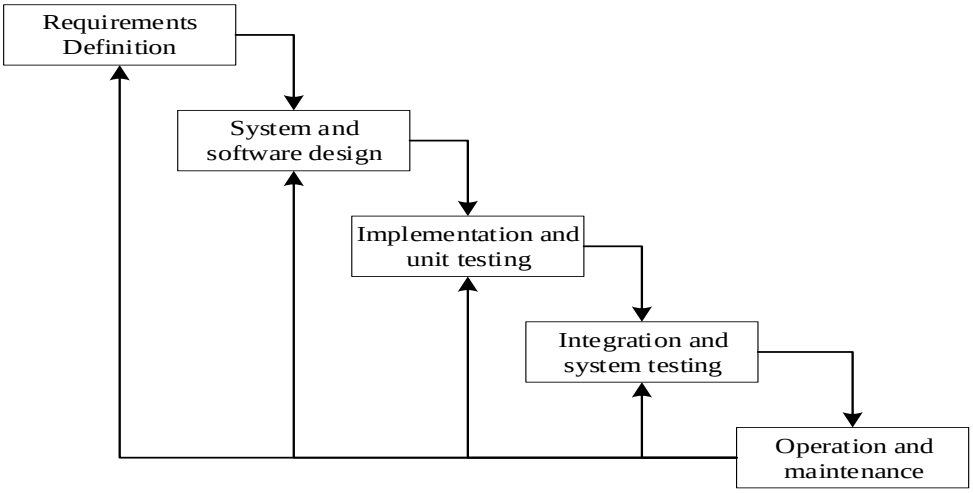
Penggunaan data sandi yang paling banyak didasarkan pada standard-standard data sandi (DES) yang diambil pada tahun 1977 oleh Standard-Standard Nasional Bureau, yang sekarang Institut Nasional Standard dan Tekhnologi (NIST), sebagai Standard Proses Informasi Umum. Untuk DES, data disandikan ke dalam 64 balok bit menggunakan 56 bit kunci. Transformasi algoritma 64 bitinput ke dalam satu serilangkah-langkah ke dalam 64 bitoutput. Langkah yang sama dengan kunci yang sama, digunakan untuk cadangan persandian (Adhar, 2019:55).

Algoritma Data Encryption Standard (DES) termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit dan mengenkripsikan 64 bit plainteks menjadi 64 bit cipher teks dengan menggunakan 56 bit kunci internal (internal key) atau up-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

METODE PENELITIAN

Metode Penelitian.

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode *waterfall*. Metode *waterfall* merupakan model pengembangan sistem informasi yang sistematik dan sekuensial. Metode *waterfall* memiliki tahapan-tahapan seperti Gambar 1.



Gambar 1. Metode Waterfall

Keterangan :

1. *Requirements analysis and definition.* Layanan sistem, kendala, dan tujuan ditetapkan oleh hasil konsultasi dengan pengguna yang kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.
2. *System and software design.* Tahapan perancangan sistem mengalokasikan kebutuhan-kebutuhan sistem baik perangkat keras maupun perangkat lunak dengan membentuk arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan penggambaran abstraksi sistem dasar perangkat lunak dan hubungannya.
3. *Implementation and unit testing.* Pada tahap ini, perancangan perangkat lunak direalisasikan sebagai serangkaian program atau unit program. Pengujian melibatkan verifikasi bahwa setiap unit memenuhi spesifikasinya.
4. *Integration and system testing.* Unit-unit individu program atau program digabung dan diuji sebagai sebuah sistem lengkap untuk memastikan apakah sesuai dengan kebutuhan perangkat lunak atau tidak. Setelah pengujian, perangkat lunak dapat dikirimkan ke *customer*
5. *Operation and maintenance.* Biasanya (walaupun tidak selalu), tahapan ini merupakan tahapan yang paling panjang. Sistem dipasang dan digunakan secara nyata. *Maintenance* melibatkan pembetulan kesalahan yang tidak ditemukan pada tahapan-tahapan sebelumnya, meningkatkan implementasi dari unit sistem, dan meningkatkan layanan sistem sebagai kebutuhan baru.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Pengujian Sistem

Adapun hasil pengujian yang telah dilakukan pada sistem keamanan pesan teks berbasis jaringan menggunakan Algoritma Data Encryption Standard (DES), seperti Tabel 1.

Tabel 1 Hasil Pengujian Sistem

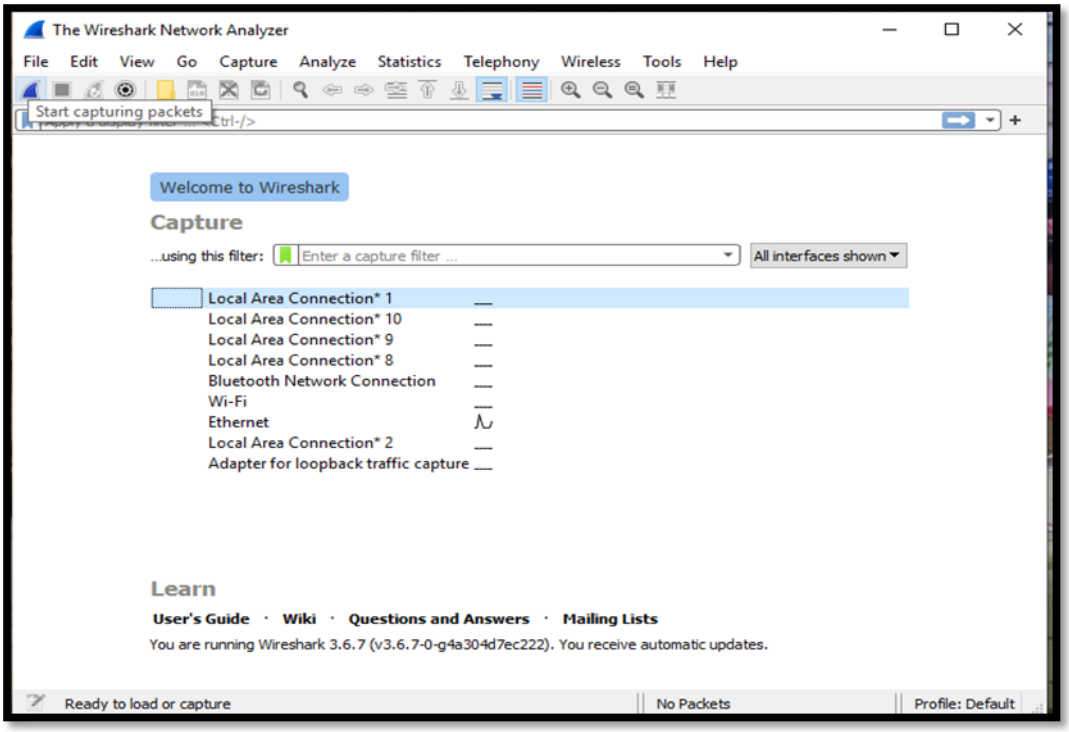
No	Komponen Pengujian	Skenario Pengujian	Hasil Pengujian
1	Menguji *Form Login*	Masukkan *username* dan *password* yang benar	Sistem berhasil menerima akses *login* dengan menampilkan pesan berhasil *login*
		Masukkan *username* atau *password* yang salah	Sistem berhasil menolak akses *login* dengan menampilkan pesan kesalahan

2	Menguji Form Kirim Pesan Teks	Mengirim pesan teks ke penerima pesan	Sistem berhasil mengirim pesan teks ke penerima pesan
3	Menguji proses enkripsi pada *form* kirim pesan teks	Melihat pesan terenkripsi yang tersimpan dalam *database*	Sistem berhasil mengacak pesan teks tersebut sehingga tidak dapat terbaca
4	Menguji *Form* Lihat Pesan Teks	melihat pesan teks terenkripsi yang telah dikirim penerima	Sistem berhasil menampilkan pesan teks terenkripsi
5	Menguji proses dekripsi pada *form* lihat pesan teks	Melakukan proses dekripsi pada pesan teks terenkripsi	Sistem berhasil menampilkan pesan teks asli
6	Pengujian *wireshark* pada proses enkripsi dan dekripsi	Melakukan *capturing* menggunakan *wireshark*	*wireshark* berhasil *capture* paket masuk dan keluar, dan terlihat bahwa *record* pada tabel dalam *database* terenkripsi

Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi mampu melakukan enkripsi dan dekripsi pesan teks menggunakan algoritma DES.

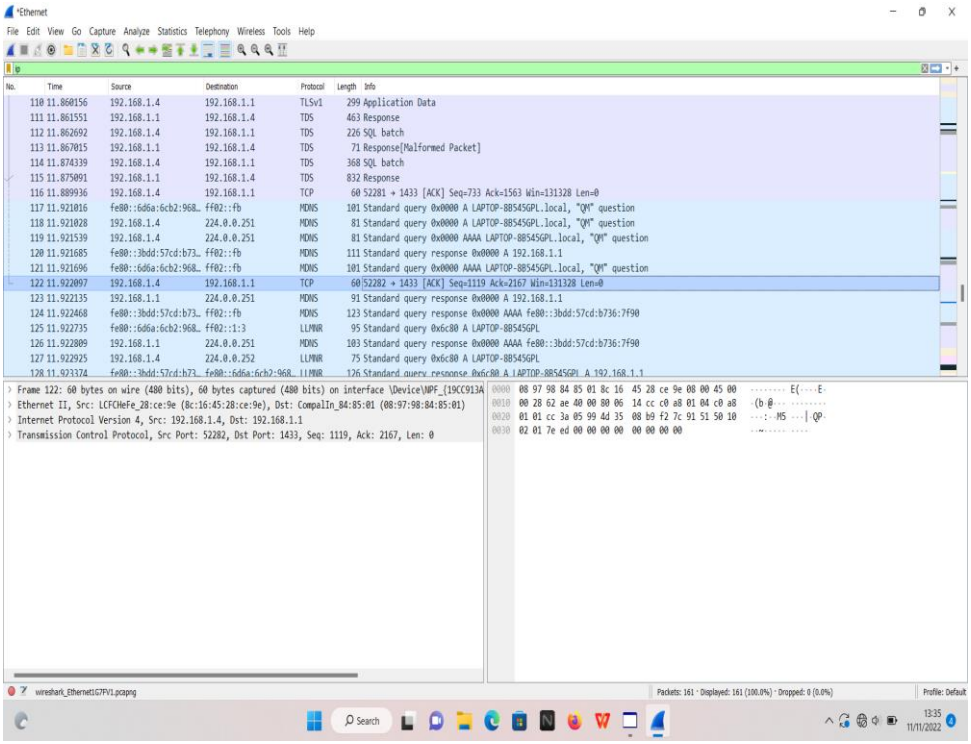
Pengujian proses enkripsi dan dekripsi menggunakan *wireshark* antara lain :

1. Membuka Aplikasi *Wireshark* seperti Gambar 1.

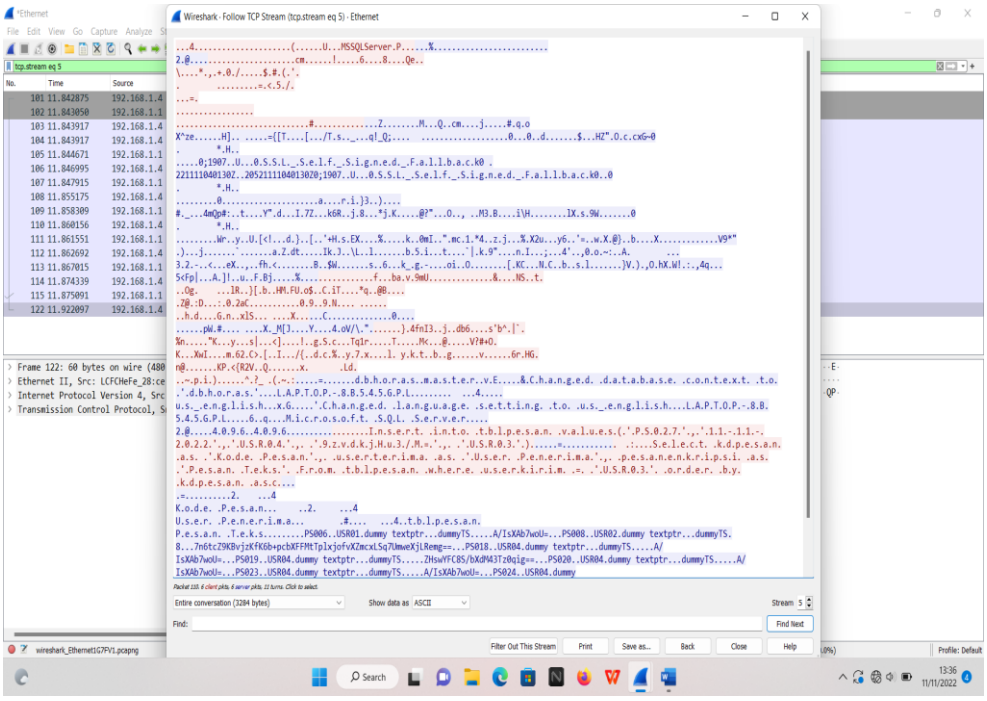


Gambar 1. Aplikasi *Wireshark*

2. Melakukan *Capturing* pada *Interface Ethernet*, kemudian klik start
3. Adapun hasil *Capturing Packets* pada saat proses enkripsi dan dekripsi dilakukan, seperti Gambar 2.



Gambar 2. *Capturing*



Gambar 3. Hasil *Capturing*

KESIMPULAN DAN SARAN

Kesimpulan

1. Sistem keamanan pesan teks berbasis jaringan menggunakan Algoritma *Data Encryption Standard* (DES) dibuat menggunakan Bahasa Pemrograman *Visual Basic .Net* dan *database SQL Server*. Sistem keamanan yang dibangun dapat membantu merahasiakan pesan yang akan dikirim dari pengirim ke penerima pesan melalui algoritma DES.

2. Proses Enkripsi dapat dilakukan oleh *user* yang akan mengirim pesan teks ke *user* yang dituju dapat membuka *form* enkripsi dan memilih *user* yang akan dituju, pesan yang telah terenkripsi akan tersimpan ke dalam *database*. Sedangkan dekripsi dapat dilakukan oleh *user* yang menerima pesan teks dengan membuka *form* dekripsi dan menampilkan pesan-pesan yang telah dikirim oleh pengirim pesan.
3. Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi mampu melakukan enkripsi dan dekripsi pesan teks menggunakan algoritma DES.
4. Berdasarkan pengujian menggunakan *wireshart*, dapat disimpulkan bahwa *wireshartk* tidak menangkap paket yang dikirimkan dikarenakan aplikasi *wireshark* adalah aplikasi pihak ketiga. Ketika aplikasi *wireshark* terlibat di dalam server maka paket atau pesan yang dikirimkan dapat terbaca.

Saran

1. Agar dapat menggunakan aplikasi ini untuk mengamankan pesan teks yang akan dikirim ke komputer lain
2. Agar dapat mengembangkan aplikasi untuk penelitian selanjutnya dengan membuat aplikasi berbasis *online*.

DAFTAR PUSTAKA

Adhar, D., 2019. Implementasi Algoritma DES (Data Encryption Satandard) Pada Enkripsi dan Dekripsi SMS Berbasis Android. Jurnal Teknik Informatika Kaputama (JTIK), Volume Vol.3 No.2 p-ISSN. 2548-9704.

Ardi, 2020. Android dan Kriptografi Algoritma Rivest Code 6 Rekayasa Perangkat Lunak SMS (Short Messages Service). Medan: CV. Sentosa Deli Mandiri.

Blazing, A., 2018. Pemrograman Windows Dengan Visual Basic .Net : Praktikum Pemrograman VB.Net. s.l.:Google Book.

Budiarto, E., 2017. Pembuatan Aplikasi Web Berbasis SMS Sebagai Media Penyalur Informasi dan Komunikasi Antara Sekolah Dengan Orang Tua Siswa. Junal Ilmiah Pendidikan Teknik Kejuruan (JIPTEK) Vol.X No.1 Januari 2017.

Hendry, 2018. Implementasi Samba Server Untuk Mendukung Sharing Printer di SD Swasta Al-Washliyah 6/39 Medan. Jurnal Ilmiah Core IT, Volume Vol.6 No.1 e-ISSN:2548-3528.

Hidayat, S. M., 2018. Aplikasi Sistem Informasi Akuntansi Penjualan Tunai Gas LPG Pada PT. Rukun. Bandung: Politeknik Komputer Niaga LPKIA Bandung (Google Books).

Indrajani, 2017. Database Design Theory, Practice, and Case Study. Jakarta: PT. Elex Media Komputindo.

Jamaludin & Romindo, 2020. Kriptografi : Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA. Medan: Yayasan Kita Menulis.

Khasanah, F. N., 2016. Perancangan dan Simulasi Jaringan Komputer Menggunakan Graphical Network Simulator 3 (GNS3). Makalah Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta..

Kusumo, A. S., 2016. Administrasi SQL Server 2014. Jakarta: PT. Elex Media Komputindo.

Pamungkas, C. A., 2017. Pengantar dan Implementasi Basis Data. Yogyakarta: Penerbit Deepublish.

Santoso & Nurmalina, R., 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). Jurnal Integrasi, Volume Vol.9 No.1 April 2017 e-ISSN : 2548-9828.

Simargolang, M. Y., Widarma, A. & Irawan, M. D., 2021. Jaringan Komputer. Medan: Yayasan Kita Menulis.

Simarmata, J. et al., 2021. Teknologi Informasi dan Multimedia. Medan: Yayasan Kita Menulis.

Yanti, N. R., Alimah & Ritonga, D. A., 2018. Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database. Jurnal Sains Komputer dan Inforamtika (J-SAKTI), Volume Vol.2 No.1 ISSN.2548-9771.

Yendrianof, D. et al., 2022. Analisis dan Perancangan Sistem Informasi. Medan: Yayasan Kita Menulis.