KOMBINASI ALGORITMA ENKRIPSI DAN DEKRIPSI MENGGUNAKAN *CAESAR CIPHER, DATA ENCRYPTION STANDARD,* DAN RIVEST SHAMIR ADLEMAN UNTUK MENDAPATKAN ALGORITMA BARU DENGAN KEAMANAN YANG LEBIH TINGGI

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar

Sarjana Sains Bidang Studi Matematika

Oleh :

MUHAMMAD NUR FAKHRIANSYAH

NIM. 08011281924050

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

KOMBINASI ALGORITMA ENKRIPSI DAN DEKRIPSI MENGGUNAKAN *CAESAR CIPHER*, *DATA ENCRYPTION STANDARD*, DAN RIVEST SHAMIR ADLEMAN UNTUK MENDAPATKAN ALGORITMA BARU DENGAN KEAMANAN YANG LEBIH TINGGI

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
Sarjana Sains Bidang Studi Matematika

Oleh

MUHAMMAD NUR FAKHRIANSYAH
NIM. 08011281924050

Indralaya, Agustus 2023

Pembimbing Kedua	Pembimbing Utama
Dr. Bambang Suprihatin, S.Si., M.Si.	**Drs. Endro Setyo Cahyono, M.Si.**
NIP. 197101261994121001	**NIP. 196409261990021002**

Mengetahui,
a.n. Ketua
Sekretaris Jurusan Matematika

Dr. Dian Cahyawati S. S.Si., M.Si.
NIP. 197303212000122001

PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini:

Nama Mahasiswa : Muhammad Nur Fakhriansyah

NIM : 08011181924018

Fakultas/Jurusan : MIPA/Matematika

Menyatakan bahwa skripsi ini adalah hasil karya saya sendiri dan karya ilmiah ini belum pernah diajukan sebagai pemenuhan persyaratan untuk memperoleh gelar kesarjanaan starata satu (S1) dari Universitas Sriwijaya maupun perguruan tinggi lain.

Semua informasi yang dimuat dalam skripsi ini berasal dari penulis lain baik yang dipublikasikan atau tidak telah diberikan penghargaan dengan mengutip nama sumber penulis secara benar. Semua isi dari skripsi ini sepenuhnya menjadi tanggung jawab saya sebagai penulis.

Demikianlah surat pernyataan ini saya buat dengan sebenarnya.

Indralaya, 9 Agustus 2023

Penulis

LEMBAR PERSEMBAHAN

Kupersembahkan skripsi ini untuk:

Yang Maha Kuasa Allah Subhanahu Wa Ta'ala,

Kedua orang tuaku tersayang

Adik laki – lakiku,

Keluarga besarku,

Semua guru dan dosenku,

Sahabat – sahabatku,

Almamaterku

Motto

"Selalu selesaikan apapun yang pernah dimulai"

"Terkadang diri kita tidak mampu melewati sesuatu bukan karena tidak mampu

Tetapi karena tidak percaya diri"

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahu wa Ta'ala yang telah memberikan rahmat dan nikmat nya sehingga penulis dapat menyelesaikan skripsi dengan judul "**Kombinasi Algoritma Enkripsi dan Dekripsi Menggunakan *Caesar Cipher, Data Encryption Standard*, dan Rivest Shamir Adleman untuk Mendapatkan Algoritma Baru dengan Keamanan yang Lebih Tinggi"** dengan baik dan selesai pada waktunya. Skripsi ini disusun sebagai salah satu syarat memperoleh gelar Sarjana Matematika di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya.

Penulis menyadari bahwa proses pembuatan skripsi ini merupakan proses pembelajaran yang sangat berharga serta tak lepas dari kekurangan. Dengan segala hormat dan kerendahan hati, penulis mengucapkan terimakasih kepada kedua orang tuaku, ayahanda **Faisol** dan ibunda **Sri Taryanti** yang selalu mendidik, memberi nasehat serta senantiasa mengiringi dengan doa untuk penulis. Dalam penulisan skripsi ini juga banyak mendapat bantuan dari berbagai pihak, baik secara langsung maupun tidak langsung. Penulis mengucapkan terima kasih dan penghargaan kepada :

1. Bapak **Drs. Sugandi Yahdin, M.M** selaku Ketua Jurusan Matematika FMIPA Universitas Sriwijaya yang telah memberikan arahan selama proses perkuliahan dan Ibu **Dr. Dian Cahyawati Sukanda, M.Si** selaku Sekretaris Jurusan Matematika FMIPA Universitas Sriwijaya yang telah mengarahkan urusan akademik kepada penulis.

2. Bapak **Drs. Endro Setyo Cahyono, M.Si** dan Bapak **Dr. Bambang Suprihatin, S.Si,. M.Si** selaku dosen pembimbing yang telah bersedia memberikan waktu, tenaga, pikiran, nasehat, dan motivasi selama proses pembuatan skripsi dengan penuh pengertian dan kesabaran.
3. Ibu **Dr. Anita Desiani, S.Si., M. Kom** dan Ibu **Indrawati, S.Si, M.Si** selaku dosen pembahas dan penguji yang telah memberikan tanggapan, kritik, dan saran yang sangat bermanfaat untuk perbaikan dan penyelesaian skripsi ini.
4. Bapak **Drs. Ali Amran, M.T.** dan Ibu **Dr. Ir. Herlina Hanum, M.Si.** selaku ketua dan sekretaris tim pelaksana tugas akhir penulis.
5. Ibu **Novi Rustiana Dewi, S.Si., M.Si** selaku dosen pembimbing akademik yang telah membimbing dan mengarahkan urusan akademik penulis.
6. Seluruh **Dosen di Jurusan Matematika FMIPA** yang telah memberikan ilmu, nasihat, motivasi, serta bimbingan selama proses perkuliahan.
7. Pak **Irwansyah** selaku admin dan Ibu **Hamidah** selaku pegawai tata usaha Jurusan Matematika FMIPA yang telah membantu penulis selama perkuliahan.
8. Adikku, **Ahmad Nauval Ramadhani** yang selalu mendoakan dan mendukung penulis.
9. Sahabat yang telah menemani sejak awal perkuliahan, **Nisa Nur Aisyah**, **Muhammad Taruna Aditama**, **Ramadhan Rafi**, **Yudha Andes Bimantoro**, **Ferdy Kurnia**, **Alga Mahida, Clarita Margo Uteh, Tri Ajeng Fadilah** yang senantiasa menemani suka dan duka, memberikan semangat, dan memberikan energi positif kepada penulis.

10. **Keluarga Matematika**, **Seluruh Angkatan 2019**, **Komputasi 2019, BPH Himastik Kabinet Gelora Karya, BPH BEM KM FMIPA Kabinet Rubik Laskarika,** dan rekan – rekan organisasi selama perkuliahan.
11. Kedua adik, **Adelvin Mahatantri dan Nur Fatimah Vita Sari,** yang telah menemani masa masa akhir perkuliahan, selalu memberikan semangat, dan memberikan energi positif kepada penulis.
12. Kakak – kakak tingkat angkatan 2016, 2017, dan 2018 serta adik – adik angkatan 2020, 2021, dan 2022, terima kasih atas segala kebaikan dan bantuan.
13. Semua pihak yang tidak dapat penulis sebutkan satu per satu. Semoga segala kebaikan yang diberikan mendapatkan balasan terbaik.

Semoga skripsi ini dapat menambah pengetahuan dan bermanfaat bagi mahasiswa/I Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya dan semua pihak yang memerlukan.

Indralaya, Juli 2023

Penulis

A COMBINATION OF ENCRYPTION AND DECRYPTION USING ALGORITHM *CAESAR CIPHER, DATA ENCRYPTION STANDARD,* AND RIVEST SHAMIR ADLEMAN TO GET A NEW ALGORITHM WITH HIGHER SECURITY

Oleh:

MUHAMMAD NUR FAKHRIANSYAH

08011281924050

ABSTRACT

Two basic techniques in cryptography are symmetric and asymmetric. Algorithm Caesar Cipher and Data Encryption Standard includes a symmetric algorithm, while the RSA algorithm includes an asymmetric algorithm. Algorithm hybrid which combines symmetric and asymmetric algorithms is formed to get the advantages of each algorithm. In the encryption and decryption process, high security is the basic benchmark. High data security can be measured by several parameters such as encryption and decryption speed, CPU usage and memory usage. In this study use a combination of algorithms with encryption that starts with the algorithm Caesar Cipher, Data Encryption Standard, and RSA and substantiated by decryption starting with the RSA algorithm, Data Encryption Standard, and Caesar Cipher. This study compare data security with a comparison of a combination of algorithms and a single algorithm. By combining the Caesar Cipher algorithm, Data Encryption Standard, and RSA you can save time, CPU and memory usage. In the combination of algorithms when encryption takes 7.9 seconds, CPU usage is 27.4%, memory used is 8533 mb and when encryption takes 8.4 seconds, CPU usage is 27.8%, memory used is 8527 mb .

Keywords : *Cryptography, Caesar Cipher, Data Encryption Standard, RSA, Data Security*

KOMBINASI ALGORITMA ENKRIPSI DAN DEKRIPSI MENGGUNAKAN *CAESAR CIPHER, DATA ENCRYPTION STANDARD,* DAN RIVEST SHAMIR ADLEMAN UNTUK MENDAPATKAN ALGORITMA BARU DENGAN KEAMANAN YANG LEBIH TINGGI

Oleh:

MUHAMMAD NUR FAKHRIANSYAH

08011281924050

ABSTRAK

Dua teknik dasar dalam kriptografi yaitu simetris dan asimetris. Algoritma *Caesar Cipher* dan *Data Encryption Standard* termasuk algoritma simetris, sedangkan algoritma RSA termasuk algoritma asimetris. Algoritma *hybrid* yang mengkombinasikan algoritma simetris dan asimetris dibentuk untuk mendapatkan kelebihan dari masing masing algoritma. Dalam proses enkripsi dan dekripsi, keamanan yang tinggi menjadi tolak ukur dasar. Keamanan data yang tinggi bisa diukur dengan beberapa parameter seperti kecepatan enkripsi dan dekripsi, penggunaan CPU dan pemakaian memori. Dalam penelitian ini menggunakan kombinasi algoritma dengan enkripsi yang dimulai dengan algoritma *Caesar Cipher, Data Encryption Standard*, dan RSA dan dibuktikan kembali dengan dekripsi yang dimulai algoritma RSA, *Data Encryption Standard*, dan *Caesar Cipher*. Penelitian ini membandingkan keamanan data dengan perbandingan kombinasi algoritma dan algoritma tunggal. Dengan mengkombinasikan algoritma *Caesar Cipher, Data Encryption Standard*, dan RSA dapat menghemat penggunaan waktu, penggunaan CPU dan memori. Dalam kombinasi algoritma ketika enkripsi menghabiskan waktu 7,9 detik, penggunaan CPU sebesar 27,4 %, memori yang terpakai sebesar 8533 mb dan ketika enkripsi menghabiskan waktu 8,4 detik, penggunaan CPU sebesar 27,8 %, memori yang terpakai sebesar 8527 mb.

Kata Kunci : Kriptografi, *Caesar Cipher*, *Data Encryption Standard*, RSA, Keamanan data

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan suatu ilmu dan seni yang mampu menjaga kerahasiaan pesan dengan cara menyandikannya ke bentuk yang sulit dimengerti lagi maknanya (Yusfrizal, 2019). Dalam kriptografi terdapat tiga fungsi dasar yaitu enkripsi, dekripsi dan *Key*. Enkripsi merupakan proses mengamankan data dengan cara mengubah *Plaintext* menjadi kode yang sulit untuk dimengerti dengan algoritma yang digunakan. *Key* adalah kunci yang digunakan dalam berjalannya enkripsi dan dekripsi. Dekripsi merupakan proses mengembalikan kode yang telah dienkripsi sebelumnya menjadi *Plaintext* dengan menggunakan algoritma dan *Key* yang sebelumnya telah digunakan (Atika Sari *et al*., 2018).

Kriptografi memiliki dua teknik dasar dalam melakukan enkripsi dan dekripsi yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris memerlukan penggunaan *Key* yang sama untuk enkripsi atau dekripsi data. Algoritma asimetris menggunakan *Public Key* dan *Private Key* untuk enkripsi atau dekripsi data (Alemami *et al*., 2019). Algoritma simetris dan algoritma asimetris memiliki kekurangan dan juga kelebihan. Untuk algoritma simetris memiliki kelebihan menggunakan satu *Key* enkripsi dan dekripsi serta penggunaan yang mudah, cepat, dan lebih ringan dibanding algoritma asimetris. Algoritma simetris terbatas pada kalimat yang menggunakan huruf latin (Busafi & Kumar, 2020).

Salah satu contoh algoritma simetris yaitu *Caesar Cipher* (Suroso, 2018). *Caesar Cipher* merupakan salah satu algoritma yang paling utama dan juga

sederhana. Algoritma ini dalam prosesnya akan menggantikan huruf pada *Plaintext* dengan posisi huruf yang ditetapkan dengan bilangan yang biasa disebut *Key*. Algoritma *Caesar Cipher* dalam proses enkripsi menggantikan huruf dengan huruf lainnya dengan panjang alfabet 26 karakter (Salmi & Siagian, 2022). Namun, *Caesar Cipher* mudah dipecahkan dengan metode pencarian kunci yang lengkap karena jumlah kuncinya yang sangat kecil yaitu 26 kunci (Limbong & Silitongan, 2017).

Caesar Cipher salah satu algoritma kriptografi yang paling sederhana dan paling awal dikenal (Gowda, 2016). *Caesar Cipher* termasuk algoritma yang cukup lampau dan jarang digunakan. Pada pertengahan 70-an, terdapat algoritma yang ditetapkan sebagai standar enkripsi data dari berbagai lembaga seperti FIPS, NIST, IEEE yaitu *Data Encryption Standard* (DES) (Taghipour *et al*., 2015). Algoritma DES termasuk salah satu algoritma simetris dengan jenis pengoperasian suatu jaringan dengan dasar matematika yang dirancang untuk kode biner, sehingga dapat melindungi data komputer dengan kata sandi. Algoritma kriptografi simetris ini menjadi sistem kriptografi yang penting dalam bidang keamanan informasi. *Plaintext* dalam algoritma DES dienkripsi dalam blok 64 bit menjadi 64 bit *Ciphertext* menggunakan kunci 56 bit (Solichin & Ramadhan, 2017). DES memiliki kunci 56 bit yang mampu mengenkripsikan dan dekripsi dengan sangat luas, namun DES memerlukan banyak perhitungan agar dapat menjaga kesinambungan algoritmanya dan membutuhkan kemampuan untuk memproses komputasi yang lebih kompleks lagi (Lu, 2022). Algoritma simetris memiliki kelemahan *Key* yang digunakan pada enkripsi sama dengan *Key* yang digunakan pada dekripsi. Ketika

Key yang digunakan pada proses enkripsi telah diketahui, maka proses dekripsi dapat dilakukan juga (Limbong & Silitongan, 2017).

Algoritma asimetris menggunakan *Public Key* dan *Private Key* memberikan keamanan lebih dan sulit untuk diretas karena *Private Key* yang digunakan pada proses dekripsi tidak dibagikan kepada siapapun (Busafi & Kumar, 2020). Menurut Maqsood *et al* (2017) yang termasuk algoritma asimetris yaitu Rivest Shamir Adleman (RSA). Algoritma RSA diusung oleh tiga figur ahli matematika yaitu Rivest, Shamir dan Adleman dari Massachusetts Institute of Technology (MIT) pada tahun 1977(Yen & Hung, 2017). RSA menjadi algoritma enkripsi yang sangat terkenal dan berpengaruh dalam bidang penyandian, karena enkripsi dan dekripsi yang dilakukan menggunakan dua kunci yaitu *Public Key* dan *Private Key*. RSA memiliki kunci dengan angka yang besar, jadi semakin panjang kunci yang digunakan maka semakin sukar untuk dipecahkan (Yen & Hung, 2017).

Algoritma simetris dan algoritma asimetris memiliki kelebihan dan kekurangan. Salah satu solusi untuk mendapatkan kelebihan dari kedua algoritma dengan cara menggunakan kedua algoritma menjadi algoritma *hybrid.* Algoritma *hybrid* menggabungkan kedua algoritma menjadi satu dengan mengkombinasikan beberapa algoritma yang ada (Alkady *et al.*, 2013). Keamanan *Key* dari algoritma asimetris yang sulit ditembus karena memilki *Public Key* dan *Private Key* serta kecepatan proses dari algoritma simetris menjadi kelebihan yang didapatkan dari kombinasi yang dilakukan (Elmogy *et al*., 2019). Hasil dari kombinasi beberapa algoritma lebih maksimal dibanding dengan algoritma tunggal dioperasikan tanpa ada kombinasi.

Keamanan yang tinggi menjadi persyaratan dasar dari algoritma enkripsi dan dekripsi data. Di sisi lain, algoritma enkripsi dan dekripsi dikenal sebagai algoritma yang selalu digunakan dalam kriptografi (Nie *et al*., 2010). Algoritma enkripsi dan dekripsi mengkonsumsi sejumlah sumber daya komputasi seperti waktu eksekusi, memori dan daya baterai. Oleh karena itu sangat penting untuk mengevaluasi kinerja algoritma enkripsi dan dekripsi. Beberapa perbandingan untuk menguji algoritma enkripsi dan dekripsi yaitu ukuran blok data yang berbeda, tipe data yang berbeda, konsumsi daya baterai, *Key* yang berbeda dan juga kecepatan dari proses enkripsi dan dekripsi (Nie *et al*., 2010). Kecepatan dari proses enkripsi dan dekripsi adalah waktu yang dibutuhkan oleh algoritma menghasilkan *Ciphertext* dari *Plaintext* (Singh *et al*., 2013).

Pada penelitian ini menggabungkan algoritma *Caesar Cipher*, DES dan RSA sehingga didapatkan kombinasi algoritma yang lebih aman. Untuk menguji keamanan data dilakukan uji dengan parameter yaitu waktu eksekusi, penggunaan CPU, dan jumlah memori yang terpakai dalam menjalankan program dari setiap algoritma *Caesar Cipher*, DES, RSA dan juga kombinasi ketiga algoritma.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini yaitu bagaimana menggabungkan algoritma enkripsi dan dekripsi dengan mengkombinasikan algoritma *Caesar Cipher*, DES, dan RSA dalam mengamankan data dengan tingkat keamanan yang lebih tinggi dibanding metode enkripsi dan dekripsi tunggal.

1.3 Batasan Masalah

Beberapa batasan masalah dalam penelitian ini yaitu :

1. Kata yang diinputkan berjumlah kelipatan 8 karakter karena algoritma DES yang memiliki proses 64 bit.
2. Mengukur efisiensinya proses enkripsi dan dekripsi yang ada di CPU.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk memperoleh algoritma enkripsi dan dekripsi baru dengan mengkombinasikan algoritma *Caesar Cipher*, DES, dan RSA dalam mengamankan data dengan tingkat keamanan yang lebih tinggi dibanding algoritma enkripsi dan dekripsi tunggal.

1.5 Manfaat Penelitian

1. Membentuk algoritma baru dengan mengkombinasikan algoritma *Caaesar Cipher*, DES dan RSA.
2. Menjadi referensi dalam mengkombinasikan beberapa algoritma enkripsi dan dekripsi dalam kriptografi.

DAFTAR PUSTAKA

Abood, Omar G., and Shawkat Guirguis. 2018. "A Survey on Cryptography Algorithms." *International Journal of Scientific and Research Publications (IJSRP)* 8 (7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978.

Alemami, Yahia, Mohamad Afendee Mohamed, and Saleh Atiewi. 2019. "Research on Various Cryptography Techniques." *International Journal of Recent Technology and Engineering* 8 (2 Special Issue 3): 395–405. https://doi.org/10.35940/ijrte.B1069.0782S319.

Alenezi, Mohammed N, Haneen Alabdulrazzaq, and Nada Q Mohammad. 2021. "Symmetric Encryption Algorithms : Review and Evaluation Study." *International Journal of Communication Networks and Information Security*, no. August 2020.

Alkady, Yasmin, Mohmed I Habib, and Rawya Y Rizk. 2013. "A New Security Protocol Using Hybrid Cryptography Algorithms." *International Computer Engineering Conference*.

Aslan, Murat, Mesut Gunduz, and Mustafa Servet Kiran. 2019. "JayaX: Jaya Algorithm with Xor Operator for Binary Optimization." *Applied Soft Computing Journal*, 105576. https://doi.org/10.1016/j.asoc.2019.105576.

Atika Sari, Christy, Eko Hari Rachmawanto, and Christanto Antonius Haryanto. 2018. "Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security." *Scientific Journal of Informatics* 5 (2): 105–17. https://doi.org/10.15294/sji.v5i2.14844.

Bokhari, Mohammad Ubaidullah, and Qahtan Makki Shallal. 2019. "A Review on Symmetric Key Encryption Techniques in Cryptography." *International Journal of Computer Applications* 147.

Busafi, Samya Al, and Basant Kumar. 2020. "Review and Analysis of Cryptography Techniques." *International Conference on System Modeling & Advancement*, 2–6.

Elmogy, Ahmed, Yassin Bouteraa, Reem Alshabanat, and Wojod Alghaslan. 2019. "A New Cryptography Algorithm Based on ASCII Code." *International Conference on Sciences and Techniques of Automatic Control and Computer Engineering*, 626–31. https://doi.org/10.1109/STA.2019.8717194.

Faheem, Muhammad, Sapiee Jamel, Abdulkadir Hassan, Zahraddeen A., Nur Shafinaz, and Mustafa Mat. 2017. "A Survey on the Cryptographic Encryption Algorithms." *International Journal of Advanced Computer Science and Applications* 8 (11). https://doi.org/10.14569/ijacsa.2017.081141.

Gowda, Shreyank N. 2016. “Innovative Enhancement of the Caesar Cipher Algorithm for Cryptography.” *International Conference on Advances in Computing, Communication and Automation*. https://doi.org/10.1109/ICACCAF.2016.7749010.

Liestyowati, Dwi. 2020. “Public Key Cryptography.” *Journal of Physics: Conference Series* 1477 (5). https://doi.org/10.1088/1742-6596/1477/5/052062.

Limbong, Tonni, and Parasian Silitongan. 2017. “Testing the Classic Caesar Cipher Cryptography Using of Matlab.” *International Journal of Engineering and Technology* 6 (02). https://doi.org/10.17605/OSF.IO/PEMA5.

Lu, Zixin. 2022. “Encryption Management of Accounting Data Based on DES Algorithm of Wireless Sensor Network.” *Wireless Communications and Mobile Computing* 2022: 1–14.

Maqsood, Faiqa, Muhammad Ahmed, Muhammad Mumtaz, and Munam Ali. 2017. “Cryptography: A Comparative Analysis for Modern Techniques.” *International Journal of Advanced Computer Science and Applications* 8 (6): 442–48. https://doi.org/10.14569/ijacsa.2017.080659.

Nie, Tingyuan, Chuanwang Song, and Xulong Zhi. 2010. “Performance Evaluation of DES and Blowfish Algorithms.”

Ratnadewi, Roy Pramono Adhie, Yonatan Hutama, A. Saleh Ahmar, and M. I. Setiawan. 2018. “Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC).” *Journal of Physics: Conference Series* 954 (1). https://doi.org/10.1088/1742-6596/954/1/012009.

Saikumar, Indumathi. 2017. “DES - Data Encryption Standard.” *International Research Journal of Engineering and Technology* 4 (3): 1777–82. https://www.slideshare.net/Simplilearn/des-data-encryption-standard-data-encryption-standard-in-cryptography-simplilearn/Simplilearn/des-data-encryption-standard-data-encryption-standard-in-cryptography-simplilearn.

Salmi, Gading Nur, and Farhan Siagian. 2022. “Implementation of the Data Encryption Using Caesar Cipher and Vernam Cipher Methods Based on CrypTool2.” *Journal of Soft Computing Exploration* 3 (2): 99–104. https://doi.org/10.52465/joscex.v3i2.86.

Senthil Kumaran, U., M. K. Nallakaruppan, and M. Senthil Kumar. 2016. “Review of Asymmetric Key Cryptography in Wireless Sensor Networks.” *International Journal of Engineering and Technology* 8 (2): 859–62.

Singh, Sombir, Sunil K Maakar, and Sudesh Kumar. 2013. "A Performance Analysis of DES and RSA Cryptography." *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 2 (3): 418–23.

Solichin, Achmad, and Erwin Wahyu Ramadhan. 2017. "Enhancing Data Security Using DES-Based Cryptography and DCT-Based Steganography." *International Conference on Science in Information Technology* 2018-Janua: 618–21. https://doi.org/10.1109/ICSITech.2017.8257187.

Suparman, Benny, and Sewaka. 2022. "Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake Dan Algoritma Des Bebasis Java Desktop." *OKTAL: Jurnal Ilmu Komputer Dan Sains* 1 (07): 808–17. https://journal.mediapublikasi.id/index.php/oktal/article/view/777%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/777/304.

Suroso, Amat. 2018. "Studi Perbandingan Kriptograpi Menggunakan Metode DES, Triple DES DAN RSA." *Jurnal Teknologi Pelita Bangsa* 8.

Taghipour, Mohammad, Arash Moghadami, and Behbood Moghadam Naghdi Shekardasht. 2015. "Implementation of Software-Efficient DES Algorithm." *Advances in Networks* 3 (3): 7. https://doi.org/10.11648/j.net.s.2015030301.12.

Verma, Rohit, and Aman Kumar Sharma. 2020. "Cryptography : Avalanche Effect of AES and RSA." *International Journal of Scientific and Research Publications* 10 (4): 119–25. https://doi.org/10.29322/IJSRP.10.04.2020.p10013.

Warnilah, A I, and S N Nugraha. 2018. "Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan." *IJCIT (Indonesian Journal on Computer and Information Technology* 3 (2): 243–52. https://repository.bsi.ac.id/index.php/unduh/item/231067/1.-Komparasi-Algoritma-Kriptografi-Elgamal-Dan-Caesar.pdf.

Yen, Neil Y, and Jason C Hung, eds. 2017. *Frontier Computing : Theory, Technologies and Applications FC 2016*. Springer Singapore.

Yusfrizal. 2019. "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan RSA Berbasis Android." *Jurnal Teknik Informatika Kaputama* 3 (2): 29–37.