Jurnal Ilmiah Wahana Pendidikan, September 2022, 8 (16), 467-476
DOI: https://doi.org/10.5281/zenodo.7068003
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan *Local*

Ragil Aria Dewanto[1], Aries Suharso[2]

[1,2]Universitas Singaperbangsa Karawang

Received: 8 Agustus 2022
Revised: 13 Agustus 2022
Accepted: 19 Agustus 2022

Abstract

The purpose of this study is to find out whether a poor network topology can be a important aspect of data leakage if someone wants to steal data without the permission of an institution. The research methodology used in this study is quantitative methods and cryptographic techniques, wherein the quantitative method there are several specifications, namely structured, planned, and systematic, by performing analysis, substitution, blocking, permutation, expansion, and compression. The topology is divided into several types, namely ring topology, star topology, bus topology, tree topology, and mesh topology. In-network attacks that usually occur are spoofing, in-the-middle-attack, and sniffing. The results show that designing a local network topology using several types of topologies can make the network structure more secure. The results also show that combining a star topology and a tree topology makes the local network more secure. The results also show that combining cryptographic techniques can prevent network attacks that have been studied, especially combining blocking and permutation cryptography techniques.

Keywords: *cryptography, LAN, topology, attack, networking.*

(*) Corresponding Author: ragil@gmail.com

How to Cite: Dewanto, R., & Suharso, A. (2022). Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan Local. *Jurnal Ilmiah Wahana Pendidikan*, *8*(16), 467-476. https://doi.org/10.5281/zenodo.7068003.

PENDAHULUAN

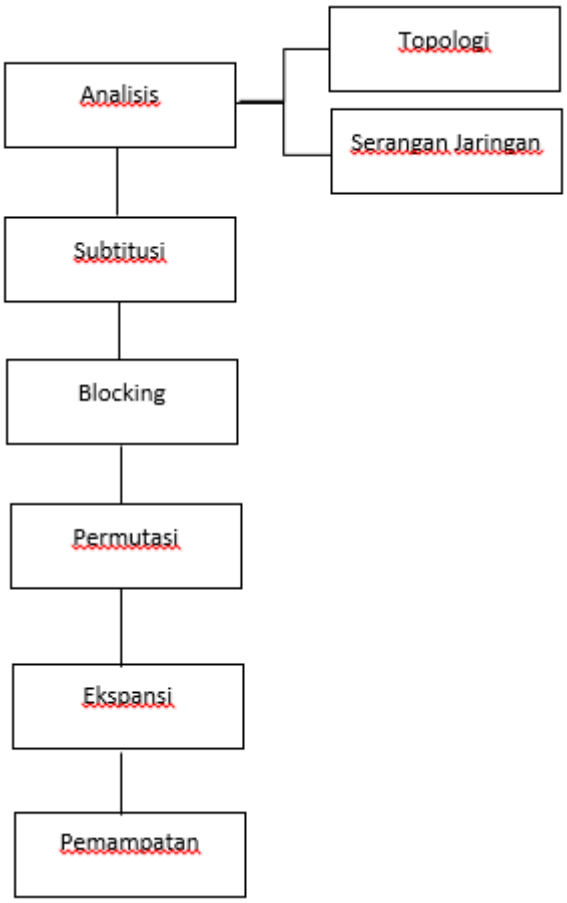
Keamanan jaringan pada sebuah struktur jaringan komputer menjadi sangatlah penting dikarenakan banyak lembaga-lembaga mengalami kebocoran data sehingga lembaga tersebut mengalami kerugian dari segi finansial dll. Dengan adanya keamanan jaringan hal-hal yang dapat merugikan tersebut akan sangat bisa diminimalisir tergantung dari cara penangan dan tahap pembuatan keamanan jaringan.

Sebuah topologi jaringan menjadi pondasi utama dalam mengatur akses jalur pengiriman data, topologi jaringan yang buruk bisa menjadi aspek utama dalam kebocoran data jikalau ada seseorangan yang ingin mencuri data tanpa seizin dari suatu lembaga. Oleh karena itu peneliti ingin melakukan penelitian dengan menggunakan teknik kriptografi dalam hal keamanan jaringannya.

Kriptografi adalah sebuah cara untuk menyamarkan suatu pesan demi menjaga kerahasiaannya. Yang biasanya pesan tersebut harus melalui proses enkripsi dimana pesan akan dikirimkan ke penerima yang sebelumnya sudah diubah kedalam bentuk yang tidak berarti. Hanya pihak yang berhak lah yang dapat dekripsi (pesan utuh) yang biasanya memakai suatu kunci yang rahasia. Kriptografi menganut prinsip kerahasiaan melalui ketidakjelasan.

METODOLOGI PENELITIAN

Pada penelitian ini metodologi penelitian yang digunakan adalah metode kuantitatif dan teknik kriptografi, dimana dalam metode kuantitatif terdapat beberapa spesifikasi yaitu terstruktur, terencana, dan sistematis.



Gambar 1. Metodologi Penelitian

Analisis

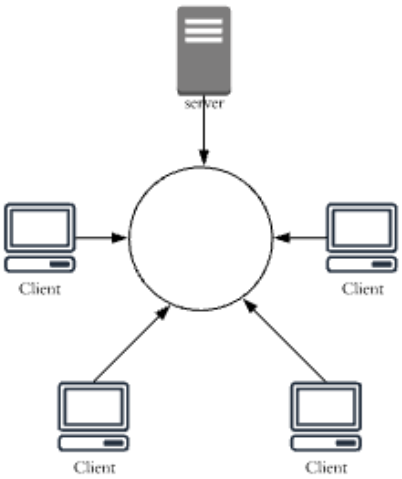
Pada tahap analisis, penelitian akan menganalisis struktur jaringan, dimulai dari melihat macam-macam topologi jaringan yang tersedia yang biasanya topologi terbagi dari beberapa macam jenis yaitu topologi cincin, topologi bintang, topologi *bus*, topologi pohon, dan topologi *mesh* lalu kemudian menganalisis serangan jaringan yang akan diteliti yaitu *spoofing, in-the-middle-attack,* dan *sniffing.*

Topologi Jaringan

Topologi adalah sebuah aturan keterkaitan antara suatu komputer ke komputer lainnya yang biasanya saling terhubung dalam sebuah jaringan, komponen-komponen fisik ini berkomunikasi melalui peralatan jaringan, seperti : *router, server, hub/switch,* dan peralatan-peralatan lainnya. Yang biasanya cara terhubungnya bisa melalui kabel (pengkabelan) atau dengan sinyal *(wireless).* Sedangkan jaringan adalah suatu kesatuan sistem yang saling terhubung, biasanya terdiri atas : komputer, perangkat komputer, dan perangkat jaringan lainnya. Satu kesatuan ini sudah ada aturan yang ditetapkan pada setiap sistem jaringannya. Topologi jaringan terdiri atas beberapa macam, yaitu : topologi *ring*, topologi *tree*, topologi *bus*, topologi *star*, topologi *mesh.*

Topologi *Ring*

Topologi *Ring* adalah sebuah topologi yang bentuknya seperti cincin. Topologi ini saling berhubungan anara suatu komputer ke komputer lainnya sehingga berbentuk cincin. Topologi ini membutuhkan perangkat tambahan yaitu LAN *card* untuk dapat saling terkoneksi.

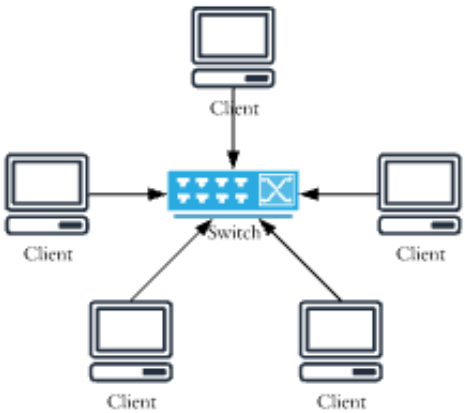


Gambar 2. Topologi *Ring*

Topologi *ring* termasuk topologi yang harganya terjangkau dalam perancangannya, ini menjadikan kelebihan yang topologi *ring* memiliki. Tetapi topologi ini sangat beresiko dikarenakan jika suatu jalur terputus maka client lainnya akan berimbas sehingga tidak bisa digunakan.

Topologi *Star*

Topologi *Star* adalah topologi yang bentuknya seperti bintang. Topologi ini memerlukan *hub* dan *switch* untuk mengkoneksikan suatu *client* ke *clien*t lainnya. Topologi ini merupakan topologi yang paling sering digunakan dalam perancangan topologi suatu jaringan.



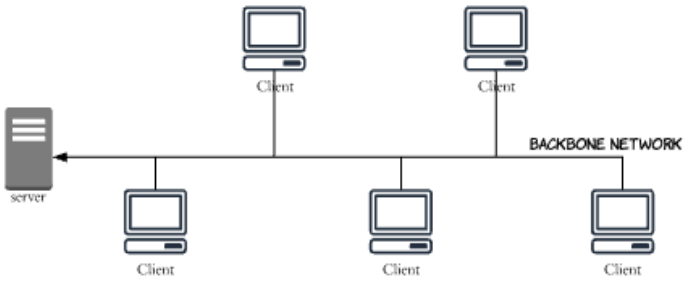
Gambar 3. Topologi *Star*

Topologi ini terbilang cukup mahal dalam pembuatannya dikarenakan membutuhkan banyak kabel untuk jalur pengiriman data, tetapi itu yang menjadikan topologi *star* adalah topologi yang paling aman dalam keamanan

jaringan. Selain itu jika ada sebuah jalur yang mati maka paket data akan tetap bisa dikirim melalui jalur lainnya.

Topologi *Bus*

Topologi *Bus* adalah topologi yang bentuknya paling sederhana dibanding dengan topologi lainnya, hal ini dikarenakan dalam pembuatan topologi ini hanya menggunakan kabel *coaxial* sepanjang *node client* dan konektor[8]. Dan biasa yang menggunakan topologi ini hanya perusahaan yang menggunakan instalasi berbasis kabel *coaxial.*

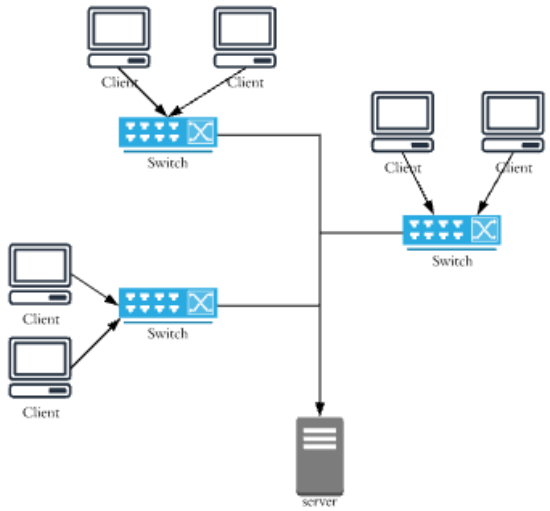


Gambar 4. Topologi *Bus*

Pada topologi ini sangat mudah jika ingin menambahkan client dan dalam pembuatannya biaya yang dikeluarkan cukup sedikit tetapi topologi ini yang paling sering terjadi penumpukan dan tabrakan data sehingga membuat pengiriman data menjadi sangat lama.

Topologi *Tree*

Topologi Tree adalah gabungan antara topologi bus dan topologi star yang biasanya topologi ini digunakan untuk interkoneksi antara hirarki dan pusat yang berbeda, itu yang membuat topologi ini berbentuk seperti pohon.

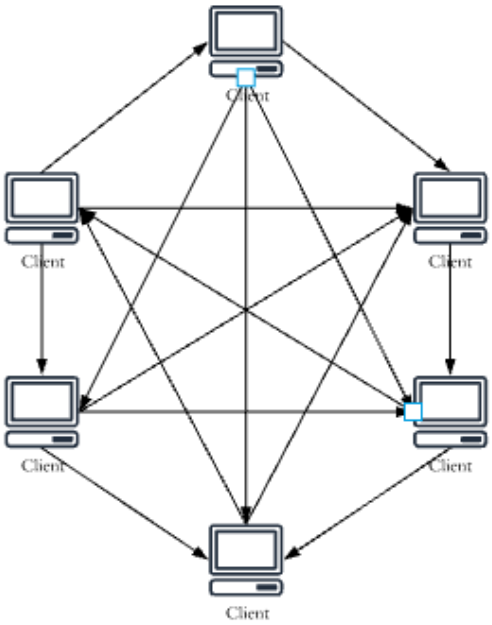


Gambar 5. Topologi *Tree*

Topologi ini terbilang mahal dalam proses pemasangannya topologi ini sangat mudah dikembangkan tergantung situasi dalam suatu perusahaan dikarenakan susunan topologinya terpusat pada suatu hirarkinya.

Topologi *Mesh*

Topologi *mesh* adalah topologi yang memiliki kecepatan pengiriman data paling tinggi dikarenakan topologi ini menggunakan kabel tunggal dalam pengiriman datanya tanpa harus melewati *switch* atau *hub* terlebih dahulu. Topologi ini memiliki banyak rute dalam pengiriman datanya[2].



Gambar 6. Topologi *Mesh*

Topologi ini memiliki keamanan jaringan yang sangat baik dikarenakan tidak akan terjadi tabrakan atau penumpukan data, dan yang paling penting topologi ini memiliki limit bandwidth yang cukup besar sehingga pengiriman setiap datanya akan lebih cepat sampai ketujuan. Tetapi dalam pemasangan topologi ini memakan banyak biaya dikarenakan membutuhkan banyak kabel untuk digunakan.

***Local Area Network* (LAN)**

Local Area Network atau yang disingkat LAN adalah suatu jaringan yang cakupan areanya kecil yang biasanya digunakan pada sebuah kantor yang tidak mempunyai cabang, atau kampus-kampus yang hanya menggunakan beberapa ruangan saja untuk jaringan internet. Biasanya LAN diimplementasikan terhadap sebuah perangkat seperti printer, voip, dan lain-lain.

LAN adalah sebuah jaringan yang saling terhubung yang biasanya menggunakan sejumlah komputer yang terdapat didalam suatu area kecil atau terbatas seperti sebuah gedung atau ruangan (Madcoms, 2010).

LAN adalah sebuah penghubungan dua atau lebih perangkat dalam sebuah geografis yang terbatas, biasanya LAN digunakan dalam suatu ruangan atau gedung yang sama sehingga setiap perangkat yang terdapat dalam area tersebut bisa saling terkoneksi (Rainer,2011).

Serangan Jaringan

Serangan jaringan adalah tindakan pencurian data yang bisa merugikan suatu lembaga, maka dari itu supaya terhindar dari serangan jaringan kita harus

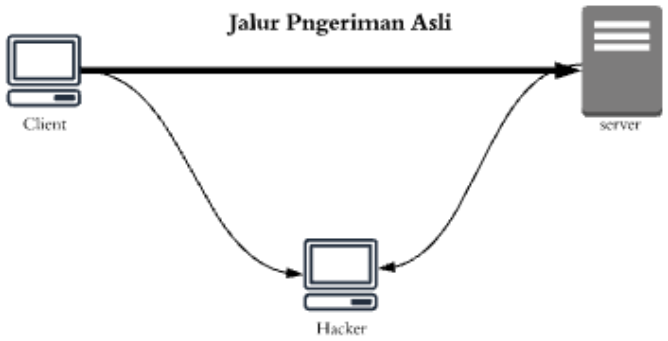
memiliki keamanan yang baik dalam struktur jaringan. Serangan yang biasa terjadi dalam sebuah jaringan antara lain *spoofing, in-the-middle-attack, sniffing.*

Spoofing

Spoofing adalah sebuah tindakan penyamaran yang bertujuan untuk menipu orang lain atau sebuah lembaga[12]. Sebagai contoh: misalkan Dika (*hacker*) adalah orang menyamar sebagai Rico (orang dalam sebuah lembaga) jadi Dika meyakinkan kepada orang lembaga tersebut bahwa dirinya adalah Rico. Jika orang-orang lembaga tersebut sudah mempercayainya barulah Dika meminta sejumlah data pribadi seperti password atau pin atm dan itulah yang menjadi tindakan merugikan banyak orang.

In-The-Middle-Attack

Pada serangan ini *hacker* akan masuk kedalam jalur pengiriman sebuah paket data, dimana ketika user mengirimkan paket data ke server maka dalam proses pengirimannya *hacker* dapat mengambil dan mengubah data tersebut sehingga data yang dikirim user ke server bisa berubah[13].



Gambar 7. MITM

Jadi proses penyerangannya *client* akan mengirimkan sebuah data yang akan dikirimkan ke server, jika *hacker* berhasil menembus keamanan jaringannya maka *hacker* akan berada ditengah-tengah pengiriman paket data tersebut. Data tersebut akan melewati *hacker* dahulu yang nantinya data tersebut bisa diubah atau diambil oleh *hacker.*

Sniffing

Sniffing adalah penyerangan yang bersifat pencurian data yang sudah di enkripsi maupun data yang belum dienkripsi *hacker* biasanya menyerang saluran komunikasi. Hal ini sering terjadi pada saluran publik jadi *hacker* dapat merekam pembicaraan-pembicaraan yang sedang terjadi.

HASIL DAN PEMBAHASAN

Subtitusi

Dalam langkah subtitusi hal harus dilakukan pertama adalah membuat tabel substitusi, tabel substitusi dapat dibuka sesuka hati dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat acak maka akan semakin sulit untuk pemecahan *ciphertext* oleh orang yang tidak berhak. Berikut adalah contoh tabel substitusi :

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-,-

B-F-1-K-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Gambar 7. Subtitusi

Gambar substitusi diatas dibuat secara acak, dengan menggunakan tabel tersebut dari plaintext "kriptografi" dihasilkan ciphertext "6MPX72AMBGP". Dengan menggunakan arah yang terbalik *(reverse)*, *plaintext* dapat diperoleh kembali dari *ciphertext*-nya.

Blocking

Sistem enkripsi terkadang membagi *plaintext* menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian di enkripsi secara independen. *Plaintext* yang di enkripsi dengan menggunakan teknik *blocking* adalah

Blok 1	I	R	G	
Blok 2	N	I	R	Y
Blok 3	I	P	A	A
Blok 4		T	F	
Blok 5	K	O	I	

Gambar 8. *Blocking*

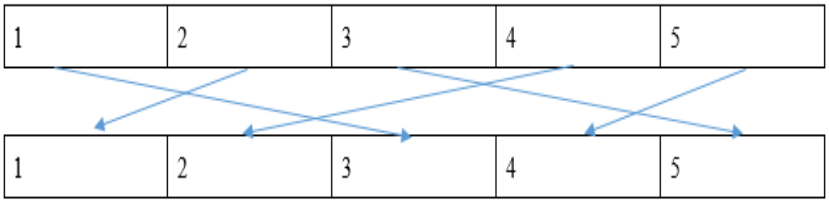
Plaintext-nya : "INI KRIPTOGRAFI YA"

Maka, enkripsi-nya : "IRG NIRY IPAA TF"

Dengan menggunakan enkripsi *blocking* dipilih jumlah jalur dan kolom untuk penulisan pesan. Jumlah jalur atau kolom menjadi kunci bagi kriptografi dengan teknik ini. *Plaintext* dituliskan secara vertikal ke bawah berurutan pada jalur dan kemudian dilanjutkan pada kolom berikutnya sampai semua tertulis.

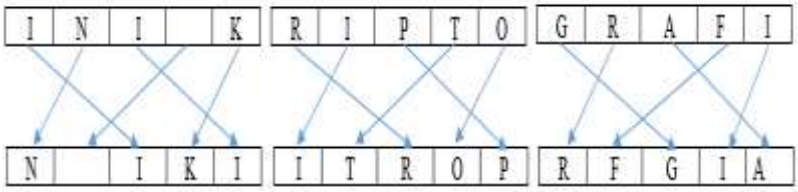
Permutasi

Permutasi bisa dibilang juga adalah teknik enkripsi yang terpenting dalam kriptografi dikarenakan teknik ini memindahkan atau merotasi kan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi, sebelum dilakukan permutasi umumnya *plaintext* terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.Berikut adalah contoh blok dari teknik permutasi :



Gambar 9. Permutasi

Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari *plaintext* "INI KRIPTOGRAFI" adalah sebagai berikut



Gambar 10. Permutasi Kriptografi

Ciphertext yang dihasilkan dengan teknik permutasi ini adalah "N IKI ITROP RFGIA"

Ekspansi

Teknik ekspansi adalah suatu metode sederhana untuk mengacak pesan dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, maka ditambah akhiran huruf konsonan "i". Berikut adalah contoh proses enkripsi dengan cara ekspansi :

plaintext "KRIPTOGRAFI"

K-RIPTOGRAFI = RIPTOGRAFI-K(AN)

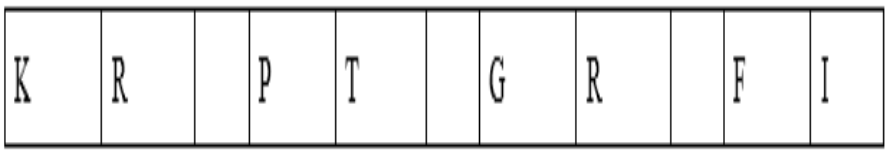
Dengan kata lain jika plaintext yang dikirimkan adalah "kriptografi" maka proses enkripsinya menjadi "riptografikan". Aturan teknik ekspansi bisa dibuat lebih kompleks, terkadang teknik ekspansi digabungkan dengan teknik lainnya dikarenakan teknik ini bila berdiri sendiri terlalu mudah untuk dipecahkan.

Pemampatan *(Compaction)*

Teknik pemampatan adalah teknik yang mengurangi pesan atau jumlah bloknya ini adalah sebuah cara lain untuk menyembunyikan pesan[16]. Contoh sederhananya menggunakan cara menghilangkan setiap karakter ketiga secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali kedalam dan disusulkan sebagai lampiran dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh yang akan dilakukan oleh penulis maka akan menggunakan simbol "&". Berikut adalah contoh *plaintext* "Kriptografi" yang akan dienkripsi :

Gambar 11. Pemampatan *plaintext*

Kemudian dihilangkannya karakter ke-tiga secara berurutan.



Gambar 12. Pemampatan *ciphertext*

Maka *chipertext* yang akan dihasilkan adalah "KRPTGRFI & IOA". Aturan penghilangan karakter dan karakter khusus yang berfungsi sebagai pemisah menjadi dasar untuk proses dekripsi *ciphertex*t menjadi *plaintext* kembali.

KESIMPULAN

Dari hasil penelitian yang telah dilakukan dapat diambil kesimpulannya, yaitu :

1. Dalam perancangan topologi jaringan *local* menggunakan beberapa jenis topologi dapat membuat struktur jaringannya menjadi lebih aman.
2. Menggabungkan topologi *star* dan topologi *tree* membuat jaringan *local* menjadi lebih aman.
3. Menggabungkan teknik kriptografi dapat mencegah serangan jaringan yang telah diteliti terutama menggabungkan teknik kriptografi blocking dan permutasi.

DAFTAR PUSTAKA

Basri, "Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi," *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 17–23, 2016, [Online]. Available: http://ejournal.fikom-unasman.ac.id.

Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Sinkron*, vol. 2, no. 2, pp. 13–17, 2018, [Online]. Available: https://jurnal.polgan.ac.id/index.php/sinkron/index.

Widodo, M. Yana, and H. Agung, "Implementasi Topologi Hybrid Untuk Pengoptimalan Aplikasi Edms Pada Project Office Pt Phe Onwj," *J. Tek. Inform.*, vol. 11, no. 1, pp. 19–30, 2018, doi: 10.15408/jti.v11i1.6472.

W. M. Ashari, "Perbandingan Performa Kriptografi Asimetris Pada Proses Key Exchange," *Sci. Tech J. Ilmu Pengetah. dan Teknol.*, vol. 6, no. 1, pp. 26–32, 2020, doi: 10.30738/jst.v6i1.6609.

M. Y. Maulana *et al.*, "Perancangan Aplikasi Media Pembelaran," *FTIK*, vol. 1, no.

1, pp. 357–367.
N. Aini, "Analisis Jaringan Local Area Network," *Prosisko*, vol. 5, no. 1, 2018, doi: 10.31219/osf.io/htxwe.
J. Rahmadoni, "PERANCANGAN SIMULASI PEMBELAJARAN KRIPTOGRAFI KLASIK MENGGUNAKAN METODE WEB BASED LEARNING," *J. Inf. Technol. Comput. Sci.*, vol. 1, no. 1, pp. 1–25, 2018, doi: https://doi.org/10.31539/intecoms.v1i1.160.
M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 4, pp. 244–247, 2021, doi: 10.32672/jnkti.v4i4.3098.
S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteksi.v6i1.395.
P. S. SIANTURI, "Aplikasi Pembelajaran Kriptografi Hill Chiper Dengan Menggunakan Metode Computer Based Instruction," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 3, no. 2, pp. 38–43, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/174.
M. A. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security," *Int. J. Sci. Res. Publ.*, vol. 9, no. 3, p. p8779, 2019, doi: 10.29322/ijsrp.9.03.2019.p8779.
J. Y. A. Elreesh and S. S. Abu-Naser, "Cloud Network Security Based on Biometrics Cryptography Intelligent Tutoring System," vol. 3, no. 3, pp. 37–70, 2019, [Online]. Available: http://dstore.alazhar.edu.ps/xmlui/handle/123456789/146.
S. Althuniba, M. Chen, G. Martinez, and M. Sheng, "Publishing Editors Board of Editors," *Int. J. Electron. Inf. Eng.*, vol. 8, no. 2, 2018.
P. B. T. Kumbara and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Permainan Tradisional Rangku Alu," *J. Tek. Inform. dan Sist. Inf.*, vol. 5, no. 2, pp. 189–200, 2019, doi: 10.28932/jutisi.v5i2.1714.
W. Susanti and R. N. Putri, "Penerapan Cloud Computing Sebagai Media Pembelajaran Berbasis Online Masa Pandemi Covid-19," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 4, no. 1, p. 56, 2020, doi: 10.35145/joisie.v4i1.663.
B. Jana and J. Poray, "A performance analysis on elliptic curve cryptography in network security," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), 2016, pp. 1-7, doi: 10.1109/ICCECE.2016.8009587.