Penerapan Kriptografi Dalam Menanggulangi Ancaman Cyber "Undangan Non Aplikasi"

Syafrillah Astro Heriadi[1], Fadia Aulia Azizah[2], Fauzan Eky Septyadi[3*]

[1] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[1]syafrillahastro@gmail.comstro

[2] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[2]auliafadia122@gmail.com

[3] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[3]fauzaneky8@gmail.com

Abstrak— **Seiring dengan berkembangnya teknologi informasi, ancaman cyber semakin beragam dan kompleks. Kriptografi merupakan salah satu teknologi yang sangat efektif dalam mengatasi berbagai ancaman tersebut. Makalah ini membahas penerapan kriptografi untuk menanggulangi ancaman cyber, dengan fokus pada implementasi dalam mengamankan undangan dan link untuk mencegah serangan berbahaya. Diterangkan juga langkah-langkah praktis instalasi dan penggunaan pustaka cryptography di lingkungan pengembangan Python, serta cara mengatasi kebijakan eksekusi PowerShell yang dapat menjadi hambatan. Perkembangan teknologi, khususnya dalam hal pengamanan data, telah mengalami kemajuan pesat dalam menjaga keamanan informasi. Untuk melindungi data informasi, terdapat beberapa bidang ilmu yang dikembangkan, seperti kriptografi dan steganografi. Dalam penerapannya, sering kali tidak hanya menggunakan satu teknik keamanan saja, melainkan kombinasi dari beberapa teknik untuk meningkatkan keamanan data informasi. Penelitian ini bertujuan untuk merancang sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada pesan teks.**

Abstract— **As information technology develops, cyber threats become increasingly diverse and complex. Cryptography is a technology that is very effective in overcoming these various threats. This paper discusses the application of cryptography to combat cyber threats, with a focus on implementation in securing invitations and links to prevent malicious attacks. Practical steps for installing and using cryptography libraries in the Python development environment are also explained, as well as how to overcome PowerShell execution policies that can become obstacles. Technological developments, especially in terms of data security, have made rapid progress in maintaining information security. To protect information data, several fields of science have been developed, such as cryptography and steganography. In its application, it often does not only use one security technique, but rather a combination of several techniques to increase the security of information data. This research aims to design a data security system by implementing cryptography in text messages.**

I. PENDAHULUAN

Dalam era digital, ancaman cyber seperti phishing, malware, dan serangan man-in-the-middle menjadi semakin lazim. Teknologi kriptografi menawarkan solusi untuk melindungi data dan komunikasi dari ancaman ini dengan menyediakan mekanisme enkripsi dan dekripsi yang kuat. Artikel ini menjelaskan cara mengimplementasikan kriptografi dalam konteks undangan digital untuk memastikan keamanan tautan dan informasi yang dibagikan.

Memahami kejahatan cyber memerlukan adanya hukum cyber yang dapat mengendalikan kejahatan siber yang telah menyerang penggunaan teknologi informasi di masyarakat. Hukum cyber adalah hukum multidisipliner yang mencakup berbagai cabang ilmu seperti hukum pidana, hukum perdata, perlindungan konsumen, ekonomi, serta administrasi yang didukung oleh teknologi, sosial budaya, dan hukum. Pentingnya menerapkan hukum cyber telah menjadi perhatian pemerintah di berbagai negara di seluruh dunia, mengingat sebagian besar masyarakat sudah bergantung pada teknologi dalam kehidupan sehari-hari. Selain itu, penting juga untuk memahami bentuk perkembangan kejahatan siber yang dilakukan oleh pihak yang tidak bertanggung jawab. Kejahatan cyber dilakukan oleh individu yang menggunakan teknologi informasi, seperti programmer, analis sistem, manajer, dan kasir, yang mampu melakukan kejahatan cyber. Faktor pendorong kejahatan ini adalah pesatnya perkembangan teknologi, baik itu handphone maupun smartphone, yang memberikan peluang bagi pelaku untuk mencuri atau merusak data demi keuntungan tertentu.

Memahami kejahatan cyber memerlukan upaya untuk menanggulangi kejahatan berbasis digital, salah satunya dengan menggunakan dan memanfaatkan teknologi kriptografi. Berbagaiteknik kriptografi telah banyak diterapkan untuk mengamankan transaksi digital yang digunakan saat ini. Dalam buku tentang manajemen keamanan, disebutkan ada tiga aspek penting dalam penggunaan

dan penerapan keamanan informasi: kerahasiaan, keutuhan data, dan ketersediaan. Penerapan teknologi kriptografi memberikan jaminan terhadap kerahasiaan komunikasi. Pengembangan ilmu pengetahuan untuk meningkatkan keamanan penggunaan teknologi perlu ditingkatkan agar masyarakat merasa aman dan nyaman saat menggunakannya. Salah satu teknik yang digunakan adalah teknologi kriptografi, yang menyandikan data atau informasi sebelum dikirim melalui internet. Teknik ini mempermudah pengamanan informasi dengan proses enkripsi yang mengacak data agar sulit ditemukan.

Tulisan ini akan mengulas penggunaan teknik kriptografi untuk mengamankan teknologi informasi dari kejahatan cyber. Selain itu, tulisan ini akan menggambarkan bagaimana teknik kriptografi membantu dalam penanganan kejahatan siber secara digital. Tujuan tulisan ini adalah untuk memahami cara kerja, peran, dan tindakan yang dapat diambil dalam menangani kejahatan cyber. Teknik kriptografi yang dibahas dalam artikel ini diharapkan dapat memberikan wawasan dan membantu penegak hukum dalam memerangi kejahatan cyber yang semakin meningkat.

II. METODOLOGI PENELITIAN

Metodologi penelitian ini dirancang untuk mengkaji penerapan kriptografi dalam menanggulangi ancaman cyber, khususnya dalam konteks pengamanan undangan dan link digital. Penelitian ini akan mencakup langkah-langkah sistematis untuk mengevaluasi efektivitas teknik kriptografi yang diterapkan serta pengaruhnya terhadap keamanan data yang dibagikan.

A. Desain Penelitian

Penelitian ini menggunakan desain eksperimental untuk menguji dan mengevaluasi penerapan kriptografi dalam skenario praktis. Eksperimen dilakukan dengan menciptakan lingkungan pengujian yang aman di mana berbagai teknik kriptografi dapat diterapkan dan diuji.

B. Alat dan Bahan

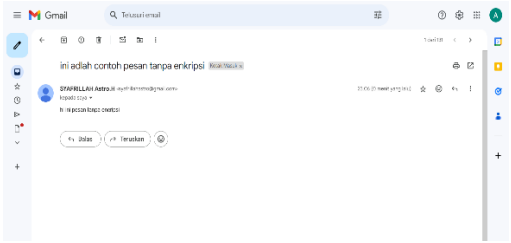
1. Perangkat Lunak :
   - Pyhton
   - Visual studio code
   - Pustaka ” c*ryptography*” di pyhton
2. Perangkat Keras:
   - Komputer dengan spesifikasi minimum:CPU dual-core, 4GB RAM, 100GB penyimpanan
3. Data Uji:
   - Undangan digital dan link yang akan dienkripsi dan diuji

C. Prosedur Penelitian

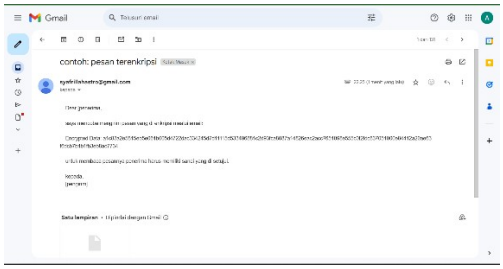
1. Instalasi dan Persiapan Lingkungan Pengujian
   - Instalasi Python dan Visual Studio Code: Unduh dan instal phyton di Python.org. dan unduh viscode di Visual Studio Code.
   - Instalasi Ekstensi Python di VS Code: Buka VS Code dan instal ekstensi Python dari Marketplace.
   - Pembuatan dan aktivasi lingkungan virtual: Buka terminal di viscode kemudian masukan code “*python -m venv env*”. akttifkan lingkungan virtual mengunakan “.\env\Scripts\activate”
   - Instalasi putaka ‘cryptography’ Berikan code “pip install cryptography” di terminal untuk menginstal.

2. Implementasi dan pengujian
   - Penerapan Teknik Enkripsi

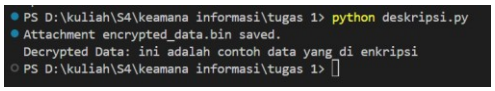
   Dalam pengujian ini, dua akun email digunakan untuk menguji efektivitas enkripsi data menggunakan algoritma AES. Pengirim (syafrillahastro@gmail.com) mengenkripsi pesan "Undangan Rapat" dengan kunci yang diturunkan dari password menggunakan algoritma AES, kemudian mengirimkan pesan terenkripsi tersebut ke penerima (abydancow@gmail.com). Penerima kemudian mendekripsi pesan yang diterima menggunakan password yang sama. Hasil pengujian menunjukkan bahwa data berhasil dienkripsi dan dikirim dengan aman melalui email, serta dapat dideskripsi oleh penerima tanpa kehilangan informasi.



Gambar 1. Pengiriman email tanpa enkripsi



Gambar 2. Pengiriman email menggunakan enkripsi



Gambar 3. mendeskrpsikan pesan yang di enkripsi

III. HASIL DAN PEMBAHASAN

A. Hasil penelitian

Hasil penelitian menunjukkan bahwa penggunaan kriptografi dalam mengamankan undangan dan link digital efektif dalam mencegah akses yang tidak sah dan serangan cyber. Enkripsi data menggunakan pustaka cryptography di Python mampu menjaga kerahasiaan dan integritas informasi yang dibagikan.

Pertukaran informasi dan data dalam proses komunikasi memerlukan tingkat keamanan dan kerahasiaan yang sangat penting. Misalnya, informasi yang disampaikan oleh pengirim kepada penerima harus tetap benar dan sesuai dengan maksud awal pengirim. Namun, ada risiko bahwa data tersebut dapat diubah oleh pihak-pihak yang tidak bertanggung jawab. Perubahan ini dapat menyebabkan kesalahpahaman antara pengirim dan penerima, serta berpotensi merugikan atau merusak reputasi pengirim pesan. Oleh karena itu, memastikan bahwa data yang dikirimkan tetap utuh dan tidak dimanipulasi selama proses komunikasi adalah aspek yang sangat krusial untuk menghindari dampak negatif tersebut.

B. Penerapan Kriptografi

Penggunaan kriptografi secara signifikan mengurangi risiko ancaman cyber. Pengujian menunjukkan bahwa data yang dienkripsi sulit untuk dipecahkan oleh serangan brute force dan tidak rentan terhadap serangan man-in-the-middle. Implementasi praktis ini juga menunjukkan bahwa langkah-langkah instalasi dan penggunaan pustaka cryptography dapat dilakukan dengan mudah oleh pengembang, meskipun ada beberapa kendala seperti kebijakan eksekusi PowerShell yang dapat diatasi dengan langkah-langkah yang sesuai.

Pengamanan informasi dan data dari kejahatan melalui teknik kriptografi saat ini sangat bermanfaat bagi para pengguna teknologi informasi. Teknik ini berfungsi melindungi data dengan cara mengenkripsinya sehingga penyadap data tidak bisa memahami isi data tersebut. Dalam kriptografi, terdapat dua proses utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses yang mengubah data asli menjadi data sandi yang sulit dipahami tanpa kunci tertentu, sementara dekripsi adalah proses mengembalikan data sandi tersebut ke bentuk aslinya.

Kriptografi telah menjadi salah satu teknik utama yang dikembangkan untuk meningkatkan keamanan data dan informasi, sehingga pengguna teknologi dapat merasa lebih aman dan nyaman. Meskipun teknik kriptografi dapat memberikan lapisan perlindungan yang kuat, upaya ini harus diimbangi dengan penguatan hukum yang mengatur kejahatan siber. Dengan demikian, pengguna, terutama dalam konteks transaksi elektronik, akan tetap terlindungi dari berbagai ancaman. Integrasi antara teknologi kriptografi dan regulasi hukum yang ketat akan memastikan keamanan dan privasi data yang lebih baik bagi masyarakat.

C. Sejarah Kriptografi

Istilah "kriptografi" berasal dari dua kata Yunani: "kripto" yang berarti menyembunyikan, dan "graphia" yang berarti tulisan. Oleh karena itu,

kriptografi adalah teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, termasuk kerahasiaan data, integritas data, autentikasi data, dan keabsahan data. Beberapa definisi kriptografi, seperti yang dijelaskan oleh Pabokory et al., menggambarkan kriptografi sebagai seni melindungi pengiriman data dengan mengubah data menjadi kode tertentu yang hanya dapat diakses dengan kunci khusus. Pada awalnya, teknologi kriptografi menggunakan metode enkripsi klasik dengan alat sederhana seperti pensil dan kertas. Metode ini terbagi menjadi dua jenis: algoritma transposisi, yang mengubah posisi huruf, dan algoritma substitusi, yang mengganti setiap huruf dengan huruf lain.

Sejak 4000 tahun yang lalu, masyarakat Mesir telah memanfaatkan bentuk hieroglif dalam bentuk kriptografi, meskipun bukan untuk menulis pesan pada saat itu. Pada zaman Romawi Kuno, Julius Caesar menggunakan teknik kriptografi untuk mengirim pesan rahasia kepada jenderalnya selama perang. Pesan tersebut dikirim melalui kurir, dan untuk menjaga kerahasiaannya dari musuh, Caesar menggunakan teknik mengacak huruf dalam pesan tersebut. Hanya jenderalnya yang memiliki cara untuk memahami pesan tersebut, yaitu dengan mengganti setiap huruf A, B, C menjadi D, E, F, dan seterusnya.

D. Tentang Cyber

Teknologi adalah hasil dari kemampuan manusia untuk merencanakan dan menciptakan objekmaterial yang bermanfaat secara praktis, seperti kendaraan bermotor, pesawat terbang, dan perangkat televisi. Pentingnya teknologi bagi masyarakat dan pemerintah sangat besar, karena teknologidigunakan dalam berbagai konteks baik yang menguntungkan maupun yang tidak. Istilah "cyber" dan "teknologi" berasal dari bahasa Yunani "Technikos", yang artinya keterampilan atau keahlian, serta "logos" yang mengacu pada prinsip- prinsip utama dalam bidang perangkat lunak. Pada era globalisasi saat ini, penggunaan yang semakin luas dari ruang cyber menghubungkan berbagai sektor kehidupan melalui jaringan internet, disesuaikan dengan tujuan masing-masing penggunaannya.

McDonnell dan Sayers mengidentifikasi tiga jenis ancaman cyber sebagai berikut:

a. Ancaman perangkat keras (hardware threat) terjadi ketika perangkat keras tertentu dipasang dalam sistem untuk mengganggu jaringan dan perangkat keras lainnya.

b. Ancaman perangkat lunak (software threat) terjadi ketika perangkat lunak tertentu dimasukkan ke dalam sistem untuk mencuri, merusak, atau memanipulasi informasi.

c. Ancaman data/informasi (data/information threat) terjadi ketika data atau informasi disebarkan dengan tujuan tertentu yang dapat membahayakan keamanan sistem.

Ancaman kejahatan cyber memiliki potensi untuk menyebabkan kerugian signifikan terhadap sistem informasi, kegiatan militer, dan infrastruktur lain yang terhubung melalui jaringan komputer dan internet. Untuk menghadapi tantangan ini, Kementerian Pertahanan (Kemhan) perlu mengembangkan kapasitas manusia yang handal dalam menguasai teknologi terkini, membangun infrastruktur yang kokoh dan dapat diandalkan, serta merumuskan kebijakan dan perundang-undangan yang mendukung dalam menjalankan operasi cyber warfare secara efektif dan efisien.

E. Ancaman Cyber

Phishing adalah praktik penipuan di mana pelaku mencoba untuk mengelabui seseorang agar memberikan informasi pribadi atau keuangan dengan cara yang menyerupai proses resmi atau sah, seringkali dengan menggunakan metode "memancing" korban. Ancaman phishing dapat berasal dari berbagai sumber, termasuk email yang mengandung tautan palsu, situs web palsu yang dirancang untuk mencuri informasi sensitif, dan perangkat lunak jahat (malware) yang menyusup ke dalam sistem korban.

Menurut hasil survei, situs web adalah salah satu sumber utama serangan phishing yang paling banyak tercatat. Untuk menghadapi ancaman ini, salah satu

pendekatan yang sering digunakan adalah meningkatkan self-efficacy, yaitu keyakinanindividu dalam mengambil langkah-langkah yang efektif untuk melindungi diri dari serangan phishing.Hal ini mencakup meningkatkan kesadaran akan taktik penipuan yang digunakan, memvalidasi keaslian situs web sebelum membagikan informasi pribadi, dan secara umum meningkatkan kewaspadaan terhadap aktivitas online yang mencurigakan. Dengan demikian, peningkatan self- efficacy dapat menjadi kunci dalam mengurangi risiko jatuh korban terhadap serangan phishing yang semakin canggih dan merugikan.

Banyak pengguna media sosial sering kali mengabaikan risiko yang mungkin timbul, menganggapnya sebagai sesuatu yang sepele dan tidak layak diperhatikan. Namun, kenyataannya adalah bahwa banyak akun media sosial telah menjadi sasaran empuk bagi penjahat cyber, terutama melalui serangan phishing. Salah satu strategi yang sering digunakan adalah penempatan tautan palsu di akun media sosial, yang disertai dengan ajakan atau iklan yang menggiurkan.

Serangan ini tidak hanya mengancam privasi pengguna, tetapi juga dapat menyebabkan kerugian finansial yang signifikan. Informasi yang dicuri dari akun media sosial dapat dieksploitasi untuk berbagai tujuan jahat, seperti pencurian dana dari rekening bank pengguna atau penggunaan rekening mereka untuk melakukan transaksi online tanpa izin. Oleh karena itu, penting bagi pengguna media sosial untuk meningkatkan kesadaran akan ancaman ini dan mengambil langkah-langkah perlindungan yang diperlukan untuk melindungi informasi pribadi mereka.

Salah satu strategi sederhana yang efektif untuk mengantisipasi serangan phishing adalah dengan tidak mengklik tautan yang berasal dari sumber yang tidak dikenal melalui akun media sosial atau email yang terhubung dengan akun tersebut. Tindakan ini penting karena tautan-tautan semacam itu sering kali merupakan upaya untuk memanipulasi pengguna dengan mengarahkan mereka ke situs web palsuyang dirancang untuk mencuri informasi pribadi atau keuangan.

Ketika pengguna menghindari mengklik tautan yang mencurigakan, mereka dapat mengurangirisiko jebakan phishing yang dapat merugikan tidakhanya mereka sendiri, tetapi juga komunitas pengguna media sosial lainnya. Selain itu, meningkatkan kesadaran akan taktik phishing dan memverifikasi sumber tautan sebelum mengambil tindakan apapun juga merupakan langkah bijak dalam menjaga keamanan online. Dengan demikian, dengan tetap waspada terhadap tautan yang tidak dikenal, pengguna dapat memastikan bahwa akun media sosial mereka tidak disalahgunakan untuk menyebarkan informasi palsu atau merugikan orang lain secara tidak sengaja.

F. Undangan Non Apk

Undangan untuk acara atau inisiatif yang bertujuan untuk mengatasi, mencegah, atau menanggulangi kejahatan cyber tanpa memfokuskan pada aplikasi atau teknologi spesifik seperti Android Package Kit (APK). Hal ini penting karena kejahatan cyber tidak hanya berkaitan dengan teknologi atau aplikasi tertentu, tetapi juga melibatkan aspek-aspek seperti keamanan informasi, kebijakan publik, kesadaran masyarakat, dan hukum. Tujuan dari undangan "non-APK" adalah untuk mengedukasi, mempersiapkan, dan membangun kesadaran tentang ancaman kejahatan cyber serta strategi pencegahannya, tanpa fokus pada teknologi atau aplikasi tertentu. Ini mencerminkan pendekatan holistik terhadap keamanan cyber yang melibatkan berbagai aspek dari masyarakat dan organisasi yang berbeda.

IV. KESIMPULAN

Penerapan kriptografi dalam menanggulangi ancaman cyber pada undangan non-aplikasi sangat efektif dalam meningkatkan keamanan dan integritas data. Dengan menggunakan enkripsi, data sensitif dalam undangan dapat dilindungi dari akses yang tidak sah dan manipulasi oleh pihak ketiga. Enkripsi tautan undangan memastikan bahwa hanya penerima yang dituju yang dapat mengakses konten undangan tersebut. Autentikasi melalui kriptografi juga memastikan identitas pengirim dan penerima, sehingga mencegah serangan rekayasa sosial dan

phishing. Selain itu, kriptografi menjaga integritas data selama transmisi, sehingga tidak ada perubahan yang dapat dilakukan tanpa terdeteksi. Penggunaan tanda tangan digital membantu memverifikasi keaslian undangan dan mencegah pemalsuan. Secara keseluruhan, penerapan kriptografi dalam undangan non-aplikasi memberikan lapisan keamanan tambahan yang sangat penting dalam melindungi privasi pengguna dan mencegah berbagai bentuk ancaman cyber.

REFERENSI

[1] M. Adam, Purwanto, *Implementasi Kriptografi Menggunakan AlgoritmE Advanced Encryption Standrard (AES-128) Berbasis Web Untuk Mengamankan File Invoice Pada PT Muara Juara Kreasi Indonesia,* SENAFTI, Vol. 3, No. 1, Jakarta, 2024.

[2] N. P. E. Merliana, *Pemanfaatan Teknologi Kriptografi Dalam Mengatasi Kejahatan Cyber,* Jurnal Ilmu Hukum, Vol. 3, No. 2, 2020.

[3] L. I. Uzlah, R. A. Saputra, Isnawaty, *Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest,* Jurnal Mahasiswa Teknik Informatika, Vol, 8, No, 3, 2024.

[4] N. B. Samantha, S. Destya, W. M. Ashari, *Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi.* Jurnal Media Informatika, Vol. 7, No. 4, 2023.

[5] F. T. Infirmasi, U. B. Luhur, K. S. Restaurant, *Pengamanan File Invoice Pada PT Mitra Teknik Menggunakan Metode Algoritma Rc4 Securing Invoice Files At PT Mitra Teknik Using The Rc4 Algorithm Method,* Vol. 2, No. 4, 2023

[6] Zaimah Panjaitan M.Kom, *ALGORITMA RC4(CONTOH PERHITUNGAN LENGKAP)*, 2024

[7] A. r. Ramadan, A. W. Prakoso, G. Dwi C, *Implementasi Kriptografi AES untuk Keamanan Pengiriman Data Internet Of Things Menggunakan WEB Service Rest,* Vol. 6, No. 1, 2021

[8] H. Wijaya, *Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan URL dari SQL Injection,* Vol. 17, No. 1, 2020

[9] A. S. Hardiansyah, Meri Hendayani, Ian Amukti Herlambang, Andhika Nove Rezki, *Implementasi Black Box Testing Pada Website,* Vol. 1, No. 1, 2022

[10] K. B. Ziliwu, *Implementasi Algoritma Kriptografi Klasik dalam Penyandian Pesan,* Batam, 2022.