ABSTRAK

KEAMANAN JARINGAN PADA WIRELESS TERHADAP SERANGAN INTRUDERS MENGGUNAKAN METODE RSA

Nama : Kevin Alfareza
NIM : 2155201112
Dosen Pembimbing : RG Guntur Alam, M.Kom. Ph. D

Pesatnya perkembangan teknologi jaringan wireless telah memberikan kemudahan dalam komunikasi serta pertukaran informasi secara cepat dan fleksibel. Meskipun demikian, karakteristik media transmisi yang bersifat terbuka menyebabkan jaringan wireless memiliki tingkat kerentanan yang tinggi terhadap berbagai ancaman keamanan, seperti penyadapan (eavesdropping) dan akses oleh pihak yang tidak berwenang (intruders). Ancaman tersebut berpotensi mengakibatkan kebocoran informasi serta mengurangi kerahasiaan data selama proses transmisi. Untuk mengatasi permasalahan tersebut, diperlukan mekanisme pengamanan yang mampu menjaga kerahasiaan informasi ketika data dikirimkan melalui jaringan. Penelitian ini bertujuan untuk mengevaluasi penerapan algoritma RSA sebagai metode kriptografi dalam meningkatkan keamanan jaringan wireless dari serangan intruders. Pendekatan penelitian yang digunakan adalah metode eksperimen (Experimental Research) dengan membangun lingkungan jaringan wireless, mengimplementasikan algoritma RSA pada proses enkripsi dan dekripsi data, kemudian melakukan simulasi serangan untuk menilai tingkat keamanan sistem. Pengujian dilaksanakan pada dua kondisi, yaitu sebelum dan setelah implementasi algoritma RSA, sehingga efektivitas metode yang diterapkan dapat dibandingkan secara objektif. Evaluasi dilakukan dengan memperhatikan beberapa indikator, meliputi kerahasiaan data (confidentiality), integritas data (integrity), kemampuan sistem dalam mencegah akses tidak sah, serta pengaruh penerapan algoritma RSA terhadap performa jaringan. Hasil penelitian diharapkan menunjukkan bahwa penggunaan algoritma RSA mampu meningkatkan tingkat keamanan jaringan wireless melalui proses transformasi data dari bentuk plaintext menjadi ciphertext. Dengan demikian, data yang berhasil diperoleh oleh pihak yang tidak berwenang tidak dapat dipahami tanpa kunci privat yang sesuai. Berdasarkan hasil tersebut, algoritma RSA dapat dijadikan sebagai salah satu alternatif solusi untuk memperkuat perlindungan data pada jaringan wireless terhadap ancaman penyadapan maupun akses yang tidak sah.

Kata kunci: Keamanan Jaringan, Wireless, Intruders, Kriptografi, RSA.

ABSTRACT

WIRELESS NETWORK SECURITY AGAINST INTRUDERS USING RSA METHOD

Name : Kevin Alfareza
Student ID : 2155201112
Supervisor : RG Guntur Alam, M.Kom. Ph. D

The rapid development of wireless network technology has provided ease in communication and exchange of information quickly and flexibly. However, the characteristics of open transmission media cause wireless networks to have a high level of vulnerability to various security threats, such as eavesdropping and access by unauthorized parties (intruders). The threat has the potential to cause information leakage and reduce data confidentiality during the transmission process. To overcome these problems, a security mechanism is needed that is able to maintain the confidentiality of information when data is transmitted over the network. This study aims to evaluate the application of RSA algorithm as a cryptographic method in improving the security of wireless networks from intruders. The research approach used is an experimental Research method by building a wireless network environment, implementing the RSA algorithm in the process of encryption and decryption of data, then perform a simulation attack to assess the level of system security. The tests were carried out in two conditions, before and after the implementation of the RSA algorithm, so that the effectiveness of the applied methods can be objectively compared. The evaluation was conducted by taking into account several indicators, including data confidentiality, data integrity, the ability of the system to prevent unauthorized access, and the effect of the application of the RSA algorithm on network performance. The results are expected to show that the use of RSA algorithm is able to increase the level of wireless network security through the process of data transformation from plaintext to ciphertext. Thus, the data successfully obtained by unauthorized parties cannot be understood without the corresponding private key. Based on these results, the RSA algorithm can be used as an alternative solution to strengthen data protection on wireless networks against the threat of eavesdropping and unauthorized access.

Keywords: Network Security, Wireless, Intruders, cryptography, RSA.

BAB I
PENDAHULUAN

1.1. latar belakang

Kemajuan teknologi informasi dan komunikasi telah mendorong terjadinya berbagai perubahan dalam kehidupan masyarakat, khususnya dalam cara memperoleh dan bertukar informasi. Salah satu teknologi yang berkembang pesat adalah jaringan nirkabel (*wireless*), yaitu teknologi komunikasi yang memungkinkan perangkat terhubung ke jaringan internet tanpa memerlukan media kabel sebagai penghubung. (Alodat, 2022). Jaringan wireless banyak digunakan di berbagai tempat, seperti rumah, sekolah, kampus, perkantoran, hingga tempat umum karena memberikan kemudahan dalam mengakses informasi dan berkomunikasi (Hamdi Putra, 2025)

Meskipun memiliki banyak kelebihan, penggunaan jaringan *wireless* juga memiliki berbagai risiko keamanan . Data yang dikirim melalui jaringan *wireless* dapat menjadi sasaran pihak yang tidak bertanggung jawab. Salah satu ancaman yang sering terjadi adalah adanya intruders, yaitu pihak yang mencoba masuk ke dalam jaringan tanpa izin untuk mengakses, mencuri, mengubah, atau merusak data yang ada. Kondisi ini dapat menyebabkan kerugian bagi pengguna maupun pengelola jaringan, terutama jika data yang disalahgunakan bersifat penting dan rahasia (PINONTOAN, 2024).

Keamanan jaringan menjadi aspek yang sangat penting untuk diperhatikan guna melindungi data dan informasi dari berbagai ancaman. Salah satu cara yang dapat digunakan untuk meningkatkan keamanan jaringan adalah dengan menerapkan teknologi kriptografi (Rafael et al., 2025). Kriptografi merupakan

teknik yang digunakan untuk mengamankan data dengan cara mengubah informasi asli menjadi bentuk yang sulit dipahami oleh pihak yang tidak memiliki hak akses (Selvi et al., 2025).

Salah satu algoritma kriptografi yang banyak digunakan adalah RSA *(Rivest-Shamir-Adleman).* RSA merupakan algoritma kriptografi asimetris yang menggunakan dua kunci, yaitu kunci publik untuk proses *enkripsi* dan kunci privat untuk proses dekripsi (Mulyanto et al., 2022). Dengan metode ini, data yang dikirim melalui jaringan wireless dapat dienkripsi terlebih dahulu sehingga tidak dapat dibaca oleh pihak yang melakukan penyadapan atau akses tanpa izin (Walle, 2024).

Berdasarkan permasalahan tersebut, penelitian ini dilakukan untuk mengkaji penerapan metode RSA dalam meningkatkan keamanan jaringan *wireless* terhadap ancaman intruders. Dengan adanya penulisan ini diharapkan dapat mengetahui sejauh mana algoritma RSA mampu melindungi data yang dikirimkan melalui jaringan *wireless* sehingga keamanan dan kerahasiaan informasi dapat lebih terjamin (Yogesh Suryawanshi, 2023).

Dengan ini, diharapkan dapat memberikan manfaat bagi pengguna jaringan wireless dalam memahami pentingnya keamanan data serta menjadi referensi bagi pengembangan sistem keamanan jaringan yang lebih baik lagi.

1.2rumusan masalah

Bagaimana efektivitas algoritma RSA dalam melindungi data pada jaringan *wireless* dari serangan *intruders?*

1.3 Batasan masalah

1) Penelitian difokuskan pada penerapan algoritma RSA sebagai metode kriptografi untuk meningkatkan keamanan data pada jaringan wireless
2) Jaringan yang digunakan dalam penelitian adalah jaringan Wireless Local Area Network (WLAN) sebagai media transmisi data.
3) Ancaman keamanan yang dibahas dalam penelitian ini dibatasi pada serangan yang dilakukan oleh *intruders*, khususnya berupa penyadapan data *(eavesdropping)* atau penangkapan paket data *(packet sniffing)* selama proses transmisi.
4) Aspek keamanan yang dianalisis dalam penelitian meliputi kerahasiaan data *(confidentiality)*, integritas data *(integrity),* dan kemampuan sistem dalam mencegah akses tidak sah oleh *intruders.*

1.4 tujuan penelitian

1) Mengimplementasikan algoritma RSA pada sistem keamanan jaringan *wireless* sebagai mekanisme untuk melindungi data dari serangan *intruders.*
2) Menganalisis efektivitas algoritma RSA dalam meningkatkan keamanan data yang ditransmisikan melalui jaringan *wireless* terhadap serangan *intruders.*
3) Membandingkan tingkat keamanan jaringan *wireless* sebelum dan sesudah penerapan algoritma RSA berdasarkan aspek kerahasiaan data *(confidentiality),* integritas data *(integrity),* serta kemampuan sistem dalam mencegah akses tidak sah.

4) Mengevaluasi pengaruh penerapan algoritma RSA terhadap kinerja sistem selama proses transmisi data pada jaringan *wireless.*

1.5 manfaat penelitian

1) Melalui penulisan ini diharapkan dapat memberikan pemahaman kepada pengguna terhadap pentingnya menjaga keamanan data pada jaringan *wireless* serta memberikan informasi tentang penerapan algoritma RSA sebagai salah satu metode untuk melindungi data dari akses tidak sah dan penyadapan oleh *intruders.*

2) kemudian dapat menjadi acuan dalam penerapan sistem keamanan jaringan *wireless* sehingga dapat membantu meningkatkan perlindungan terhadap data dan informasi yang ditransmisikan melalui jaringan.

3) Selanjutnya diharapkan dapat menambah pengetahuan dan pengalaman dalam mengimplementasikan algoritma RSA pada sistem keamanan jaringan *wireless* serta memahami proses pengujian keamanan terhadap serangan *intruders.* Selain itu, penelitian ini dapat menjadi sarana untuk mengembangkan kemampuan dalam bidang keamanan jaringan dan kriptografi.