# ANALISIS KRIPTOGRAFI RIVEST-SHAMIR-ADLEMAN PADA JARINGAN SENSOR NIRKABEL DENGAN METODE CLIENT-SERVER DAN SOCKET PROGRAMMING

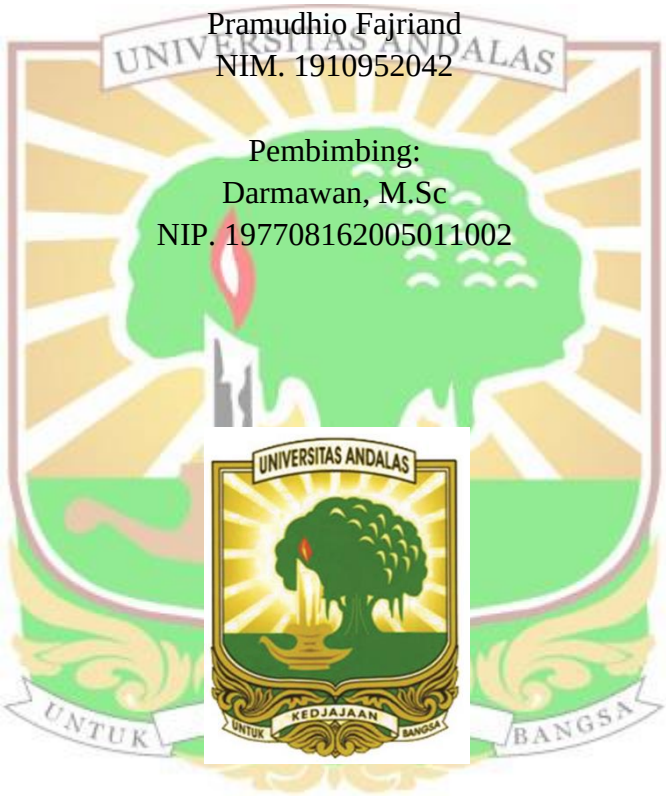
**TUGAS AKHIR**

Karya Ilmiah sebagai salah satu syarat untuk menyelesaikan jenjang Strata Satu (S-1) di Departemen Teknik Elektro, Fakultas Teknik, Universitas Andalas


Oleh:

Pramudhio Fajriand
NIM. 1910952042

Pembimbing:
Darmawan, M.Sc
NIP. 197708162005011002


**Program Studi Sarjana**
**Teknik Elektro Fakultas Teknik**
**Universitas Andalas**
**2023**

| Judul | Analisis Kriptografi Rivest-Shamir-Adleman pada Jaringan Sensor Nirkabel dengan Metode *Client*-Server dan *Socket Programming* | Pramudhio Fajriand |
|---|---|---|
| Program Studi | Teknik Elektro | 1910952042 |
| Fakultas Teknik Universitas Andalas | | |


Abstrak

Perkembangan teknologi komunikasi pada aplikasi *Internet of Things* (IoT) yang digunakan pada setiap lini kehidupan mempermudah kehidupan dengan otomatisasinya. Perkembangan teknologi komunikasi sejalan dengan ancaman pada komunikasi data yang terjadi pada IoT. Salah satu langkah antisipasi serangan pada komunikasi data adalah menggunakan kriptografi. Kriptografi berperan untuk mengamankan data yang dikirim pada komunikasi data, sehingga apabila data diperoleh oleh pihak ketiga, data yang diperoleh akan berupa data hasil enkripsi. Proses kriptografi menggunakan langkah ekstra untuk mengamankan data dan dapat berpengaruh pada *QoS (Quality of Service)* jaringan. Maka dilakukan analisis pengaruh kriptografi Rivest-Shamir-Adleman (RSA) kepada jaringan sensor nirkabel untuk mendeteksi gerak benda menggunakan metode *client-server* dan *socket programming*. Penelitian ini melakukan pengujian pada dua jenis protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) menggunakan transkripsi RSA dan tanpa transkripsi dengan parameter yang dibandingkan adalah nilai QoS *throughput* dan *delay*. Pada pengujian dengan transkripsi protokol TCP didapatkan *throughput* sebesar 46,632 Kbps dan *delay* sebesar 22,7 ms. Pada protokol UDP didapatkan *throughput* sebesar 114,605 Kbps dan *delay* sebesar 20,9 ms. Untuk pengujian tanpa transkripsi protokol TCP didapatkan *throughput* sebesar 34,25 Kbps dan *delay* sebesar 20,9 ms. Pada protokol UDP didapatkan *throughput* sebesar 152,42 Kbps dan *delay* sebesar 3,61 ms. Nilai *delay* pada protokol TCP dan UDP dengan transkripsi lebih lama karena ada algoritma tambahan yang dieksekusi untuk melakukan pembuatan dan distribusi *key* serta proses enkripsi dan dekripsi pesan yang menambah beban pada sisi *client* dan server. Nilai *throughput* pada protokol TCP lebih besar untuk komunikasi dengan transkripsi karena peningkatan *delay* tidak lebih besar dibanding peningkatan ukuran tiap *packet* yang dikirimkan pada komunikasi data. Peningkatan nilai *throughput* tidak serta merta membuat kualitas komunikasi data lebih baik, karena pada kasus ini banyak *packet* per detik yang dikirimkan lebih sedikit

untuk komunikasi yang menggunakan transkripsi dengan 44,02 paket per detik pada protokol TCP dan 48,08 paket per detik pada protokol UDP dibanding tanpa transkripsi dengan 49,56 paket per detik pada protokol TCP dan 68,8 paket per detik pada protokol UDP.

Kata kunci: *IoT (Internet of Things), kriptografi, QoS (Quality of Service), Rivest-Shamir-Adleman, socket programming, TCP (Transmission Control Protocol), UDP (User Datagram Protocol).*

| | | |
|---|---|---|
| *Title* | *Rivest-Shamir-Adleman Cryptographic Analysis on Wireless Sensor Networks Using Client-Server and Socket Programming Methods* | Pramudhio Fajriand |
| *Mayor* | *Electrical Engineering Department* | 1910952042 |
| *Engineering Faculty of Andalas University* | | |


Abstract

*The rapid advancement of communication technology in Internet of Things (IoT) applications, integrated into various aspects of daily life, has significantly streamlined processes through automation. However, this technological progress has also brought forth challenges, particularly concerning data communication security within IoT. To address these challenges, the use of cryptography has emerged as a fundamental security measurement. Cryptography plays a pivotal role in safeguarding transmitted data, rendering it unintelligible to unauthorized parties. Yet, the cryptographic process introduces additional computational steps, potentially impacting the Quality of Service (QoS) in network communication. Thus, this study conducts a comprehensive analysis of the influence of Rivest-Shamir-Adleman (RSA) cryptography on wireless sensor networks tasked with object motion detection, employing the client-server method and socket programming. The research encompasses assessments of two prominent communication protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), both with and without RSA encryption, with QoS parameters including throughput and delay under scrutiny. With RSA encryption, the TCP protocol exhibited a throughput of 46.632 Kbps and a delay of 22.7 ms, whereas the UDP protocol demonstrated a throughput of 114.605 and a delay of 20.9. In contrast, without encryption, the TCP protocol achieved a throughput of 34.25 and a delay of 20.9, while the UDP protocol yielded a throughput of 152.42 and a delay of 3.61. The prolonged delay values observed in both TCP and UDP protocols with encryption stem from the execution of additional cryptographic algorithms, encompassing key generation, distribution, and message encryption and decryption, thereby augmenting the computational load on both client and server sides. Although encrypted communication through the TCP protocol featured enhanced throughput, this did not necessarily correspond to superior data communication quality. This was chiefly attributed to the lower number of packets transmitted per second in encrypted communication, totaling 44.02 packets per second for the TCP protocol and 48.08 packets per second for the UDP protocol, in contrast to*

*unencrypted communication, which achieved 49.56 packets per second for the TCP protocol and 68.8 packets per second for the UDP protocol.*

*Keywords*: *IoT (Internet of Things), kriptografi, QoS (Quality of Service), Rivest-Shamir-Adleman, socket programming, TCP (Transmission Control Protocol), UDP (User Datagram Protocol).*