

PERBANDINGAN METODE ELLIPTIC CURVE CRYPTOGRAPHY DAN RIVEST SHAMIR ADLEMAN (RSA) PADA SISTEM DATA SECURITY E-HEALTH PRAKTIK MANDIRI BIDAN

Archi Rafif Nevandya

Teknik Informatika

Network and Cyber Security

Pembimbing :

Maya Hilda Lestari Louk, M.Sc.

Fitri Dwi Kartikasari, M.Si.

ABSTRAK

Penelitian ini bertujuan untuk membandingkan keefektifan metode *Elliptic Curve Cryptography* (ECC) dan *Rivest Shamir Adleman* (RSA) dalam menjaga keamanan data pada sistem *E-Health* Praktik Mandiri Bidan. ECC memanfaatkan sifat-sifat kurva eliptik untuk menghasilkan kunci yang pendek namun kuat, sementara RSA menggunakan operasi matematika pada angka besar. Perbandingan dilakukan dengan mempertimbangkan aspek keamanan, efisiensi, dan skalabilitas dalam konteks *E-Health* Praktik Mandiri Bidan, yang melibatkan pertukaran informasi sensitif antara pasien dan bidan. Selain itu, penelitian ini juga mengamati dampak penggunaan kedua metode terhadap kinerja sistem dan kecepatan proses enkripsi-dekripsi. Hasil penelitian ini diharapkan dapat memberikan panduan yang lebih baik dalam memilih metode kriptografi yang paling sesuai untuk melindungi data sensitif dalam sistem tersebut, sekaligus menawarkan wawasan tambahan terkait efisiensi operasional dan kinerja sistem secara keseluruhan..

Kata Kunci: *Elliptic Curve Cryptography* (ECC), *Rivest Shamir Adleman* (RSA), *E-Health*, keamanan data, sistem praktik mandiri bidan, efisiensi kriptografi, skalabilitas.

COMPARISON OF ELLIPTIC CURVE CRYPTOGRAPHY AND RIVEST SHAMIR ADLEMAN (RSA) METHODS IN INDEPENDENT MIDDLE PRACTICE E-HEALTH SECURITY DATA SYSTEMS

Archi Rafif Nevandya

Information Technology

Network and Cyber Security

Supervisor :

Maya Hilda Lestari Louk, M.Sc.

Fitri Dwi Kartikasari, M.Si.

ABSTRACT

This research aims to compare the effectiveness of the Elliptic Curve Cryptography (ECC) and Rivest Shamir Adleman (RSA) methods in maintaining data security in the Independent Midwife Practice E-Health system. ECC exploits the properties of elliptic curves to generate short but strong keys, while RSA uses mathematical operations on large numbers. The comparison was carried out by considering aspects of security, efficiency, and scalability in the context of Midwife Independent Practice E-Health, which involves exchanging sensitive information between patients and midwives. Apart from that, this research also observed the impact of using both methods on system performance and the speed of the encryption-decryption process. The results of this research will provide better guidance in selecting the most appropriate cryptographic method to protect sensitive data in such systems, while also offering additional insights regarding operational efficiency and overall system performance.

Keywords: Elliptic Curve Cryptography (ECC), Rivest Shamir Adleman (RSA), E-Health, data security, midwife independent practice system, cryptographic efficiency, scalability.