KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah swt. karena berkat rahmat dan hidayah-Nya penyusunan laporan Tugas Akhir dengan judul "Integrasi OpenSSL dan AES-256 untuk Meningkatkan Keamanan Transmisi Data" dapat diselesaikan sebagai syarat untuk menyelesaikan Program Sarjana (S1) pada Program Sarjana Fakultas Teknik Jurusan Informatika Universitas Siliwangi.

Penulis menyadari bahwa selama penyusunan laporan ini banyak mendapat dukungan dan motivasi dari berbagai pihak. Oleh sebab itu, penulis mengucapkan terima kasih kepada:

1. Prof. Dr. Rudi Priyadi, Ir., M.S. selaku Rektor Universitas Siliwangi.
2. Prof. Dr. Eng. H. Aripin selaku Dekan Fakultas Teknik Universitas Siliwangi.
3. Nur Widyasono, M.Kom., CEH, CHFI selaku Ketua Jurusan Informatika Universitas Siliwangi sekaligus Pembimbing yang telah memberikan motivasi, nasihat, arahan, dan bimbingan yang membuat penulis lebih teliti dan lebih baik dalam melaksanakan Tugas Akhir.
4. Rohmat Gunawan, S.T., M.T. selaku Pembimbing yang telah memberikan motivasi, nasihat, arahan, dan bimbingan yang membuat penulis lebih teliti dan lebih baik dalam melaksanakan Tugas Akhir.
5. Cecep Muhamad Sidik R., S.T., M.T. selaku Dosen Wali yang telah memberikan motivasi, nasihat, arahan, dan bimbingan yang membuat penulis lebih teliti dan lebih baik dalam melaksanakan Tugas Akhir.
6. Rekan-rekan seperjuangan Informatika Universitas Siliwangi yang telah memotivasi untuk menyelesaikan penyusunan laporan ini.

7. Semua pihak yang terkait dan berjasa dalam proses pelaksanaan maupun penulisan laporan yang tidak bisa penulis sebutkan satu persatu.

Penulis menyadari masih memiliki banyak kekurangan, baik dalam hal isi maupun sistematika dan teknik penulisannya. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran yang membangun kesempurnaan laporan ini, serta tanggapan positif yang dapat menyempurnakan penyusunan laporan kegiatan. Semoga laporan ini bisa memberikan manfaat bagi semua pihak.

Tasikmalaya, Agustus 2021

Penulis

DAFTAR ISI

PENGESAHAN i
PENGESAHAN PENGUJI ii
LEMBAR PERNYATAAN KEASLIAN iii
ABSTRAK iv
ABSTRACT v
HALAMAN PERSEMBAHAN DAN MOTO vi
KATA PENGANTAR vii
DAFTAR ISI ix
DAFTAR TABEL x
DAFTAR SOURCE CODE xii
DAFTAR GAMBAR xiii
BAB I PENDAHULUAN I-1
1.1. Latar Belakang I-1
1.2. Rumusan Masalah I-3
1.3. Tujuan Penelitian I-3
1.4. Manfaat Penelitian I-3
1.5. Batasan Masalah I-4
BAB II TINJAUAN PUSTAKA II-1
2.1. Landasan Teori II-1
2.2. Penelitian Terkait dan Kebaruan Penelitian II-10
BAB III METODOLOGI PENELITIAN III-1
3.1. Metode Penelitian III-1
3.2. Tahap Penelitian III-3
BAB IV HASIL DAN PEMBAHASAN IV-1
4.1. Implementasi IV-1
4.2. Pengujian IV-6
BAB V KESIMPULAN DAN SARAN V-1
5.1. Kesimpulan V-1
5.2. Saran V-1
DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 2.1 State of The Art Advanced Encryption Standard II-10

Tabel 2.2 Lanjutan Tabel 2.1 ..... II-11

Tabel 2.3 Lanjutan Tabel 2.1 ..... II-12

Tabel 4.1 Spesifikasi hardware Windows 10 ..... IV-1

Tabel 4.2 Spesifikasi hardware OS Linux IV-1

Tabel 4.3 Spesifikasi hardware Mikrotik IV-1

Tabel 4.4 Waktu enkripsi pada beberapa jenis file IV-6

Tabel 4.5 Lanjutan tabel 4.4 ..... IV-7

Tabel 4.6 Waktu dekripsi pada beberapa jenis file IV-7

Tabel 4.7 Waktu transmisi pada file yang sudah dienkripsi IV-9

Tabel 4.8 Waktu transmisi pada file tanpa enkripsi IV-9

Tabel 4.9 Perbedaan ukuran file IV-10

Tabel 4.10 Perbedaan waktu transmisi IV-10

Tabel 4.11 Lanjutan tabel 4.10 ..... IV-11

Tabel 4.12 Entropy shannon file original IV-13

Tabel 4.13 Entropy shannon enkripsi AES-256 jenis hexa IV-13

Tabel 4.14 Lanjutan Tabel 4.13 ..... IV-14

Tabel 4.15 Entropy shannon enkripsi OpenSSL jenis hexa IV-14

Tabel 4.16 Entropy shannon enkripsi AES-256 dan OpenSSL jenis hexa IV-15

Tabel 4.17 Entropy shannon enkripsi AES-256 jenis binary IV-15

Tabel 4.18 Lanjutan Tabel 4.17 ..... IV-16

Tabel 4.19 Entropy shannon enkripsi OpenSSL jenis binary IV-16

Tabel 4.20 Entropy shannon enkripsi AES-256 dan OpenSSL jenis binary....IV-17

DAFTAR SOURCE CODE

Source Code 3.1 Tampilan aplikasi III-7

Source Code 3.2 Lanjutan Source Code 3.1..... III-8

Source Code 3.3 File proses.php III-9

Source Code 3.4 Lanjutan Source Code 3.3..... III-9

Source Code 3.5 File enkripsi.php..... III-10

Source Code 3.6 Lanjutan Source Code 3.5..... III-10

Source Code 3.7 Lanjutan Source Code 3.5..... III-11

Source Code 3.8 Proses pengujian waktu III-13

DAFTAR GAMBAR

Gambar 2.1 Transformasi SubBytes II-2

Gambar 2.2 Transformasi ShiftRows II-2

Gambar 2.3 Transformasi MixColumns II-3

Gambar 2.4 Transformasi AddRoundKey II-4

Gambar 2.5 Enkripsi mode ECB II-5

Gambar 2.6 Dekripsi mode ECB II-5

Gambar 2.7 Enkripsi mode CBC II-5

Gambar 2.8 Dekripsi mode CBC II-6

Gambar 2.9 Enkripsi mode CFB II-6

Gambar 2.10 Dekripsi mode CFB II-6

Gambar 2.11 Enkripsi mode OFB II-7

Gambar 2.12 Dekripsi mode OFB II-7

Gambar 2.13 Enkripsi mode CTR II-8

Gambar 2.14 Dekripsi mode CTR II-8

Gambar 2.15 Rumus entropy shannon II-9

Gambar 3.1 Proses enkripsi III-1

Gambar 3.2 Proses dekripsi III-2

Gambar 3.3 Tahap penelitian III-3

Gambar 3.4 Tampilan aplikasi III-7

Gambar 3.5 Tampilan website tools entropy III-13

Gambar 4.1 Arsitektur jaringan IV-2

Gambar 4.2 Tampilan aplikasi.....IV-2
Gambar 4.3 File png yang tidak dienkripsi.....IV-3
Gambar 4.4 File png terenkripsi AES-256 jenis Hexa.....IV-3
Gambar 4.5 File png terenkripsi AES-256 jenis Binary.....IV-4
Gambar 4.6 File png terenkripsi OpenSSL jenis Hexa.....IV-4
Gambar 4.7 File png terenkripsi OpenSSL jenis Binary.....IV-5
Gambar 4.8 File png terenkripsi AES-256 dan OpenSSL jenis Hexa.....IV-5
Gambar 4.9 File png terenkripsi AES-256 dan OpenSSL jenis Binary.....IV-6
Gambar 4.10 File png yang sudah terenkripsi.....IV-8
Gambar 4.11 JSON Original.....IV-11
Gambar 4.12 Proses pengubahan data.....IV-11
Gambar 4.13 Hasil dari server.....IV-12
Gambar 4.14 JSON terenkripsi.....IV-12
Gambar 4.15 Hasil dari server.....IV-12