BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari implementasi algoritma Diffie-Hellman, AES-128 dan ECDSA pada sistem pengamanan aplikasi *instant messaging* adalah:

1. Pengenkripsian dan pendekripsian pesan pada *mobile instant messaging* dilakukan sebagai berikut:

   Algoritma AES-128 digunakan pada proses enkripsi pesan, menghasilkan pesan rahasia atau *ciphertext* dalam bentuk blok biner berukuran 128 bit, dan algoritma Diffie-Hellman digunakan untuk menghasilkan kunci cipher atau *cipherkey* dalam bentuk format blok biner 128 bit. Selain itu, algoritma ECDSA digunakan untuk membuat tanda tangan digital dengan ukuran 256 bit. Dari gabungan ketiga algoritma yang dibuat, enkripsi pesan menghasilkan pesan berbentuk acak sehingga isi pesan asli yang dikirimkan tidak dapat dilihat oleh pihak lain selain pengirim dan penerima pesan.

   Pada proses dekripsi, tanda tangan digital pesan yang telah digenerasi algoritma ECDSA akan diverifikasi keasliannya. Setelah tanda tangan digital diverifikasi keasliannya, penerima mengambil *cipherkey* yang sebelumnya sudah digenerasi dengan algoritma Diffie-Hellman. Selanjutnya kunci tersebut digunakan untuk melakukan dekripsi *ciphertext* menjadi pesan sebenarnya menggunakan algoritma AES-128. Hasil dari proses dekripsi *ciphertext* akan menampilkan pesan asli yang dikirim oleh pengirim pesan, sehingga penerima pesan dapat mengetahui maksud pesan yang diterimanya.

2. Pengaruh penggabungan algoritma Diffie-Hellman, AES-128, dan ECDSA pada sistem keamanan pesan *mobile instant messaging* yang meliputi kerahasiaan, integritas data, autentikasi dan non-penyangkalan sebagai berikut:

   Pengujian proses enkripsi pada 10 data pesan menghasilkan 100% pesan acak pada *ciphertext* sehingga proses dekripsi dapat dilakukan. Pengujian dekripsi pesan dengan memodifikasi 1 bit *ciphertext* memperoleh hasil 100%

pesan acak. Modifikasi 1 bit *ciphertext* memperoleh 100% pesan tetap acak. Hasil ketiga pengujian yang dilakukan, menunjukkan bahwa hasil yang diperoleh memiliki nilai di atas 50% sehingga memenuhi kerahasiaan dan integritas data. Ini berarti algoritma AES-128 dapat digunakan dalam menjaga kerahasiaan dan integritas data pesan yang dikirim pada proses pengiriman pesan.

Pada pengujian yang dilakukan dengan menggunakan kunci yang berbeda pada proses dekripsi terhadap 10 data pesan didapat hasil 100% hasil tidak ada yang sesuai dengan isi *plaintext* asli. Sehingga penggunaan algoritma Diffie-Hellman pada pertukaran kunci AES-128 dapat menjaga integritas data. Hal ini menunjukkan aspek integritas data pada implementasi pengiriman pesan dengan menggunakan algoritma AES-128 dengan Diffie-Hellman terpenuhi.

Pengujian autentikasi dilakukan terhadap 10 pesan yang dikirim menunjukkan hasil validasi 100% dikirim dari pengirim asli. Hal ini menunjukkan, penggunaan algoritma ECDSA pada pengiriman pesan memenuhi tujuan kriptografi yaitu autentikasi dan nir-penyangkalan.

Selanjutnya adalah pengujian keamanan dengan metode *Brute Force*. Hasil menunjukkan bahwa penyerang melakukan 200.000 serangan dalam waktu 0.0014 ms. Banyaknya usaha yang dilakukan penyerang di bawah 1 detik mengindikasikan bahwa penyerang sulit untuk membobol sistem keamanan yang telah dibuat. Oleh karena itu pada proses pengujian ini dapat dinyatakan bahwa gabungan algoritma Diffie-Hellman, AES-128 dan ECDSA dapat menjaga keamanan aplikasi *instant messaging*.

Berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan pengaplikasian ketiga algoritma kriptografi, yaitu algoritma Diffie-Hellman, algoritma AES-128, dan algoritma ECDSA berpengaruh pada sistem pengamanan aplikasi *instant messaging* berupa kerahasiaan, integritas data, autentikasi dan non-penyangkalan. Sehingga, pengaplikasian algoritma Diffie-Hellman, algoritma AES-128, dan algoritma ECDSA dapat memenuhi kerahasiaan, integritas data, autentikasi dan non-penyangkalan.

3. Pengujian ketiga dilakukan untuk melihat berapa banyak data yang dapat ditransfer dalam waktu tertentu (*throughput*) pada proses enkripsi dan dekripsi. Pada pengujian proses waktu untuk enkripsi dan dekripsi, didapatkan rata-rata kecepatan proses enkripsi yaitu sebesar 43540,375 bit/detik. Sedangkan, untuk proses dekripsi memiliki rata-rata kecepatan proses dekripsi sebesar 1251,705 bit/detik. Hal ini menunjukkan bahwa *throughput* dari proses dekripsi lebih lambat dibandingkan dengan proses enkripsi, dan proses dekripsi secara keseluruhan mengalami kenaikan waktu sejalan dengan semakin panjangnya bit, walaupun pada kenaikan tersebut terjadi fluktuatif dalam waktu proses dekripsi.

5.2 Saran

1. Penelitian implementasi algoritma Diffie-Hellman, AES-128 dan ECDSA pada pengamanan aplikasi *instant messaging* hanya berfokus pada pengamanan percakapan dalam berbentuk teks saja. Oleh karena itu, untuk penelitian lanjutan dapat dikembangkan pada pengamanan pengiriman dokumen (gambar, video, dokumen), panggilan audio atau video.
2. Pada penelitian ini, sistem pertukaran kunci yang digunakan adalah algoritma Diffie-Hellman. Pada penelitian lanjutan pertukaran kunci bisa menggunakan algoritma lain, misalnya menggunakan algoritma ECDH.