BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan beberapa hal sebagai berikut :

1. Metode kombinasi enkripsi AES-256 dan RSA bekerja dengan penggunaan *library Openssl* yakni dengan melakukan proses enkripsi terhadap AES-256 dengan format blok CBC terlebih dahulu dengan menentukan panjang iv (*initialization vector*) dan *key* serta pembacaan *plaintext* melalui input data dari proses *Create* atau *Update* dengan hasil berupa *ciphertext* dari AES-256. *Ciphertext* dari AES-256 ini kemudian diproses kembali sebagai *plaintext* untuk enkripsi RSA. Inisiasi dilakukan terlebih dahulu untuk *generate public key* dan *private key* menggunakan perintah OpenSSL via *command prompt*. Enkripsi kemudian melibatkan hasil enkripsi AES beserta dengan *public key*. Hasil enkripsi RSA tersebut kemudian tersimpan pada *database* sistem dengan format data biner dan tipe data "blob" pada PHPMyAdmin.
2. Hasil serangan *SQL Injection* menunjukkan *output* jika enkripsi dua tahap menggunakan AES-256 CBC dan RSA dapat diimplementasikan pada sistem. Proses *dumping* data menunjukkan hasil data *ciphertext* RSA dengan format biner pada kolom dimana enkripsi dua tahap dipasang yaitu kolom "credit" dan "phone" dimana kedua kolom tersebut berisikan data nomor kartu kredit dan nomor telepon pada sistem.
3. Hasil akhir dari penelitian menunjukan jika kombinasi AES-256 dan RSA dapat mengamankan data pada *database*. Hal tersebut ditunjang dengan hasil pada poin sebelumnya dimana data pada kolom "credit" dan "phone" muncul dalam bentuk biner yang sulit terbaca dimana kedua kolom tersebut merupakan kolom dimana enkripsi dua tahap AES-256 dan RSA diterapkan.

5.2 Saran

Penelitian ini masih jauh dari kata sempurna dan masih memiliki banyak kekurangan. Kekurangan tersebut diantaranya adalah sistem yang masih sangat

sederhana. Selain itu, peneliti harus membuka parameter *SQL Syntax* pada tautan agar dapat melakukan pengujian pada sistem. Berikut adalah beberapa saran yang bisa penulis berikan diantaranya :

1. Perbaikan sistem secara keseluruhan dimana banyak aspek yang dapat ditingkatkan seperti penerapan *framework* (*Laravel*, *Code Igniter* dan lain-lain). Selain itu, sistem sangat rentan apabila terkena serangan direktori atau *folder* seperti Google *Dork* dimana peneliti menyimpan *public key* dan *private key* langsung pada hierarki yang sama dengan berkas web yang lain (index.php, function.php dan lain-lain).
2. Pengujian menggunakan sistem *database* yang berbeda seperti Oracle, PostgreSQL ataupun Microsoft SQL Server. Selain itu, dapat juga diimplementasikan menggunakan tipe kombinasi enkripsi yang berbeda, baik dari sisi jumlah kombinasi (kombinasi dari 2 enkripsi atau lebih) atau dari jenis enkripsi yang digunakan (contohnya kombinasi simestris dengan simetris, asimetris dengan asimetris atau hash dengan asimetris dan masih banyak lagi).
3. Pengalokasian *user* khusus untuk *database* tertentu agar *database* lain yang terhubung dengan domain utama tidak ikut ter-*dumping* ketika *subdomain* menerima serangan *SQL Injection*.
4. Diharapkan kedepannya penelitian ini dapat bermanfaat bagi para pembaca dan dapat menjadi referensi untuk penelitian berikutnya yang lebih baik lagi.