BAB III

METODOLOGI PENELITIAN

3.2.1 Objek dan Subjek Penelitian

3.1.1 Objek Penelitian

Untuk objek Penelitiannya yaitu system keamanan *database*. Dalam system yang dirancang akan diterapkan method kombinasi kriptografi *Merkle-hellman Knapsack* dan Advanced *Encryption* Standard sebagai pengamanan *database*. System yang dirancang menggunakan PHP, CSS dan *database* dalam perancangan system ini.

3.1.2 Subjek Penelitian

Penelitian ini memeiliki subjeck penelitian yaitu system yang dirancang dengan berbasis web dengan keamanan login dengan methode kriptografi. Methode kriptografi nantinya akan dilengkapi dengan methode *Merkle-hellman Knapsack* dan *Data Encription Standard*. Alat dan bahan yang nantinya akan digunakan salah satunya adalah *web hosting*.

3.2.2 Alat dan Bahan

Dalam penelitian ini peneliti memiliki alat serta bahan sebagai berikut:

3.3.2.1 Alat Penelitian

Penelitian ini membutuhkan sebuah alat penelitian berupa web hosting dan juga computer penyerang dengan spesifikasi:

1. Spesifikasi web hosting

Spesifikasi Web Hosting yang digunakan adalah sebagai berikut :

Tabel 3.1 Spesifikasi Web Hosting

No.	Aspek	Spesifikasi
1.	Vendor	Nusantara Host
2.	Penyimpanan	12 GB NVMe SSD

No.	Aspek	Spesifikasi
3.	RAM	6 GB
4.	*Processor*	2 Core CPU @2Ghz
5.	Domain	Gratis
6.	*Bandwidth*	*Unlimited*
7.	Kontrol Panel	Plesk
8.	Server Basis Data	MariaDB
9.	Jenis Basis Data	MySQL
10.	Tautan Terdaftar	aziznative.skirpsidimasgum.my.id

2. Spesifikasi computer penyerang

Penyerang memiliki spesifikasi computer sebagai berikut yaitu :

Tabel 3.2 Spesifikasi perangkat tester

No.	**Aspek**	**Spesifikasi/Keterangan**
1.	Merek	HP
2.	Tipe Perangkat	HP 14
3.	RAM	4 GB
4.	Prosesor	Intel Celeron
5.	Penyimpanan	500 gb
6.	Sistem Operasi	Kali Linux 2022
7.	Aplikasi *Tester*	SQL Map

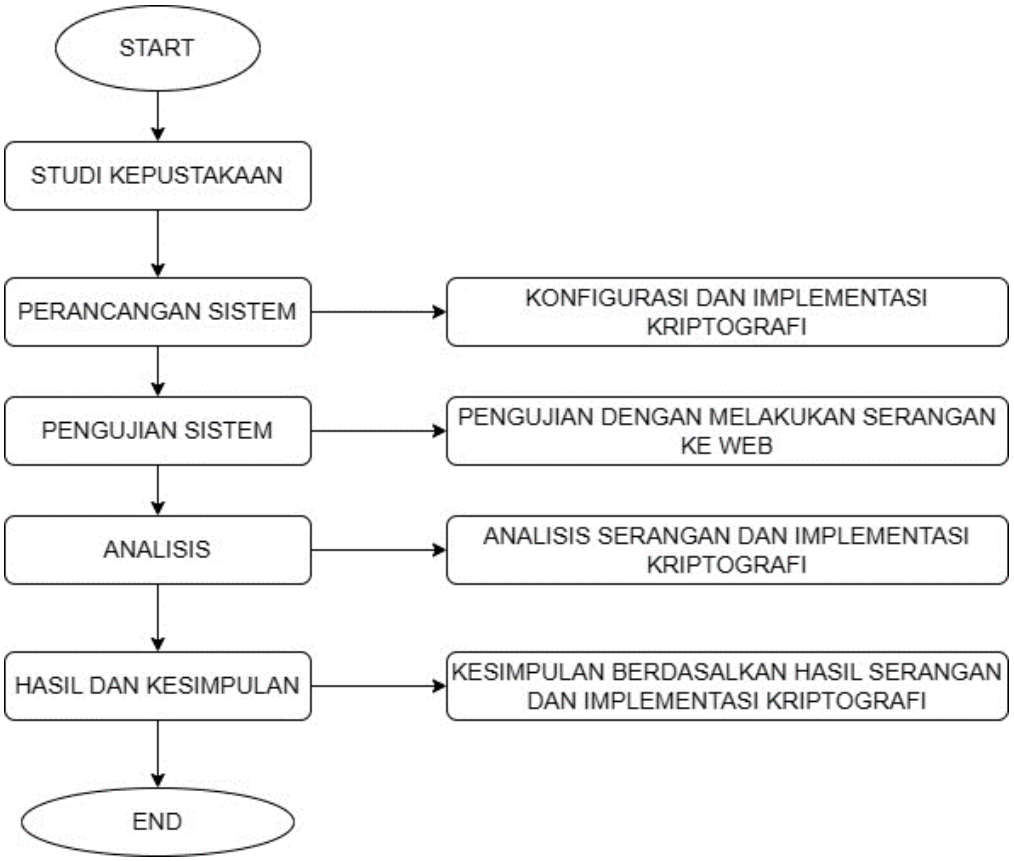
3.3.2.2 Bahan Penelitian

Bahan dari penelitian yang akan peneliti gunakan adalah bahan yang nantinya akan dianalisis pada penelitian ini. Bahan yang digunakan yaitu database dengan fungsi keamanan *Merkle-hellman Knapsack* yang dikombinasikan dengan *AES-256* serta bagaimana hasilnya dalam pengujian menggunakan *SQL Injection.*

3.2.3 Diagram Alur Penelitian

Peneliti memiliki metode penelitian untuk penelitian ini yaitu berupa studi kepustakaan, perancangan sistem, pengujian sistem, penelitian kepustakaan,

analisis dan penarikan kesimpulan. Aliran yang terkandung dalam pencarian ini terkandung dalam Gambar 3.1



Gambar 3.1 Diagram Penelitian

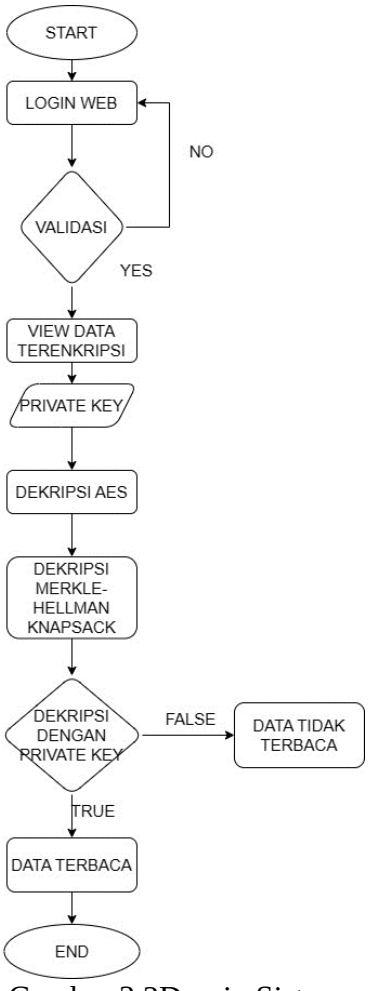
3.2.1 Studi Kepustakaan

Dalam ini peneliti melakukan studi kepustakaan tentang konsep enkrisi dan dekripsi *Merkle-hellman Knapsack* dan *Advanced Encryption Standard (AES)* .Proses ini bertujuan untuk mencari referensi seperti karya ilmiah, journal penelitian, seminar buku dan sumber lainya yang memiliki relevasi dengan penelitian yang dilakukan peneliti.

3.2.2 Perancangan Sistem

Sistem yang dirancang berbasis Web dengan system login untuk keamanan *database*nya. System login ini nantinya dilengkapi dengan algoritma enkripsi *Merkle-hellman Knapsack* dan *Advanced Encryption Standard (AES)*. Selain

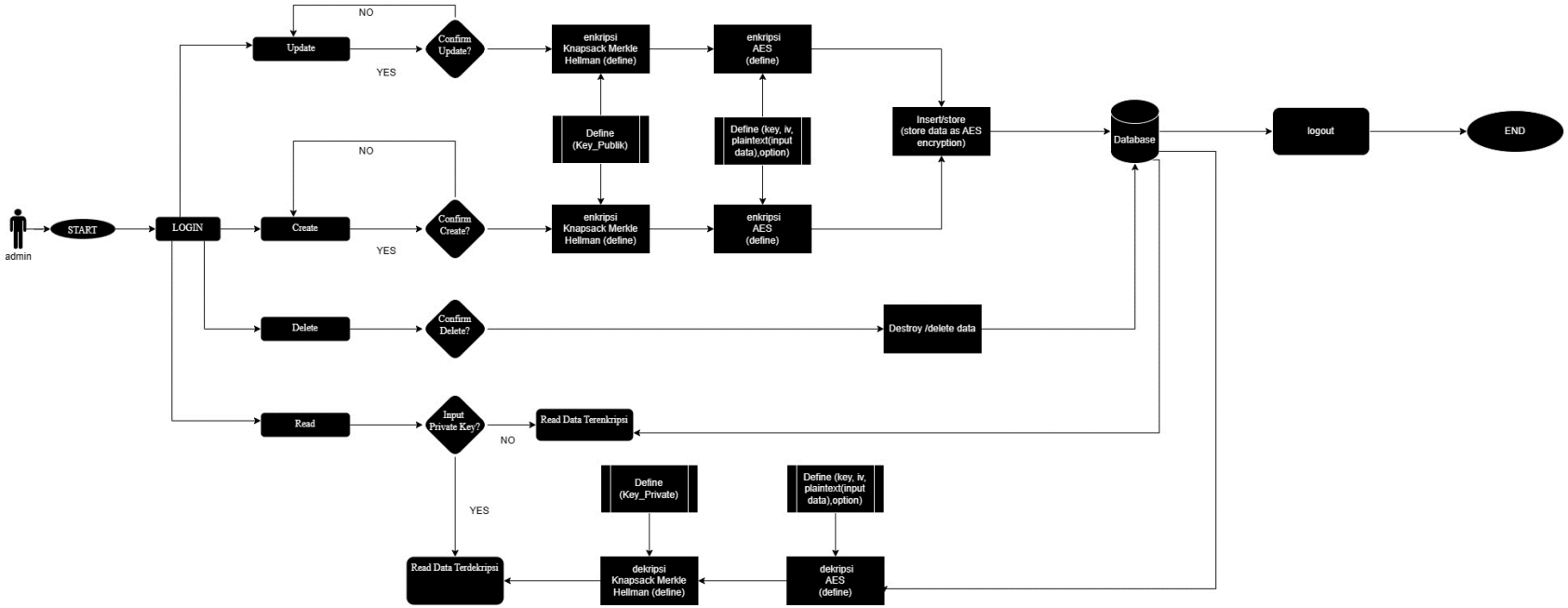
system login juga terdapat data yang nantinya juga akan dienkripsi dengan algoritma *Merkle-hellman Knapsack* dan *Advanced Encryption Standard (AES)*. Sistem kriptografi ini nantinya akan emlakukan enkripsi *Merkle-hellman Knapsack* terlebih dahulu dan apabila sudah selesai dilanjutkan melakukan enkripsi *Advanced Encryption Standard (AES)*. Sistem akan berjalan dalam sebuah *Web Hosting* yang dapat diakses pada http://aziznative.skirpsidimasgum.my.id/ .



Gambar 3.2Desain Sistem

3.2.2.1 Perancangan Arsitektur Sistem

perancangan system ini akan dijadikan objek penelitian oleh peneliti. Perancangan ini menggunakan *Double Encryption* sebagai enkripsinya dengan menggunakan arsitekstur sistem yang tertuang pada gambar 3.3 arsitektur sistem **:**



Gambar 3.3 Arsitektur Sistem

3.2.2.2 Konfigurasi Web

ada web hosting, konfigurasi fitur sistem dilakukan dengan skema seperti berikut :

Tabel 3.3 Konfigurasi Web Hosting

Fitur	Keterangan/Status
Web Application Firewall	Tidak aktif
Secure Socket Layer	Tidak aktif
Transport Layer Security	Tidak aktif
HTTPS	Tidak aktif
Password Protected Directory	Tidak aktif

Konfigurasi diatur dengan menonaktifkan sebagian fitur keamanan pada web server dengan tujuan untuk memudahkan proses pengujian serangan *SQL Injection* pada situs web.

3.2.2.3 Pemodelan Basis data

Pada tahap ini dilakukan konfigurasi dari basis data yang akan digunakan sebagai target pengujian sistem nantinya. Basis data dibuat dengan *PHPMyAdmin* yang sudah tersedia pada layanan *web hosting*. Untuk konfigurasinya bisa dilihat pada tabel 3.4 Konfigurasi Tabel Target

Tabel 3.4 Konfigurasi Tabel Target

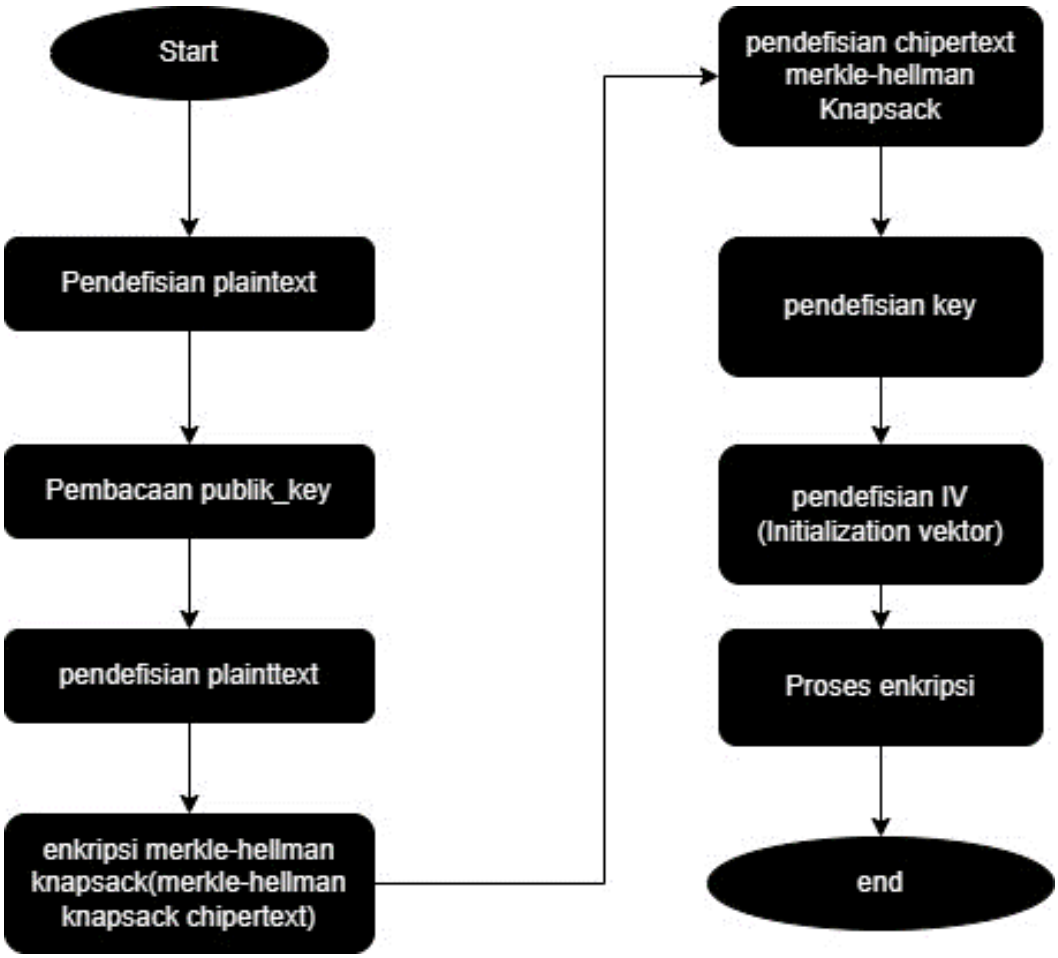
No	Nama	Type
1	id -anggota(PK)	Int
2	*username*	*Long Text*
3	nama	*Long Text*
4	alamat	*LongText*

No	Nama	Type
5	*email*	*LongText*
6	no hp	*LongText*

Pada skema diatas id_anggota digunakan sebagai *Primary Key* dengan tipe integer dan untuk *field* selain id_anggota bertipe *Long Text* pada *field* ini sesuai dengan produk akhir *ciphertext* hasil proses enkripsi. *Field* selain id_anggota nantinya adalah *field* yang akan dienkripsi pada sistem untuk diuji apakah enkripsi dan dekripsi dua tahap Merkle-hellman Knapsack dan AES-256 dapat diimplementasikan pada sistem.

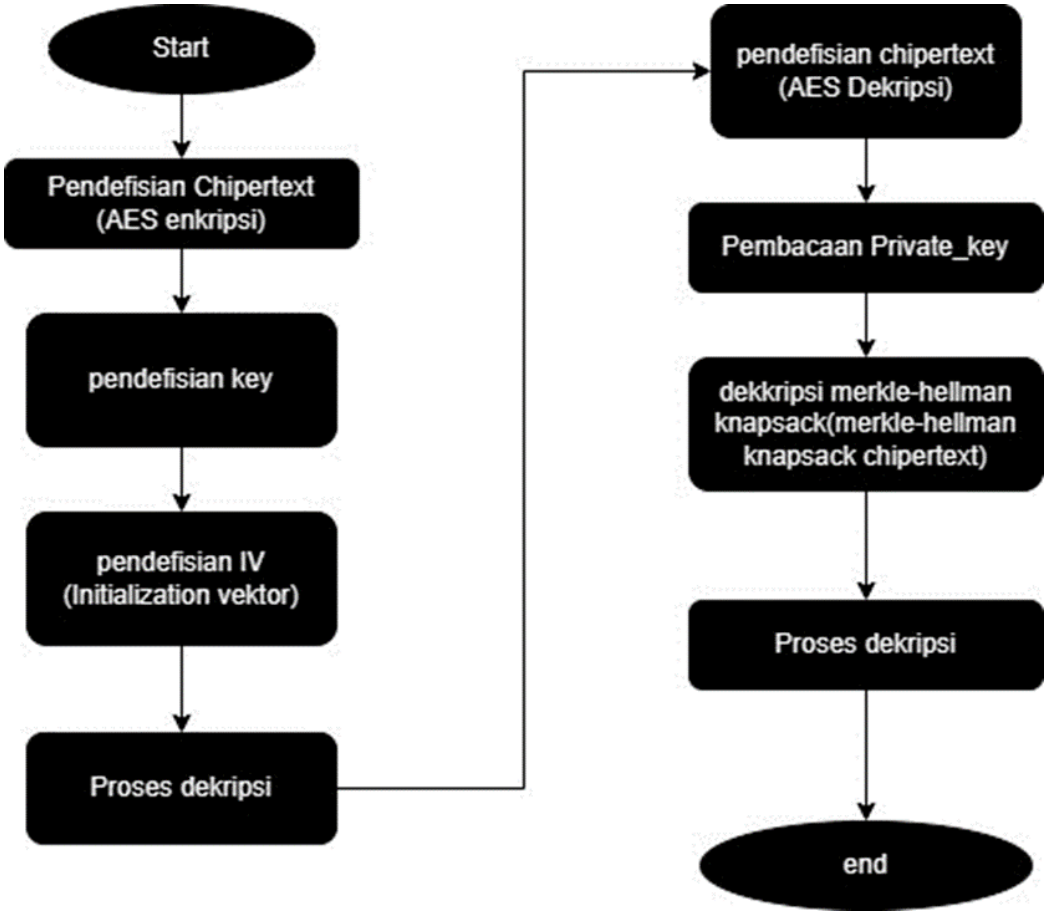
3.2.2.4 Implementasi Algoritma Merkle-hellman knapsack dan AES

Pada tahap ini, dilakukan perancangan enkripsi dan dekripsi *plain text* yang akan di *inputkan.* Dengan menginputkan *plaintext* atau inputan, enkripsi dilakukan dengan *cryptograph merkle-hellman knapsack* terlebih dahulu dilanjut dengan melakukan proses enkripsi AES, dengan rancangan pada Gambar 3.4 :



Gambar 3.4 Alur Enkripsi System

Setelah proses enkripsi selesai, hasilnya akan di simpan dalam data base untuk memunculkan data aslinya maka ada proses dekripsi dengan penginputan key untuk memunculkan hasilnya. Dengan proses dekripsi AES terlebih dahulu dilanjut dengan proses dekripsi merkle-hellman Knapsack dengan gambar 3.5 sebagai proses dekripsinya.

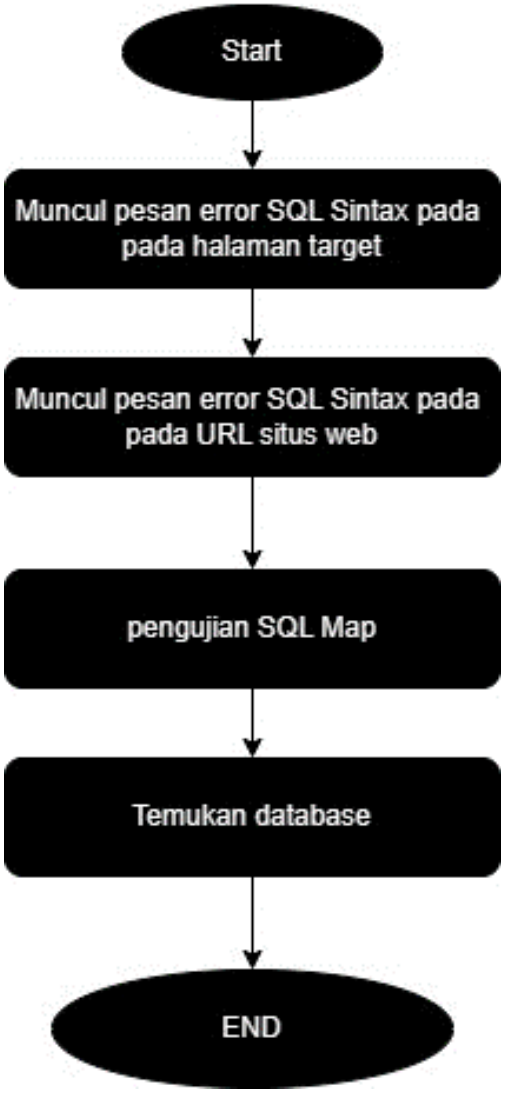


Gambar 3.5 Alur Dekripsi Sistem

3.2.3 Pengujian Sistem

Pengujian yang dilakukan oleh peneliti setelah melakukan perancangan system selesai dibuat . Tujuan pengujian ini yaitu untuk mendemonstrasikan

enkripsi ganda yang sudah dirancang apakah dapat mengamankan data terhadap serangan SQL-Injection. Diagram pengujian sistem dijelaskan pada gambar 3.6



Gambar 3.6 Alur Pengujian Sistem

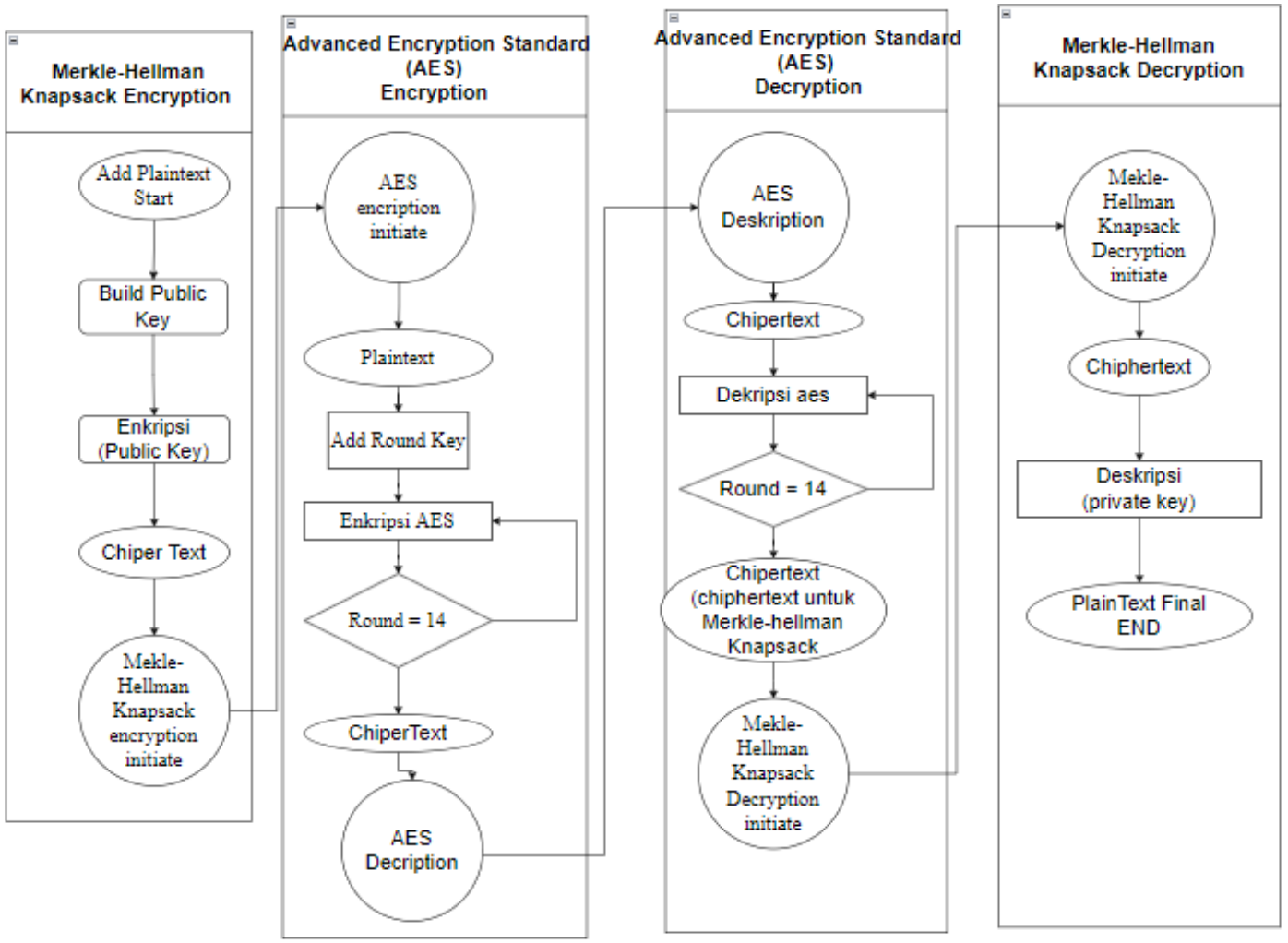
Pengujian dilakukan berdasarkan data yang sudah terenkripsi pada sistem. Database dari *dual encryption* dapat dilihat dan dapat terbaca setelah melakukan pengujian SQL Injection.

3.2.4 Analisis

Analisis dilakukan dengan menggunakan data hasil pengujian. Analisis datanya menggunakan implementasi Enkripsi *Merkle-hellman Knapsack* dan AES.

Analisis dilakukan dengan tujuan untuk menentukan kesimpulan dari semua Proses penelitian yang dilakukan.

Pendekatan yang dilakukan adalah menganalisis hasil pengujian serangan pada isi data pada system.parameternya adalah berhasil tidaknya data terambil dan berhasil tidaknya data terbaca oleh attacker. Jika pengujian menunjukan bahwa data tidak dapat terbaca maka bisa disimpulkan bahwa system diimplementasikan dengan baik dan dapat menangkal serangan.



Gambar 3.7 proses kriptografi

3.2.5 Hasil Analisis Dan Kesimpulan

Hasil analisis dan Kesimpulan yaitu tahapan diambil setelah dilakukan pengujian terhadap system yang dibuat. Ansalisis dan Kesimpulan diambil berdasarkan data yang terlah terkumpul setelah pengujian. Analisis dan Kesimpulan juga memuat saran untuk penelitian selanjutnya dibidang yang sama, dengan potensi adanya perbedaan metode, objek, maupun jenis serangan yang akan diujikan di penelitian-penelitian berikutnya.