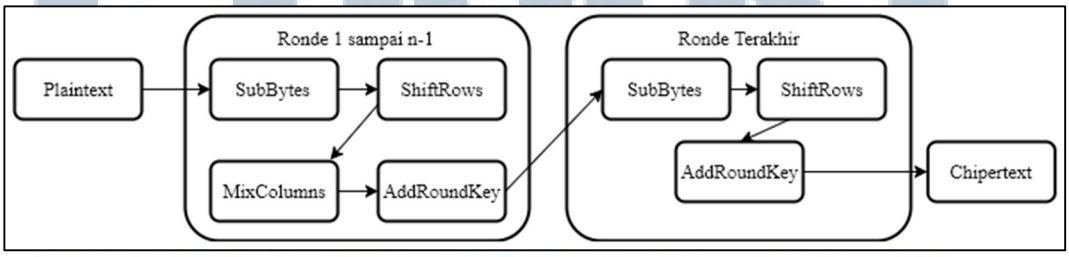
BAB II

LANDASAN TEORI

2.1 Advanced Encryption System (AES)

AES merupakan sebuah algoritma enkripsi-dekripsi dengan kunci simetris. AES diadopsi oleh pemerintah Amerika Serikat dan dijadikan sebagai standar enkripsi. AES tersedia dalam 3 blok cipher, yaitu AES-128, AES-192 dan AES-256. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit (Putra, 2015).

Pada proses enkripsi dan dekripsi AES terjadi beberapa ronde dengan empat langkah utama pada setiap rondenya. Langkah tersebut adalah *subbytes*, *shiftrows*, *mixcolumns*, dan *addroundkey* (Kak, 2017). Jumlah ronde pada setiap jumlah bit algoritma AES bervariasi. Untuk AES-128 bit memiliki jumlah ronde yaitu 10, sedangkan untuk AES-192 bit dan AES-256 bit memiliki jumlah ronde sebesar 12 dan 14. Setiap ronde dilakukan proses yang sama, hanya saja untuk ronde terakhir tidak dilakukan proses *mixcolumns* (Putra, 2015). Penjelasan lebih lanjut digambarkan pada Gambar 2.1.

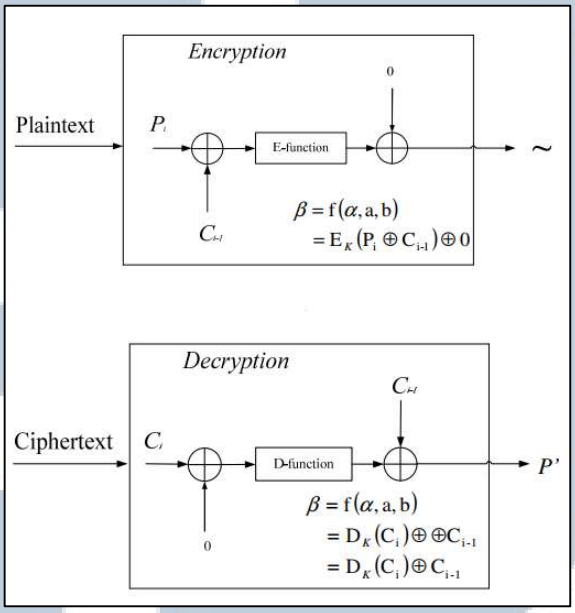


Gambar 2.1 Skema AES

2.1.1 Cipher Block Chaining (CBC)

CBC adalah sebuah blok cipher yang menyediakan *confidentiality* pesan tetapi tidak dengan *integrity* pesan (Huang dkk., 2013). Di dalam metode CBC,

setiap *plaintext block* yang akan dienkripsi dilakukan operasi XOR dengan *plaintext block* sebelumnya yang telah dienkripsi. Proses enkripsi dan dekripsi AES dengan metode Cipher Block Chaining dijelaskan pada Gambar 2.1.



Gambar 2.2 Metode Cipher Block Chaining

Pada Gambar 2.1 digambarkan bahwa sebelum melalui proses enkripsi, blok akan dilakukan operasi XOR terhadap blok sebelumnya. Demikian juga dengan proses dekripsi, blok yang sudah didekripsi akan dilakukan operasi XOR dengan blok sebelumnya.

2.2 One Time Password (OTP)

OTP adalah *password* yang berlaku hanya untuk satu sesi login atau transaksi. OTP menghindari sejumlah kelemahan yang berkaitan dengan *password* tradisional (statis). Kelemahan yang paling penting yang ditunjukan oleh OTP dengan *password* statis adalah OTP tidak rentan terhadap serangan *replay*. Ini berarti jika penyusup potensial berhasil merekam OTP yang sudah digunakan untuk masuk ke layanan atau untuk melakukan transaksi, penyusup tidak akan dapat menyalahgunakannya karena tidak berlaku lagi. Sistem OTP adalah layanan yang

bisa diimplementasikan pada banyak hal yang berhubungan dengan keamanan suatu akun atau melewati tahap otentikasi pemakai. Sistem ini lebih baik jika dilakukan pada layanan yang berhubungan dengan keuangan, misalkan layanan validasi pembayaran kuliah, validasi pembayaran internet, dan transfer uang (Mustofa, 2013).

One Time Password telah dikembangkan menjadi *HMAC Based One Time Password Algorithm* (HOTP) dan *Time Based One Time Password Algorithm* (TOTP).

2.2.1 HMAC Based One Time Password Algorithm (HOTP)

HOTP menggunakan hash SHA untuk hash *password* yang telah dibuat. SHA-1, SHA-2, dan juga SHA-3 dapat digunakan dalam enkripsi HOTP. HOTP dijelaskan pada rumus sebagai berikut.

$$\boldsymbol{HOTP(K, C) = Truncate\big(HMAC - SHA(K, C)\big)} \quad \ldots(2.1)$$

Dimana K adalah *key* dan C adalah *counter*. Hash dilakukan pada *key* dan *counter* dengan menggunakan *function* HMAC-SHA(). Di dalam *function* HMAC-SHA(), *key* dan *counter* diproses menjadi sebuah One Time Password dengan memanfaatkan *random* dari *byte string key* yang telah disediakan dan *counter* untuk dijadikan *offset* dari One Time Password yang telah dibuat. One Time Password yang telah dibuat selanjutnya akan dimodulus untuk mendapatkan One Time Password dengan panjang digit sesuai kebutuhan.

2.2.2 Time Based One Time Password Algorithm (TOTP)

TOTP adalah pengembangan dari HOTP dengan menggunakan faktor waktu dalam pembuatan OTP. TOTP dijelaskan pada rumus sebagai berikut.

$$\boldsymbol{TOTP = HOTP(K, T)} \quad \ldots(2.2)$$

K adalah k*ey* yang diberikan dan T adalah waktu pada saat One Time Password akan dibuat dengan diubah menjadi format *Unix Time*, yaitu waktu dalam detik yang telah berjalan dari 1 January 1970. *Unix Time* tersebut dipakai untuk menggantikan *Counter* pada HOTP.

2.3 Bluetooth Low Energy (BLE) Beacon

Bluetooth Low Energy adalah protokol terbaru yang tidak kompatibel dengan bluetooth tradisional. BLE memancarkan spektrum sinyal pada frekuensi 2.4GHz. Kekuatan sinyal BLE Beacon dapat mencapai lima puluh meter atau lebih dengan mengatur kekuatan transmisi sinyal (Rijswijk-Deij, 2013). Sinyal yang dipancarkan oleh BLE Beacon merupakan sinyal *heartbeat*.

Sinyal yang dipancarkan oleh BLE Beacon memiliki panjang 31 bytes data. Dimana data yang dipancarkan mengandung 128 bit *Universally Unique IDentifier* (UUID), 16 bit nilai major, dan 16 bit nilai minor (Rijswijk-Deij, 2013). Nilai major dan minor tersebut dapat digunakan untuk menyimpan nilai yang digunakan sebagai *identifier.*

2.4 Skala Likert

Skala likert adalah skala yang digunakan untuk mengukur sikap, pendapat, dan persepsi seseorang atau sekelompok orang tentang fenomena sosial (Sugiyono, 2012). Skala likert yang digunakan untuk kuesioner penelitian ini adalah skala likert dengan lima level. Dimana setiap kategori penilaian memiliki skor tersendiri dan digunakan untuk perhitungan skor total untuk setiap variabel penelitian.

Tabel 2.1 Kategori Bobot Penilaian

Kategori	Skor	Interval
Sangat Positif	5	100% >= Skor > 84%
Positif	4	84% >= Skor > 68%
Cukup	3	68% >= Skor > 52%
Negatif	2	52% > =Skor > 36%
Sangat Negatif	1	36% >= Skor >= 20%

Perhitungan skor akhir dilakukan dengan cara menjumlahkan total setiap kategori jawaban yang dikalikan dengan bobot penilaian kategori jawaban tersebut. Kemudian skor akhir digunakan untuk menghitung presentase skor terhadap bobot penilaian. Perhitungan tersebut dijelaskan sebagai berikut.

$$\text{Skor Akhir} = \frac{\text{Jumlah Total}}{\text{Alternatif Jawaban} \times \text{Jumlah Sampel}} \times 100\% \qquad \ldots(2.3)$$

Dengan demikian didapatkan persentase skor sesuai dengan bobot kategori penilaian yang telah ditentukan. Setelah itu dapat ditarik kesimpulan penilaian untuk setiap variabel sesuai dengan bobot penilaian.