BAB II
TEORI PENUNJANG

2.1 Algoritma Kriptografi

Kriptografi berasal dari bahasa yunani yaitu *cryptos* yang artinya *secret*(rahasia) dan *grapein* yang artinya *writing* (tulisan). Jadi kriptografi berarti *secret writing*(tulisan rahasia). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat yang lain.

Pada kriptografi dikenal istilah – istilah seperti *plain text, chipper text,*enkripsi, dan dekripsi. *Plain text* adalah pesan asli yang akan dikirimkan. *Chipper text* adalah pesan yang telah disandikan dengan metode enkripsi. Enkripsi adalah proses mengubah sebuah *plain text* menjadi *chipper text*, dan dekripsi adalah proses mengubah sebuah *chipper text* menjadi *plain text*.[3]

2.1.1 Jenis – Jenis Algoritma Kriptografi

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakai, yaitu : algoritma simetri dan algoritma asimetri dan fungsi hash.

2.1.2 Algoritma Simetri

Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi maupun dekripsi. Bila mengirim pesan dengan menggunakan algoritma ini, sipenerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang terkirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri di antaranya adalah :[3]

1. *Data Encryption Standard* (DES),
2. RC2, RC4, RC5, RC 6
3. *International Data Encryption Algorithm* (IDEA)
4. *Advanced Encryption Standard* (AES)
5. *On Time Pad* (OTP)
6. A5

2.1.3 Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci public, dengan arti kata kunci yang digunakan melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu :

1. Kunci umum (*public key*), kunci yang boleh semua orang tahu (dipublikasikan).
2. Kunci rahasia (*private key*), kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci public orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsikannya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsikan pesan tersebut. Algoritma asimetri bisa mengirimkan pesan dengan lebih aman daripada algoritma simetri.

Algoritma yang memakai kunci public di antaranya adalah :

1. *Digital Signature Algorithm* (DSA).
2. RSA.
3. *Diffle-Hellman* (DH).
4. *Elliptic Curve Cryptography* (ECC).
5. Kriptografi Quantum, dan lain sebagainya.

2.2 Algoritma *Tiny Encription Algorithm* (TEA)

Tiny Encription Algorithm (TEA) adalah algoritma sandi yang diciptakan oleh David Wheeler dan Roger Needham. Algoritma ini merupakan algoritma penyandian *block chipher* yang dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal [4].

Algoritma TEA (*Tiny Encryption Algorithm*) memiliki sistem penyandian menggunakan proses *feistel network* dengan menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Hal ini dimaksudkan untuk menciptakan sifat non-linearitas. Pergeseran dua arah (ke kanan dan ke kiri) menyebabkan semua bit kunci dan data bercampur secara berulang ulang.

2.1.4 Cara Kerja Algoritma TEA

1. Pergeseran (*shift*)

   Blok teks terang pada kedua sisi yang masing – masing sebanyak 32 bit akan digeser kekiri sebanyak (4) kali dan digeser kekanan sebanyak (5) kali.
2. Penambahan

   Setelah melakukan pergeseran, maka Y dan Z yang telah digeser akan ditambahkan dengan kunci k[0] – k[3]. Sedangkan Y dan Z awal akan ditambahkan dengan sum(delta).
3. Peng-XOR-an

   Proses selanjutnya setelah dioprasikan dengan penambahan pada masing – masing register maka akan dilakukan peng-XOR-an dengan rumus untuk satu *round* adalah sebagai berikut :

   y = y + (((z<<4)+k[0])^z + sum^((z>>5)+k[1]))

   z = z + (((y<<4)+k[2]^y + sum^((y>>5)+k[3]))

Hasil penyandian dalam satu *cycle* satu blok teks terang 64-bit menjadi 64-bit teks sandi adalah dengan cara menggabungkan Y dan Z. untuk penyandian pada *cycle* berikutnya Y dan Z ditukar posisinya, sehingga Y1 menjadi Z1 dan Z1 menjadi Y1 lalu dilanjutkan proses seperti langkah – langkah sebelumnya sampai 16 *cycle* (32 *round*).

4. Key Schedule

   Algortima TEA menggunakan *key schedule*-nya sangat sederhana. Yaitu kunci k[0] dan k[1] konstan digunakan untuk *round* ganjil sedangkan k[2] dan k[3] konstan digunakan untuk *round* genap.

5. Dekripsi dan Enkripsi

   Proses dekripsi sama halnya seperti pada proses penyandian yang berbasis *feistel cipher* lainnya.yaitu pada prinsipnya adalah sama pada saat proses enkripsi. Hal yang berbeda adalah penggunaan teks sandi sebagai *input* dan kunci yang digunakan urutannya dibalik. Proses dekripsi semua *round* ganjil menggunakan k[1] terlebih dahulu kemudian k[0], demikian juga dengan semua *round* genap digunakan k[3] terlebih dahulu kemudian k[2]. Rumus enkripsi dan dekripsi ditunjukan dibawah ini :

   Proses enkripsi digunakan rumus :

   L0 = L0 + f (R0 , k[0], k[1], sum)

   R0 = R0 + f (L0, k[2], k[3], sum)

   Jadi L0 merupakan hasil penjumlahan dari L 0 ditambahkan dengan f (R0, k[0], k[1], sum).

   Proses enkripsi untuk satu round digunakan rumus :

   Y = y + (((z<<4)+k[0])^z + sum^((z>>5)+k[1]))

   z = z + (((y<<4)+k[2]^y + sum^((y>>5)+k[3]))

   Proses dekripsi digunakan rumus :

   L0 = L0 + f (R0 , k[1], k[0], sum)

   R0 = R0 + f (L0, k[3], k[2], sum)

Jadi L0 merupakan hasil penjumlahan dari L 0 ditambahkan dengan f (R0, k[0], k[1], sum).

Proses dekripsi untuk satu round digunakan rumus :

y = y + (((z<<4)+k[1])^z + sum^((z>>5)+k[0]))

z = z + (((y<<4)+k[3]^y + sum^((y>>5)+k[2]))

Rumus Y diatas menjelaskan bahwa Y merupakan hasil dari Y yang ditambahkan dengan Z yang digeser kekiri sebanyak empat kali dengan penambahan kunci k[1]. Kemudian hasilnya di XORkan dengan Z yang dijumlahkan dengan sum(delta). Hasil dari peng-XOR-an dari kedua penjumlahan tadi di XORkan lagi dengan Z yang digeser kekanan sebanyak lima kali dengan penambahan kunci k[0]. Demikian juga dengan rumus Z sama halnya dengan rumus Y, hanya kunci yang digunakan menggunakan kunci k[3] dan k[2].

2.3 Sidik Jari

Sidik jari adalah gurat – gurat yang terdapat pada kulit ujung jari. Sidik jari berfungsi untuk memberi gaya gesek lebih besar agar jari – jari dapat memegang benda agar lebih erat. Sistem pengamanan dengan menggunakan sidik jari sudah mulai dipergunakan di Amerika oleh seorang bernama E. Henry pada tahun 1902. Henry mengguanakan metode sidik jari untuk melakukan identifikasi para pekerja dalam rangka mengatasi pemberian upah ganda. Sistem Henry menggunakan pola ridge (punggung alur pada kulit), yang terpusat pola jari tangan, khususnya telunjuk. Untuk memperoleh gambar pola ridge dapat dilakukan dengan cara menggulung jari yang diberi tinta pada suatu kartu cetakan hingga dihasilkan suatu pola ridge yang unik bagi masing – masing orang. Para pakar membuktikan bahwa setiap orang memiliki pola sidik jari yang berbeda. Pola ridge tidaklah diwariskan. Pola ridge dibentuk waktu embrio dan tidak dapat dirubah seumur hidup. Perubahan pola ridge hanya dapat terjadi jika akibat trauma, misalnya akibat luka – luka, terbakar, penyakit, atau penyebab lainnya. Sistem biometric sidik jari merupakan sistem yang paling banyak digunakan saat ini karena

memiliki tingkat akurasi yang tinggi dan mudah untuk diterapkan. Dari hasil penelitian ditemukan terdapat 9 macam pola utama ridge, yaitu :

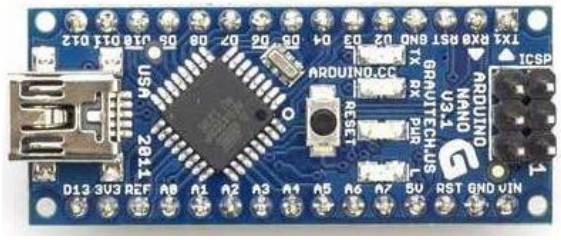
1. Loop : Terdiri dari satu atau lebih kurva bebas dari ridge dan sebuah delta.
2. Arch : Membentuk pola dengan ridge berada diatas ridge yang lain dalam bentuk lengkungan umum.
3. Whorl : Pola ini terdiri dari satu atau lebih kurva bebas ridge dan dua buah delta.
4. Tented Arch : Pola ini terdiri dari paling tidak sebuah ridge yang melengkung keatas yang kemudian bercabang menjadi dua ridge.
5. Double Loop: Pola ini membentuk dua formasi lengkungan yang lalu berpisah, dengan dua titik delta.
6. Central Pocket Loop : Terdiri dari satu atau lebih kurva ridge dan dua titik delta.
7. Accidental : Pola ini mempunyai dua titik delta. Satu delta akan berhubungan dengan lengkungan keatas, dan delta yang lain terhubung dengan lengkungan yang lain.
8. Composite : Terdiri dari gabungan dua atau lebih pola yang berbeda.
9. Lateral Pocket Loop : Pola ini terdiri dari dua lengkungan yang terpisah. Ada dua titik dua delta.

Sekitar 60% orang memiliki pola sidik jari loop, sekitar 30% pola sidik jari whorl, sekitar 5% yang berbentuk arch dan sisanya berbentuk yang lainnya. Semua pola dapat dibedakan dengan cara melihat langsung. Komputer dapat menganalisa garis – garis perubahan arah bentuk ridge, dengan kemampuan seperti mata manusia yang terlatih area papillary ridge kadang – kadang dikenal sebagai pattern area. Masing – masing pola papillary ridge menghasilkan suatu bentuk pola area yang berbeda. Pusat gambar jari mencerminkan pola area, dikenal sebagai inti *core point.* Bagian ridge yang berwujud dua parallel yang berbeda mengelilingi pola area inti disebut *type lines*. Titik awal percabangan dua ridge disebut *delta*. Proses perpecahan sebuah garis menjadi dua garis ridge disebut *bifurcation*. Banyaknya persimpangan ridge di dalam pola area disebut suatu ridge

count. Komputer Tormography dapat digunakan untuk mendeteksi titik – titik tersebut berdasarkan sumbu koordinat x dan y. [5]

2.4 Arduino Nano

Arduino Nano adalah salah satu papan pengembangan mikrokontroler yang berukuran kecil, lengkap dan mendukung penggunaan breadboard.Arduino Nano diciptakan dengan basis mikrokontroler ATmega328 (untuk Arduino Nano versi 3.x) atau ATmega 168 (untuk Arduino versi 2.x). Arduino Nano kurang lebih memiliki fungsi yang sama dengan Arduino Duemilanove, tetapi dalam paket yang berbeda. Arduino Nano tidak menyertakan colokan DC berjenis Barrel Jack, dan dihubungkan ke komputer menggunakan port USB Mini-B. Gambar 2.1 menunjukan bentuk fisik dari Arduino Nano.[6]



Gambar 2. 1 Tampilan Arduino Nano

Berikut spesifikasi *board* Arduino Uno ditunjukan pada tabel 2.1.

Tabel 2. 1 Spesfikasi Arduino Nano

No	Nama	Keterangan
1	Mikrokontroler	Atmega328
2	Tegangan pengoprasian	5 V
3	Tegangan input	7 – 12 V
4	Batas tegangan input	6 – 20 V
5	Pin I/O digital	14 (6 diantaranya menyediakan PWM)

Tabel 2. 2 Tabel Lanjutan Spesifikasi Arduino Nano

No	Nama	Keterangan
6	Pin input analog	8
7	Arus DC tiap pin I/O	40 mA
8	Arus DC pin 3.3 V	50 mA
9	Memori flash	32 KB, sekitar 0.5 KB digunakan sebagai bootloader
10	SRAM	2 KB
11	EEPROM	1 KB
12	Clock speed	16 MHz

2.5 Sensor Sidik Jari

Sensor sidik jari merupakan perangkat elektronika yang berfungsi menangkap gambar digital dari sidik jari manusia. Terdapat dua proses dalam sistem sensor sidik jari, proses pengambilan gambar dan proses pencocokan gambar. Metode yang paling sering digunakan oleh sensor sidik jari adalah metode *optical Scanning*. Gambar 2.2 menunjukan bentuk fisik dari Sensor Sidik Jari.[7]

Gambar 2. 1 Sensor Sidik Jari

Berikut spesifikasi sensor sidik jari ditunjukan pada tabel 2.3.

Tabel 2. 3 Spesifikasi Sensor Sidik Jari

No	Nama	Keterangan
1	Tegangan supply DC	3.6 – 6 V
2	Waktu citra	1.0 detik
3	Jendela ukuran	14 x 18 mm
4	Fitur file	256 bytes
5	File template	512 bytes
6	Cari waktu	1.5 detik

2.6 Keypad 4x4

Keypad 4x4 merupakan modul yang berukuran 4 kolom x 4 baris. Modul ini dapat difungsikan sebagai device masukkan dalam aplikasi – aplikasi seperti pengaman digital, data logger, absensi, pengendali kecepatan motor, robotik dan sebagainya.[8] Gambar 2.3 menunjukan bentuk fisik dari keypad 4x4.

Gambar 2. 2 Keypad 4x4

2.7 Relay

Relay merupakan komponen elektronika yang memiliki fungsi bekerja sebagai saklar mekanik yang digerakkan oleh energi listrik. Relay menggunakan gaya elektromagnetik untuk memutuskan atau menghubungkan suatu rangkaian elektronika yang satu dengan rangkaian elektronika yang lainnya.Relay terdiri dari *coil* dan *contact*. *Coil* adalah gulungan kawat yang mendapat aruslistrik, sedangkan *contact* adalah sejenis saklar yang pergerakannya tergantung dari adat idaknya arus listrik di *coil*. *Contact* ada 2 jenisyaitu *normally open* (kondisi awal sebelum diaktifkan *open*), dan *normally closed* (kondisi awal sebelum diaktifkan *closed*). Gambar 2.4 menunjukan bentuk fisik dari relay.

Gambar 2. 3 Relay

Berikut spesifikasi relay ditunjukan pada tabel 2.4.

Tabel 2. 4 Spesifikasi Relay

No	Nama	Keterangan
1	Input DC	5 V
2	Maksimum load	30VDC/10 A
3	Output	1 Channel

2.8 LCD (Liquid Crystal Display)

LCD (*Liquid Crystal Display*) adalah suatu jenis media tampilan yang menggunakan kristal cair sebagai penampil utama. LCD bisa memunculkan tulisan dikarenakan terdapat banyak sekali titik cahaya (piksel) yang terdiri dari satu buah kristal cair sebagai sebuah titik cahaya.Walau disebut sebagai titik cahaya, namun kristal cair ini tidak memancarkan cahaya sendiri. Sumber cahaya didalam sebuah perangkat LCD adalah lampu neon berwarna putih di bagian belakang susunan kristal cair tadi. Titik cahaya yang jumlahnya puluhan ribu bahkan jutaan inilah yang membentuk tampilan citra. Kutub kristal cair yang dilewati arus listrik akan berubah karena pengaruh polarisasi medan magnetik yang timbul dan oleh karenanya akan hanya membiarkan beberapa warna diteruskan sedangkan warna lainnya tersaring.[9] Gambar 2.5 menunjukan bentuk fisik dari LCD (*Liquid Crystal Display*).

Gambar 2. 4 LCD (Liquid Crystal Display)

Berikut spesifikasi LCD (*Liquid Crystal Display*) ditunjukan pada tabel 2.5.

Tabel 2. 5 Spesifikasi LCD (Liquid Crystal Display)

No	Nama	Keterangan
1	Input supply DC	5 V
2	Ukuran	16 karakter x 2 baris
3	Controller / driver	HD44780 / equivalent

Tabel 2. 6 Tabel Lanjutan Spesifikasi LCD (Liquid Crystal Display)

No	Nama	Keterangan
4	View area	64 x 15 mm
5	Dimensi modul	80 x 36 x 13 mm

2.9 Solenoid

Solenoid adalah salah satu jenis kumparan yang terbuat dari kabel panjang yang dililitkan secara rapat dandapat diasumsikan bahwa panjangnya lebih besar daripada diameternya. Sedangkan Kunci selenoid adalah gabungan antara kunci dan solenoid dimana biasa digunakan dalam elektronisasi suatu alat sebagai pengunci otomatis dan lain – lainnya. Prinsip selenoid ditemukan oleh fisikawan perancis yang bernama Andre Marie Ampere. Pada bidang rekayasa istilah ini menunjukkan pada perangkat tranduser yang mengkonversi energi kegerakan linear. Pada saat kumparan dialiri arus litrik maka gaya elektromagnetik akan muncul dan menarik besi yang ada pada bagian tengah kumparan secara linear.[10] Gambar 2.6 menunjukan bentuk fisik dari Solenoid.

Gambar 2. 5 Solenoid

2.10 NodeMCU

NodeMCU merupakan sebuah platform IoT (*Internot Of Things*) yang bersifat *opensource.* Terdiri dari perangkat keras yang berupa *System On a Chip* ESP8266 jenis ESP-12E dan *firmware* yang digunakan, menggunakan bahasa pemrograman *scripting* Lua. Istilah NodeMCU sebenarnya mengacu pada *firmware* yang digunakan daripada perangkat keras *development kit.*

NodeMCU telah me-peckage modul ESP8266 yang berjenis ESP-12E ke dalam sebuah board yang memiliki berbagai fitur layaknya mikrokontroler ditambah dengan bias akses terhadap Wifi, dan sudah menggunakan chip komunikasi USB to serial. Sehingga untuk memprogramnya hanya memerlukan kabel data microUSB untuk menghubungkannya. Sedangkan modul ESP8266 akan terasa sedikit sulit karena diperlukan beberapa teknik *wiring* serta tambahan modul USB to serial untuk mengunduh programnya.[11] Gambar 2.8 menunjukan NodeMCU ESP8266.

Gambar 2. 6 NodeMCU ESP8266

2.11 Aplikasi Line Notify

Line Notify adalah API *gateway* untuk menghubungkan layanan eksternal secara web sehingga Line dapat memberikan notifikasi setelah menghubungkannya dengan layanan web yang dimaksud. Layanan ini dapat digunakan oleh siapapun secara gratis dengan menggunakan dua jenis

authentication yakni OAtuh2 dan HTTPS API untuk menghubungkannya. Layanan utama yang dapat dihubungkan untuk saat ini bias didapat Github, IFTT, Mackeret. Tak hanya itu, Line Notify juga memungkinkan untuk menggunakan akses token personal sehingga developer dapat menghubungkan aplikasinya dengan Line Notify.

Gambar 2. 7 Logo Line Notifiy

Messaging-API terbaru yang diperkenalkan dengan fungsionalitas bot untuk para developer ini memiliki format baru, yakni :

1. Confirm Type, di mana pengguna dapat memilih pilihan yang telah diberikan seperti “ya” atau “tidak”
2. Button Type, di mana pengguna akan disuguhi beberapa jenis tombol yang terdiri dari gambar, teks, atau tombol tindakan lain yang kemudian dapat mengalihkan pengguna ke aksi tertentu
3. Carousel Type, tipe ini merupakan tipe yang hampir sama seperti jenis Button tetapi diletakkan pada format scrolling horizontal sehingga ada beragam jenis kontn yang dapat ditampilkan sekaligus
4. Ketiga jenis API Messaging terbaru tersebut dapat digunakan di LINE Bot Platform, sehingga pengguna bisa berkomunikasi dengan chatbot dengan lebih mudah tanpa harus bersusah payah mencari keyword atau chat tertentu untuk bisa mendapatkan konten atau pesan tertentu yang tepat.

Dengan kemudahan yang diberikan API Messaging tersebut, para perusahaan atau pembisnis yang menggunakan chatbot dapat lebih mudah juga untuk bisa memenuhi kebutuhan para penggunanya. Selain itu, Messaging API terbaru ini juga dapat digunakan dalam Group Chat sehingga informasi dapat dibagikan dengan berbagai pihak. LINE Bot API yang terbaru kali ini juga memiliki arsitektur yang lebih mudah dan sederhana, dengan dukungan kode sample yang lebih banyak, perilisan SDK resmi yang mendukung lima bahasa pemprograman (Java, golang, Ruby, PHP, dan Perl5). LINE API Messaging baru ini juga memungkinkan pengguna yang memiliki akun LINE Official dan LINE@ juga dapat mengirim pesan menggunakan API, di mana pesan terbagi atas 2 jenis yaitu push messages dan reply messages.[12]