Tugas 1

19 September 2018

Nama : Patricia Joanne
NPM : 140810160065

1. **Sebutkan dan jelaskan pengaplikasian (implementasi) kriptografi pada sebuah system/perangkat lunak (selain login), minimal 3!**
    - Transaksi lewat ATM

      Anjungan Tunai Mandiri atau *Automatic Teller Machine* (*ATM*) digunakan nasabah bank untuk melakukan transaski perbankan seperti menarik uang secara tunai, transfer uang, mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya. Transaksi lewat ATM memerlukan kartu magnetik (disebut juga kartu ATM) yang terbuat dari plastik dan kode PIN (*Personal Information Number*) yang berasosiasi dengan kartu tersebut. PIN terdiri dari 4 angka yang digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM. Bentuk perlindungan yang dilakukan selama proses verifikasi tersebut adalah dengan mengenkripsikan PIN. Algoritma enkripsi yang digunakan adalah DES dengan mode ECB. Karena DES bekerja dengan mengenkripsikan blok 64-bit, maka PIN yang hanya terdiri dari 4 angka (32 bit) harus ditambah dengan *padding bits* sehingga panjangnya menjadi 64 bit. *Padding bits* yang ditambahkan berbeda-beda untuk setiap PIN, bergantung pada informasi tambahan pada setiap kartu ATM-nya. Karena panjang PIN hanya 4 angka, maka peluang ditebak sangat besar. Oleh karena itu selain dari enkripsi PIN, beberapa jaringan ATM sekarang menggunakan penggunaan kriptografi kunci publik. Kartu ATM pengguna mengandung kunci privat dan sertifikat digital yang ditandatangani oleh *card issuer* (CA) untuk mensertifikasi kunci publiknya. ATM mengotentikasi kartu dengan cara mengirimkan suatu *string* ke kartu untuk ditandatangani dengan menggunakan kunci privat, lalu tanda tangan tersebut diverifikasi oleh ATM dengan menggunakan kunci publik pemilik kartu.
    - Transaksi dalam *e-commerce*

      Pembayaran barang yang dibeli di *e-commerce* dilakukan dengan menggunakan kartu kredit, yang berarti bahwa pembeli harus mengirimkan kode PIN kartu kredit

dan informasi lainnya melalui internet. *Browsing* secara aman adalah fitur paling penting pada *e-commerce*. *Secure Socket Layer* (SSL) adalah protokol yang digunakan untuk *browsing* secara aman. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara *website* dan *web browser*. SSL adalah protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*. *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*. Fungsi paling dasar yang digunakan SSL adalah membentuk saluran untuk mengirimkan data terenkripsi, seperti data kartu kredit, dari *browser* ke *website* yang dituju.

- Transaksi menggunakan *cryptocurrency* seperti Bitcoin

  Cryptocurrency mempunyai langkah keamanan yang bisa mencegah terjadi kecurangan dalam sistemnya. Pengguna tidak harus membayar kepada pengguna lainnya menggunakan koin digital yang sama. Tidak seperti mata uang kertas, pengamanan mata uang digital dilakukan murni secara teknologi, dan tanpa harus bergantung pada kebijakan pemerintah pusat. Dengan cara *encoding* atau mengkodekan aturan-aturan dalam sistem mata uang digital, transaksi mata uang digital bisa aman dari gangguan keamanan pada sistemnya.

2. **Apa itu Kriptografi sederhana (klasik)?**

   Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang.

3. **Sebutkan contoh Algoritma Kriptografi Sederhana (klasik) beserta penjelasan singkatnya!**

   Algoritma Ceasar Cipher

   Setiap huruf dimajukan 3 huruf

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Contoh:

Plain text = NAMA SAYA PATRICIA

Cipher text = QDPD VDBD SDWULFLD

Referensi

https://www.edukasibitcoin.com/pengantar-kriptografi-dan-cryptocurrency/

https://www.unisbank.ac.id/ojs/index.php/fti2/article/view/1313

https://ejournal.unib.ac.id/index.php/pseudocode/article/view/1042

http://cheesterzone.blogspot.com/2011/10/contoh-aplikasi-dan-pembahasan.html

http://ilmu-kriptografi.blogspot.com/2011/05/kriptografi-dalam-kehidupan-sehari-hari.html

http://itjambi.com/kriptografi-klasik/

http://amilul.blogspot.com/2012/11/algoritma-kriptografi-klasik-dan-modern.html