# Analisis Penggunaan Kriptografi dalam Online Banking

Marvello Oni (13508031)
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*If18031@s.if.itb.ac.id*

***Abstract* — Internet banking atau perbankan internet adalah salah satu fasilitas layanan perbankan yang ditujukan bagi nasabah untuk dapat melakukan transaksi perbankan melalui situs internet yang telah disediakan oleh bank bersangkutan. Maraknya penggunaan internet dikalangan masyarakat membuat layanan ini makin dipakai oleh banyak nasabah untuk melakukan transaksi karena kemudahannya. Berbeda dengan ATM, nasabah dapat menggunakan fasilitas ini tanpa memakai komputer yang telah disediakan oleh bank. Keunggulannya ini lah yang membuat internet banking menjadi sangat rawan keamanannya. Karena nasabah menggunakan komputer bukan dari bank, maka ancaman keamanan yang dapat terjadi antara lain phising, keylogger, dan man in the middle. Hal ini disebabkan karena bank tidak dapat mengatur keamanan dari komputer yang dipakai oleh nasabah. Untuk menjaga keamanannya dilakukan beberapa cara salah satunya yaitu penggunaan *Banking token* berupa alat kecil semacam kalkulator untuk mengamankan transaksi *internet banking* dan juga algoritma enkripsi tertentu. Dalam makalah ini akan dianalisis mengenai Algoritma yang digunakan dalam mengenkripsi data-data yang dikirmkan oleh *client* menuju *server* dan sifat dasar dari banking token serta garis besar bagimana mereka membantu dalam proses pengamanan online bangking.**

***Index Terms*— Security, Online Banking, Banking Token, Enkripsi**

## I. PENDAHULUAN

Internet Banking atau perbankan internet adalah sebuah layanan yang disediakan oleh bank yang dapat memfasilitasi nasabahnya untuk melakukan transaksi perbankan melalui situs internet. Dengan menggunakan layanan ini, nasabah tidak perlu mendatangi kantor bank dan juga ATM untuk melakukan transaksi. Nasabah hanyamemerlukan koneksi internet dan mengunjungi situs yang telah disediakan untuk pelayanan. Setelah melakukan autentikasi pada situs tersebut, nasabah dapat melakukan transaksi yang diinginkan sesuai menu yang disediakan oleh situs. Sama halnya dengan layanan perbankan populer seperti SMS Banking, nasabah dapat melakukan transaksi di mana saja dan kapan pun juga asalkan tersedia jaringan internet.

Layanan ini sudah ada di dunia sejak awal dekade 1980an salah satunya oleh Nottingham Building Society pada tahun 1983 di Inggris. Sedangkan di Indonesia, fasilitas ini pertama kali digunakan oleh Bank Papan Sejahtera pada awal dekade 1990an meski kemudian pada tahun 1995 bank ini ditutup karena masalah keuangan. Akan tetapi kini telah banyak bank di Indonesia yang telah menyediakan layanan serupa seperti Bank Mandiri, Bank BCA, Bank Niaga, Citibank, dan lain-lain.

Pada internet bangking ini terdapat beberapa masalah keamanan seperti phising, keylogger, dan man in the middle.

Phising adalah upaya untuk mencuri data pribadi seperti nama pengguna, sandi lewat, dan nomor rekening dengan cara meniru sebagai instansi terkait pada jalur komunikasi elektronik. Salah satu contoh phising adalah meniru sebuah situs milik bank tempat nasabah melakukan transaksi atau mengirim surat elektronik kepada nasabah dengan berpurapura sebagai bank terkait untuk meminta data pribadi yang diperlukan. Kegiatan yang pertama lebih sering disebut dengan website spoofing.

Keylogger adalah sebuah aplikasi yang berjalan secara tersembunyi pada sistem operasi sebuah komputer yang digunakan terutama untuk merekam aktivitas pengguna komputer tersebut. Dalam hal ini, aplikasi ini memberi ancaman yakni merekam nama pengguna serta sandi yang dimasukkan oleh nasabah pada situs internet banking. Para pemasang keylogger kemudian dapat mengambil rekaman tersebut dan menggunakannya untuk hal-hal yang tidak diinginkan

Man In The Middle, adalah sebuah serangan di mana penyerang dapat membaca dan memodifikasi pesan-pesan yang dikirim oleh nasabah dengan sistem informasi bank atau sebaliknya.

Karena begitu banyaknya ancaman keamanan pada fasilitas internet banking maka sekarang bank-bank menggunakan kriptografi dan juga pemanfaatan bangking token yang dimaksudkan untuk meningkatkan keamanan..

## II. DASAR TEORI

### 2.1 Internet Banking

Internet Banking , atau Electronic banking (E-Bangking) bisa diartikan sebagai aktifitas perbankan di internet. Layanan ini memungkinkan nasabah sebuah bank dapat melakukan hampir semua jenis transaksi perbankan melalui sarana internet, khususnya via web. Mirip dengan penggunaan mesin ATM, lewat sarana internet seorang nasabah dapat melakukan pengecekan rekening, transfer dana antar rekening, hingga pembayaran tagihan-tagihan rutin bulanan (listrik, telepon, dsb.) melalui rekening banknya. Jelas banyak keuntungan yang akan bisa didapatkan oleh nasabah dengan memanfaatkan layanan ini, terutama bila dilihat dari waktu dan tenaga yang dapat dihemat karena transaksi e-banking jelas bebas antrian dan dapat dilakukan dari mana saja sepanjang nasabah dapat terhubung dengan jaringan internet.

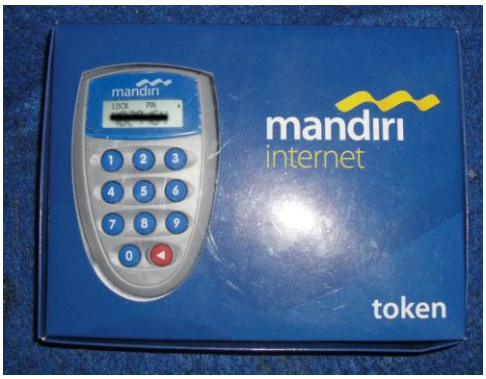
Keamanan merupakan isu utama dalam e-banking karena sebagaimana kegiatan lainnya seperti di internet, transaksi perbankan di internet juga rawan terhadap pengintaian dan penyalahgunaan oleh tangan-tangan yang tidak bertanggung jawab. Oleh karena itu sebuah situs e-banking diwajibkan untuk menggunakan standar keamanan yang sangat ketat untuk menjamin bahwa setiap layanan yang mereka sediakan hanya dimanfaatkan oleh mereka yang memang betul-betul berhak. Salah satu teknik pengamanan yang sering dugunakan dalam e-banking adalah melalui protokol HTTPS (***Secure HTTP*** ).

Dalam studi kasus ini diambil contoh yaitu KlikBCA. Untuk menjamin keamanan transaksi pada Internet Banking KlikBCA makan sisten dilengkapi dengan sistem keamanan berlapis berikut:

- **SSL 128-bit encryption**
  Seluruh data di Internet Banking BCA dikirimkan melalui Secure Socket Layer (SSL) yang mulai diaktifkan sejak Anda login ke IB BCA. SSL akan mengacak data yang dikirim menjadi kode-kode rahasia dengan menggunakan 128-bit encryption yang artinya terdapat 2 pangkat 128 kombinasi angka kunci tetapi hanya satu kombinasi yang dapat membuka kode-kode tsb.
- **User ID dan Personal Identification Number (PIN)**
  Anda harus memasukkan User ID dan PIN IB BCA setiap kali Anda login ke IB BCA.
- **Firewall**
  Firewall berfungsi untuk membatasi akses User yang tidak bertanggung jawab.
- **Otomatis Logout**
  Anda akan "dipaksa" untuk logout bila tidak melakukan transaksi selama 10 menit.
- **Notifikasi**
  Anda akan medapat surat pemberitahuan yang dikirim ke alamat email Anda sebagai konfirmasi atas transaksi finansial yang telah Anda lakukan melalui IB BCA.
- **KeyBCA**
  Alat pengaman tambahan yang dapat menghasilkan password yang berubah-ubah sehingga transaksi finansial yang Anda lakukan di KlikBCA lebih aman.

Security token merupakan objek fisik untuk otentikasi sebuah sistem. Bentuknya bervariasi dan biasanya berukuran kecil dan mudah dibawa. Smart card, ID card, papan bertombol, handphone, gantungan kunci, pemancar infrared/Bluetooth merupakan contoh bentuk security token. Jenis security token yang umum adalah security token untuk infrastruktur kunci public, OTP, dan communication means. Security token yang termasuk ke dalam infrastruktur kunci public berisi data identitas pengguna yang digunakan untuk tanda tangan digital. Sedangkan security token yang termasuk jenis OTP digunakan untuk menghasilkan sandi lewat dan hanya dapat digunakan sekali karena sandi ini akan terus berubah. Dan untuk yang termasuk jenis communication means mempunyai kemampuan untuk mentransmisikan datanya kepada server. Sampai saat ini sebagian besar token yang banyak digunakan untuk fasilitas internet adalah token yang termasuk dalam jenis OTP yang mebangkitkan barisan acak berdasarkan waktu. Dalam hal ini, dibutuhkan sinkronisasi waktu antara waktu pada token dan waktu pada server

**Gambar 1. Contoh Token KlikBCA**




**Gambar 2. Contoh Token Mandiri**

2.2 **Kriptografi**

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

- **Kerahasiaan**, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- **Integritas data**, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- **Autentikasi**, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- **Non-repudiasi.**, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

**Enkripsi** ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi.

## III. PEMBAHASAN

### *A. Algoritma Enkripsi*

Online Bangking umumnya berjalan diatas protocol HTTPS. HTTPS adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web. Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris.

Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers, dan man in the middle attacks. Pada umumnya port HTTPS adalah 443.

Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithma penyandian yang actual Oleh karena itu, pada halaman web digunakan HTTPS, dan URL yang digunakan dimulai dengan ‘https://’ bukan dengan ‘http://’

Ide dasar dari HTTPS adalah untuk membuat sebuah jalur diatas jaringan yang tidak aman. Ini memastikan hal itu maka digunakanlah algoritma enkripsi SSL dan server certificate. Kepercayaan pada HTTPS adalah berdasarrkan sertificate yang dimasukan sebelumnya pada *internet browser* untuk mengetahuin mana sajakah *website* yang dapat dipercaya. Maka dari itu koneksi HTTPS bias dipercaya jika dan hanya jika syarat-syarat berikut terpenuhi :

1. Browser mengimplementasi dengan benar HTTPS dengan sebelumnya memasukan *certificate* yang berwenang
2. Pengguna yakin *certificate* yang berwenang menjamin akses hanya dilakukan pada website yang sah tanpa adanya nama yang menyesatkan
3. Website memberikan *certificate* yang valid yang di-‘tanda tangani’ oleh pihak yang berwenang. Pada umumnya *certificate* yang tidak valid akan memunculkan pesan *error* pada browser
4. Certificate mengindentifikasi dengan tepat dan benar sebuah website.
5. Penggunaan jalur router yang terpercaya ataupun penggunaan algoritma enkripsi yang terpercaya

Dengan memenuhi syarat-syarat diatas maka sebuah jaringan HTTPS dapat digunakan untuk tujuan online bangking.

Algoritma enkripsi yang digunakan untuk mengaman kan saluran HTTPS adalah SSL. SSL adalah sebuah algoritma yang mengijinkan proxy server untuk bertindak sebagai sebuah terowongan antara client dan server. SSL berjalan pada lapisan aplikasi pada protocol TCP/IP dan menyediakan sebuah saluran yang aman untuk bertukar informasi-informasi penting seperti nomor kartu kredit maupun username dan sandi untuk pnline bangking. SSL memanfaatkan *certificate* seperti dijelaskan diatas, juga pertukaran kunci privat dan public dan persetujuan kunci Diffie-Hellman key untuk menyediakana pertukaran kunci yang bersifat rahasia,

autentikasi dan juga integritas degan Message Authentication Code (MAC). Informasi ini juga dikenal sebagai Cypher Suite dan ada didalam **Public Key Infrastructure (PKI)**.

**[Dikarenakan SSL termasuk di dalam algoritma kunci asimetrik yang tidak termasuk dalam bahan makalah 1, maka tidak dilakukan penjelasan mendalam terhadapat algoritma ini]**

### *B. Penggunaan Bangking Token*

Penggunaan Bangking Token pada dasarnya adalah untuk otentikasi. Otentikasi ini bertujuan untuk membuktikan siapa anda sebenarnya, apakah anda benar-benar orang yang anda klaim sebagai dia (who you claim to be). Ada banyak cara untuk membuktikan siapa anda. Metode otentikasi bisa dilihat dalam 3 kategori metode:

1. **Something You Know**
   Ini adalah metode otentikasi yang paling umum. Cara ini mengandalkan kerahasiaan informasi, contohnya adalah password dan PIN. Cara ini berasumsi bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali anda seorang.

2. **Something You Have**
   Cara ini biasanya merupakan faktor tambahan untuk membuat otentikasi menjadi lebih aman. Cara ini mengandalkan barang yang sifatnya unik contohnya adalah kartu magnetik/smartcard, hardware token, USB token dan sebagainya. Cara ini berasumsi bahwa tidak ada seorangpun yang memiliki barang tersebut kecuali anda seorang.

3. **Something You Are**
   Ini adalah metode yang paling jarang diapakai karena faktor teknologi dan manusia juga. Cara ini mengandalkan keunikan bagian-bagian tubuh anda yang tidak mungkin ada pada orang lain seperti sidik jari, suara atau sidik retina. Cara ini berasumsi bahwa bagian tubuh anda seperti sidik jari dan sidik retina, tidak mungkin sama dengan orang lain.

Pada otentikasi pada online bangking menggunakan Two Factor Authentication yang menggunakan 2 dari factor (metode) yang berbeda dengan tujuan untuk meningkatkan keamanan. Otentikasi pada e-bangking mengkombinasikan "Something You Know" berupa pin dan "Something You Have" berupa bangking token itu sendiri.

Pada e-bangking untuk BCA dan Mandiri, token berfungsi untuk men-generate password/PIN menjadi sebuah sandi yang dinamis dimana sandi ini akan dihasilkan setiap satuan waktu tertentu. Semakin pendek rentang waktu dalam pembuatan sandi ini maka tingkat keamanan system akan semakin tinggi. Contohnya adalah bangking token BCA dan Mandiri yang menghasilkan sandi dinamis tersebut setiap 8 detik. sehingga password yang digunakan dalam sistem selalu berubah-ubah. Dengan arti, sistem akan meminta password yang berlainan setiap 8 detik, ini yang menyebabkan system yang digunakan menjadi lebih secure. Bagaimana bila user memasukan sandi setelah 8 detik? Token pada online bangking menggunakan teknologi online window sehingga server masih dapat mengenali beberapa value sandi pada interval waktu tertentu. Dalam kasus ini *server* menyimpan semua sandi yang dihasilkan dalam waktu tertentu sehingga bila user terlambat dalam memasukan sandi tersebut, sandi tersebut tetap bias digunakan tetapi hanya pada selang waktu tertentu.

Bangkin token untuk online bangking pada BCA dan Mandiri dibuat oleh sebuah perusahaan yang sama sehingga keduanya mempunyai fungsi yang sama. Terdapat 3fungsi pada bangking token tersebut yaitu :

- Response Only (RO), aplikasi ini memiliki 2 variable yaitu, secred/seed value dan time (waktu saat ini), untuk men-generate password/pin.
- Challenge Response (C/R), aplikasi ini memiliki 3 variable yaitu, secred/seed value dan time (waktu saat ini) & challenge yaitu berupa angka dengan digit tertentu yang digenerate oleh server VA yang harus di input ke dalam token, untuk men-generate password/pin.
  Salah satu fungsi dari aplikasi C/H ini adalah untuk menghidari jebakan pada website palsu ,seperti yang pernah terjadi pada klikbca. karena website tersebut tidak mungkin menampilkan angka challenge dari server VA.
- Digital Signature, aplikasi ini mirip dengan C/H, hanya saja challenge yang disediakan lebih dari 1 challenge (max 8) yang dapat diinputkan kedalam token, dan challenge ini tidak berasal dari server VA, bisa berupa angka dari mana saja. fungsi dari aplikasi ini salah satunya adalah untuk transfer uang antar rekening. field/challenge yang digunakan olek BCA/mandiri adalah 3 buah. field 1 = no rekening pengirim, field 2 no rekening tujuan, field 3 = nominal tranfer. ketiga filed ini dikombinasikan dengan secret/seed value & time, akan menghasilkan pin/password.

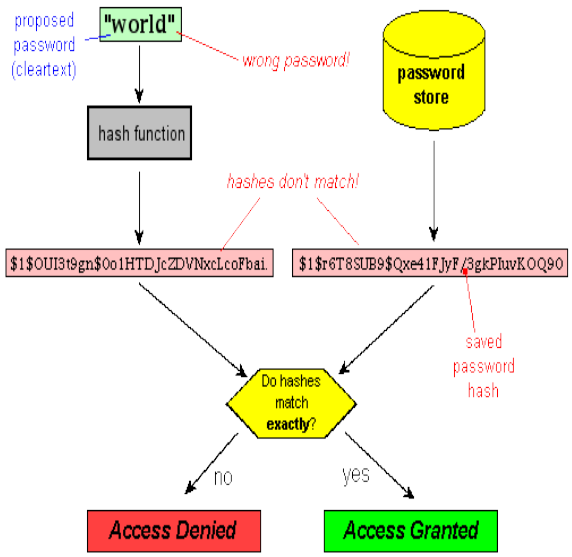
Penggunaan dari fungsi-fungsi diatas berbeda untuk setiap transaksi yang dilakukan. Misalkan untuk melakukan transfer antar rekening maka akan digunakan fungsi Digital Signature.

Selain itu untuk alasan keamanan maka sandi yang disimpan dalam server disimpan dalam bentuk hash sehingga sandi yang diperoleh dari token akan dikirimkan dalam bentuk hash ketika dikirimkan ke server. Fungsi yang digunakan disini adalah fungi MD 5 yang digunakan secara luas dengan *hash value* 128-bit. Fungsi MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file.

Algoritma MD5 yang utama beroperasi pada kondisi 128-bit, dibagi menjadi empat*word* 32-bit, menunjukkan *A*, *B*, *C* dan *D*. Operasi tersebut di inisialisasi dijaga untuk tetap konstan. Algoritma utama kemudian beroperasi pada masing-masing blok pesan 512-bit, masing-masing blok melakukan pengubahan terhadap kondisi.Pemrosesan blok pesan terdiri atas empat tahap, batasan *putaran*; tiap putasan membuat 16 operasi serupa berdasar pada fungsi non-linear *F*, tambahan modular, dan rotasi ke kiri. Gambar satu mengilustrasikan satu operasi dalam putaran. Ada empat macam kemungkinan fungsi *F*, berbeda dari yang digunakan pada tiap-tiap putaran

$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

Proses otentikasi setelah dilakukan fungsi hash dapat dilihat pada gambar berikut.




**Gambar 3. Proses Otentikasi**

Meskipun fungsi hash digunakan disini tetapi itu tidak lah cukup dikarenakan meskipun fungsi dikatakan sebagai sebuah fungsi yang satu arah tetapi tetap dapat dipecahkan dengan menggunakan database pemetaan terhadap fungsi hash tersebut. Salah satu contoh database hash online yang bisa dipakai untuk crack hash adalah gdataonline.com/seekhash.php . Misalkan kunci token adalah "secret". Jika dalam situs tersebut kita mencoba masukkan nilai 5ebe2294ecd0e0f08eab7690d2a6ee69, maka situs tersebut akan memberikan hasil "secret". Hal ini disebabkan karena situs tersebut telah menyimpan pemetaan informasi secret <=> 5ebe2294ecd0e0f08eab7690d2a6ee69.

Dikarenakan hal ini maka sebelum dikirmkan ke server terlebih dahulu kunci ditambahkan string acak yang disebut dengan salt. karena nilai salt ini dibangkitkan secara random, maka tiap user memiliki nilai salt yang berbeda sehingga tidak mungkin attacker bisa membangun database pemetaan antara plaintext dan hash secara lengkap.

Penggunaan Kriptografi pada pemanfaatan bangking token ini terdapat pada bagaimana token tersebut menghasilkan sebuah kunci yang dinamis yang bersifat One Time Password dikarenakan penggunaan variable berupa waktu dan variable lainnya yang bersangkutan. Sehingga antara sebuah token dan token lainnya tidak akan menghasilkan sebuah kunci yang sama dan token yang sama tidak akan menghasilkan kunci yang sama walaupun pembuatan kunci dinamis diulang berkali-kali. Jadi bisa disimpulkan bahwa password yang dikeluarkan token bersifat:

1. Selalu berubah-ubah secara periodik
2. Memiliki umur yang singkat
3. Hanya bisa dipakai 1 kali

### *C. Kelemahan Keamanan*

Meskipun telah digunakan saluran HTTPS dan juga bangking token, online bangking masih mempunyai beberapa kelemahan yaitu penggunaan program seperti Trojan dan Malware.

Hal ini tetap dimungkinkan apabila seorang hacker melakukan penjebolan jaringan dalam waktu nyaris bersamaan. Dikarenakan server hanya mengautentikasi apakah user memasukan username dan sandi yang tepat, tetapi tidak dilakukan pengecekan apa sandi dinamis tersebut sudah pernah digunakan atau tidak sebelumnya. Walaupun terdapat kelemahan seperti ini kejadian tersebut bisa dibilang sangat jarang sekali terjadi.

Selain itu juga menurut penelitian yang dilakuakan terdapat beberapa kelemahan yang disebabkan oleh user yang tidak berhati-hati. Serangan-serangan seperti menghilangkan indicator HTTPS, gambar autentikasi, dan kemunculkan pesan error yang diabaikan merupakan beberapa diantaranya. Menurut penelitian lebih 80% user yang dicoba tidak menyadari serangan-serangan seperti ini dan hal ini tidak dapat sepenuhnya ditangani oleh system. Sehingga hacker dapat dengan gampang mengambil informasi dari user. Dikarenakan itu sebagai user kita harus meningkatkan perhatian terhadap ancaman-ancaman seperti ini.

## V. KESIMPULAN

Dengan menggunakan fasilitas Internet Banking, nasabah dapat dengan mudah melakukan transaksi perbankan dengan menggunakan internet. Fasilitas ini sudah banyak disediakan oleh bank-bank di Indonesia seperti Bank Mandiri dan BCA. Akan tetapi fasilitas ini rawan serangan keamanan seperti phising, keylogger, dan man in the middle.

Oleh karena itu dilakukan beberapa usaha untuk

meningkatkan keamanan itu yaitu penggunaan kriptografi dalam prosesnya seperti protocol HTTPS yang memanfaatkan algortima Secure Socket Layer (SSL) dan juga penggunaan Bangking token yang mampu menghasilkan sandi yang dinamis dan bersifat One Time Password. Meskipun begitu masih terdapat kelemahan keamanan pada online bangkin walaupun hal tersebut jarang sekali terjadi.

## REFERENCES


1. Schneier, Bruce, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996.
2. Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
3. Adikusuma, Yan. Tia Narang Ali, Tri Wahyudi. Secure Authentication for Internet Banking with SMS Key, 2009.
4. Schechter,Stuart E. Rachna Dhamija, Andy Ozment, and Ian Fische. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies
5. http://www.klikbca.com
6. http://www.vasco.com/


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

ttd

Marvello Oni
13508031

**Lampiran**

```
//Catatan: Seluruh variable pada unsigned integer 32-bit dan dan wrap modulo

//Mendefinisikan r sebagai berikut
var int[64] r, k
r[ 0..15] := {7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22}
r[16..31] := {5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20}
r[32..47] := {4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23}
r[48..63] := {6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21}

//Menggunakan bagian fraksional biner dari integral sinus sebagai konstanta:
for i from 0 to 63
    k[i] := floor(abs(sin(i + 1)) × 2^32)

//Inisialisasi variabel:
var int h0 := 0x67452301
var int h1 := 0xEFCDAB89
var int h2 := 0x98BADCFE
var int h3 := 0x10325476

//Pemrosesan awal:
append "1" bit to message
append "0" bits until message length in bits ≡ 448 (mod 512)
append bit length of message as 64-bit little-endian integer to message

//Pengolahan pesan paada kondisi gumpalan 512-bit:
for each 512-bit chunk of message
    break chunk into sixteen 32-bit little-endian words w(i), 0 ≤ i ≤ 15

    //Inisialisasi nilai hash pada gumpalan ini:
    var int a := h0
    var int b := h1
    var int c := h2
    var int d := h3

    //Kalang utama:
    for i from 0 to 63
        if 0 ≤ i ≤ 15 then
            f := (b and c) or ((not b) and d)
            g := i
        else if 16 ≤ i ≤ 31
            f := (d and b) or ((not d) and c)
            g := (5×i + 1) mod 16
        else if 32 ≤ i ≤ 47
            f := b xor c xor d
            g := (3×i + 5) mod 16
        else if 48 ≤ i ≤ 63
            f := c xor (b or (not d))
            g := (7×i) mod 16

        temp := d
        d := c
```

```
        c := b
        b := ((a + f + k(i) + w(g)) leftrotate r(i)) + b
        a := temp

    //Tambahkan hash dari gumpalan sebagai hasil:
    h0 := h0 + a
    h1 := h1 + b
    h2 := h2 + c
    h3 := h3 + d

var int digest := h0 append h1 append h2 append h3 //(diwujudkan dalam little-
endian)
```