Analisis Penggunaan Kriptografi pada Proses Autentikasi BCA Mobile

Brandon Jonathan Latif (18220103)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): brandonjonathan7320@gmail.com

***Abstract*—Dalam era yang terus berkembang, peran teknologi semakin penting dalam berbagai aspek kehidupan manusia, termasuk dalam bidang keuangan. Namun, perkembangan teknologi juga membawa potensi celah keamanan yang perlu diatasi. Bank Central Asia (BCA), salah satu bank terbesar di Asia, telah mengadopsi teknologi untuk meningkatkan layanan perbankan kepada nasabahnya. Salah satu teknologi yang digunakan oleh BCA untuk meningkatkan aksebilitas layanan perbankan adalah aplikasi mobile BCA Mobile. Penelitian ini bertujuan untuk menganalisis langkah-langkah keamanan yang diimplementasikan dalam proses autentikasi aplikasi BCA Mobile. Hasil penelitian menunjukkan bahwa BCA telah berhasil mengembangkan berbagai fungsi pengaman dalam proses autentikasi aplikasi BCA Mobile. Fungsi-fungsi yang menggunakan teknologi kriptografi bermanfaat untuk menjaga kerahasiaan informasi dan menjaga kebenaran informasi sehingga proses autentikasi aplikasi BCA Mobile dapat memastikan bahwa hanya pengguna yang sah yang dapat melakukan akses layanan-layanan yang tersedia. Hasil penelitian ini diharapkan dapat memberikan wawasan tentang pentingnya keamanan dalam aplikasi perbankan.**

Keywords—BCA Mobile; Kriptografi; Enkripsi; Autentikasi; Mobile Banking; Keamanan

I. PENDAHULUAN

Pada zaman yang terus berkembang, teknologi yang dikembangkan manusia menjadi lebih maju dan lebih kompleks. Teknologi yang dikembangkan manusia telah berhasil membantu manusia dalam menyelesaikan berbagai macam masalah maupun melewati berbagai macam rintangan sehingga manusia sampai di titik ini. Teknologi-teknologi yang dikembangkan oleh manusia beragam. Mulai dari waktu yang lampau dimana manusia berhasil mengembangkan teknologi untuk membantu proses berburu dan bercocok tanam hingga melakukan pendaratan manusia pertama di bulan. Teknologi telah berhasil membawa manusia melewati berbagai macam zaman dan merubah cara hidup manusia pada zaman-zaman tersebut.

Dewasa ini, manusia berhasil mengembangkan teknologi-teknologi baru yang kemudian mengubah cara hidup. Keseharian manusia dipenuhi dengan memanfaatkan teknologi, mulai dari proses pengolahan makanan dengan menggunakan oven dan *air fryer*, penulisan makalah dengan menggunakan komputer dan internet, hingga melakukan pembayaran secara virtual dengan menggunakan teknologi *mobile banking*.

Bank swasta terbesar di Indonesia, Bank Central Asia (BCA) telah berhasil mengimplementasikan berbagai macam teknologi dalam meningkatkan kualitas layanan perbankannya, seperti diluncurkannya aplikasi *mobile banking* yang dinamakan BCA Mobile. Dengan adanya BCA Mobile, proses transfer uang yang sebelumnya mengharuskan nasabah untuk mencari sebuah mesin ATM, dapat dilakukan dengan mudah dan cepat melalui beberapa ketukan pada ponsel nasabah. Begitu pula dengan proses-proses layanan perbankan lainnya. Bahkan dengan memanfaatkan BCA Mobile, BCA berhasil mengembangkan layanan-layanan perbankan baru yang sebelumnya tidak dapat dilakukan, seperti QRIS.

Namun dengan segala manfaat dan kemudahan yang berhasil ditawarkan oleh BCA Mobile, terdapat juga masalah-masalah baru bermunculan. Baik masalah-masalah lama yang bertransformasi bentuk menjadi digital, seperti masalah penipuan yang masih kerap terjadi. Dengan adanya layanan BCA Mobile yang dapat diakses kapan saja dan dimana saja, penipuan menjadi lebih sering terjadi pada nasabah-nasabah yang kurang teliti. Muncul juga masalah-masalah baru yang sebelumnya tidak pernah terjadi sebelum peluncuran BCA Mobile, seperti pembajakan akun nasabah atau kebocoran informasi-informasi penting sehingga para pelaku mendapatkan akses ke akun nasabah dan melakukan pengurasan uang nasabah.

BCA sebagai pihak penyedia layanan BCA Mobile telah melakukan berbagai macam usaha untuk mengurangi kemungkinan terjadinya berbagai insiden selama masa hidup BCA Mobile. Contoh usaha yang dilakukan oleh BCA adalah proses autentikasi yang perlu dilakukan oleh setiap nasabah untuk mendapatkan akses layanan-layanan pada BCA Mobile. Proses autentikasi yang diimplementasikan oleh BCA pada BCA Mobile mengandung berbagai macam konsep dalam ilmu kriptografi untuk menjaga kerahasiaan data maupun pertukaran data yang dilakukan melalui layanan-layanan yang disediakan oleh aplikasi.

Kriptografi adalah sebuah teknik untuk melindungi informasi di dalam saluran komunikasi. Metode ini memungkinkan pengirim dan penerima pesan saja yang bisa melihat isi informasi di dalamnya. [1]

BCA Mobile memanfaatkan API dalam menyediakan seluruh layanan-layanannya. API BCA menggunakan Oauth 2.0 sebagai *framework* autentikasinya. Ilmu-ilmu kriptografi

yang digunakan meliputi SHA-256, SHA-512, HMAC, RSA, dan *signature*.

Penelitian dan penulisan laporan penelitian didasarkan pada rasa penasaran dan keingintahuan penulis, sebagai salah satu pengguna aplikasi BCA Mobile mengenai komponen-komponen penyusun proses autentikasi dan bagaimana hubungan antara komponen-komponen tersebut dalam menjaga keamanan pada BCA Mobile.

II. Metode

A. *Pengalaman Pribadi*

Pengalaman pribadi penulis menjadi salah satu metode pada penelitian dan penyusunan laporan penelitian ini. Penulis telah menggunakan aplikasi BCA Mobile selama lebih dari 3 tahun dengan frekuensi pemakaian harian pada waktu penulisan laporan ini.

B. *Studi Literatur*

Studi literatur menjadi metode utama pada penelitian dan penyusunan laporan penelitian ini. Studi literatur dilakukan pada situs-situs yang tersedia di internet, materi kuliah, serta dokumentasi ofisial yang diterbitkan oleh BCA.

C. *Batasan Penulisan*

Penelitian dan penulisan laporan penelitian ini dibatasi pada bahasan proses autentikasi aplikasi BCA Mobile serta komponen-komponen penyusunnya.

III. Landasan Teori

A. *Kriptografi*

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kriptografi atau *cryptography* berasal dari bahasa Yunani, yaitu cryptós yang berarti rahasia dan gráphein yang berarti tulisan, sehingga dapat disimpulkan bahwa kriptografi adalah tulisan-tulisan rahasia. [2]

Ilmu kriptografi mendukung beberapa aspek keamanan.

- Confidentiality / Privacy / Secrecy: pesan yang dikirim terjaga kerahasiannya.
- Integrity: pesan yang dikirimkan terjaga keasliannya.
- Authentication: pesan berasal dari pengirim yang asli dan diterima oleh penerima yang asli.
- Non-repudation: pengirim pesan tidak dapat menyangkal telah mengirim pesan.

Seperti pada ilmu-ilmu lainnya, pada ilmu kriptografi juga terdapat beberapa terminologi yang sering digunakan.

- Message: informasi pada keadaan awalnya sebelum dipengaruhi oleh proses apapun. Informasi dapat berupa berbagai macam bentuk, seperti teks (*plaintext*), gambar (*plain-image*), vidio (*plain-video*), dan berbagai macam bentuk lainnya.
- Enkripsi: sebuah proses yang mengubah *message* awal menjadi sebuah bentuk lain yang tidak bermakna dan menyembunyikan isi pesan awalnya.
- Ciphertext: hasil enkripsi sebuah *message* yang tidak bermakna. Ciphertext menyembunyikan isi pesan message sebelum dienkripsi.
- Dekripsi: sebuah proses yang mengubah ciphertext menjadi *message* semula.
- Key: sebuah parameter pada proses enkripsi dan dekripsi yang menentukan hasilnya. Sebuah proses enkripsi ataupun dekripsi yang sama dapat menghasilkan yang berbeda ketika menggunakan key yang berbeda.
- Pengirim: pihak yang mengirimkan *message* semula. Pengirim memiliki banyak wujud, manusia ataupun komputer, tergantung pada konteksnya.
- Penerima: pihak yang menerima *message* yang sudah melalui proses enkripsi. Sama seperti pengirim, penerima juga memiliki banyak wujud, manusia ataupun komputer, tergantung pada konteksnya.
- Penyadap: pihak ketiga yang mencoba untuk menyadap atau mencuri informasi yang dikirmkan oleh pengirim ke penerima. Pada umumnya, informasi yang dikirimkan oleh pengirim sudah dienkripsi dan berada dalam bentuk *ciphertext*.

Kriptografi sudah ada sejak zaman dahulu, bahkan sebelum Masehi. Oleh karena itu, kriptografi dikelompokkan menjadi 2 kategori, kriptografi lama dan kriptografi modern. Perbedaan kriptografi lama dengan kriptografi modern hanya terletak pada media yang digunakan untuk menuliskan kriptografi tersebut, kriptografi lama menggunakan kertas, sedangkan kriptografi modern menggunakan komputer.

B. *Bank Central Asia (BCA)*

Bank Central Asia atau yang biasa disingkat sebagai BCA merupakan sebuah bank swasta yan didirikan pada 21 Februari tahun 1957 dengan nama Bank Central Asia, N. V. BCA buka untuk publik pada tahun 2002 dan mengganti namanya menjadi PT Bank Central Asia, Tbk. Kantor pusat BCA terletak di jalan Jenderal Sudirman Kav. 22-23, Jakarta Selatan. [3]

Gambar 1. Logo BCA (sumber: https://upload.wikimedia.org/wikipedia/commons/thumb/5/5c/Bank_Central_Asia.svg/2560px-Bank_Central_Asia.svg.png)

Pada saat penulisan laporan, total asset BCA mencapai 1.322 triliun rupiah. BCA memiliki sebanyak 1.247 kantor cabang, 18.348 mesin ATM, serta lebih dari 35 juta rekening nasabah yang terdaftar. [4]

Visi yang dipegang oleh BCA adalah “Bank pilihan utama andalan masyarakat, yang berperan sebagai pilar penting perekonomian Indonesia”. Sedangkan terdapat 3 misi yang menjadi acuan perusahaan BCA.

- Membangun institusi yang unggul di bidang penyelesaian pembayaran dan solusi keuangan bagi nasabah bisnis dan perseorangan
- Memahami beragam kebutuhan nasabah dan memberikan layanan finansial yang tepat demi tercapainya kepuasan optimal bagi nasabah
- Meningkatkan nilai francais dan nilai stakeholder BCA

C. *BCA Mobile*

BCA Mobile merupakan sebuah layanan produk perbankan PT Bank Central Asia Tbk. yang dapat diakses secara langsung oleh nasabah melalui telepon seluler / handphone. [5]

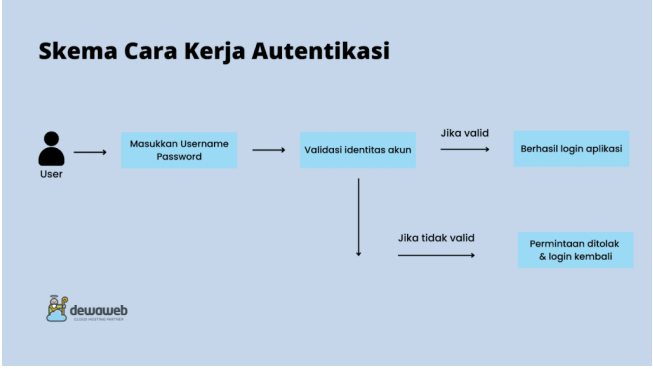
Gambar 2. Logo BCA Mobile (sumber: https://play-lh.googleusercontent.com/ggZzVVDWsTm7gSnVl8m3cNFgoeUN2r7dhAZdB8lz0d_s6ZcYOkvUQdbG3dPU5LHZnWvc)

BCA Mobile memiliki 9 fitur yang beragam. Berikut merupakan fitur-fitur yang terdapat pada BCA Mobile. [6]

- Debit Contactless: kartu debit yang memiliki fitur pembayaran dengan teknologi nirkontak yang memungkinkan nasabah untuk dapat melakukan transaksi hanya dengan mendekatkan kartu debit pada mesin EDC.
- QRIS: metode transaksi menggunakan kode QR berstandar Indonesia yang dikeluarkan oleh Bank Indonesia dengan melakukan scan QR, kemudian melakukan pembayaran dengan mudah di semua toko / outlet yang sudah mendukung penggunaan QRIS.
- Lifestyle: fitur yang mengakomodasi berbagai kebutuhan transaksi, seperti donasi, zakat, tiket bioskop, gadget, atraksi dan rekreasi, kesehatan, dan sebagainya.
- Debit Online: fitur kartu debit BCA Mastercard yang memberikan kemudahan pembayaran transaksi di berbagai situs, aplikasi, atau layanan offline.
- m-Payment: memudahkan transaksi, seperti membayar tagihan pascabayar handphone, kartu kredit, asuransi dan sebagainya.
- Buka Tabungan: membuka tabungan BCA.
- BagiBagi: fitur untuk berbagi uang melalui aplikasi BCA Mobile bagi pengguna yang memiliki aplikasi Sakuku.
- BCA Keyboard: transaksi perbankan di layar smartphone tanpa harus membuka BCA Mobile.
- Cardless: Transaksi setor tunai dan tarik tunai tanpa kartu.

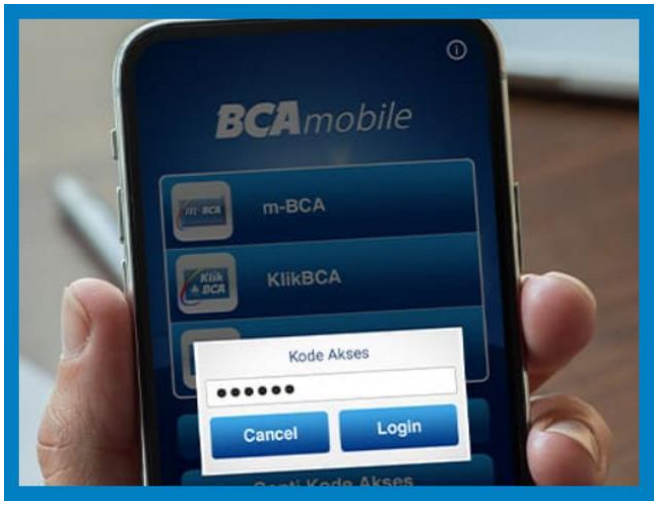
D. *Autentikasi*

Autentikasi adalah proses validasi atau pembuktian terhadap identitas atau kredensial yang hendak memasuki sebuah sistem atau layanan yang penting. Autentikasi ini dilakukan untuk membuktikan bahwa pengguna yang hendak login benar-benar pemilik akun yang sah. [7]



Gambar 3. Skema Cara Kerja Autentikasi (sumber: https://dwblog-ecdf.kxcdn.com/wp-content/uploads/2022/10/cara-kerja-autentikasi-1024x576.png)

Hampir semua sistem memiliki proses autentikasi untuk memastikan bahwa pengguna yang hendak menggunakan sistem tersebut benar merupakan pengguna yang memiliki wewenang. Begitu pula dengan BCA Mobile. Sebelum pengguna dapat menggunakan layanan-layanan pada aplikasi BCA Mobile, pengguna harus melewati proses autentikasi. Proses autentikasi pada BCA Mobile yang harus diperhatikan oleh pengguna hanya memasukan kode akses pada kolom yang telah ditampilkan. Sedangkan proses autentikasi sebenarnya yang terjadi di belakang layar, antara gawai yang digunakan dengan API BCA.



Gambar 4. Tampilan Autentikasi BCA Mobile (sumber: https://www.norekening.com/wp-

content/uploads/2023/02/cara-buat-kode-akses-bca-mobile-re.jpg)

E. Algoritma RSA

Algoritma RSA merupakan sebuah algoritma kunci publik yang ditemukan oleh tiga peneliti dari Massachussets Institute of Technology (MIT), yaitu Ronald Rivest, Adi Shamir, dan Len Adleman pada tahun 1976. Semenjak itu, algoritma RSA menjadi algoritma yang paling terkenal dan paling banyak diaplikasikan pada berbagai macam sistem. Titik kuat algoritma RSA adalah pada sulitnya memfaktorkan bilangan bulat yang besar menjadi faktor-faktor prima. [8]

Berikut merupakan langkah-langkah penyusun algoritma RSA.

Inisialisasi p dan q sebagai bilangan prima yang berbeda.

$$n = p \, . \, q \tag{1}$$

Inisialisasi n yang bernilai hasil kali p dengan q.

$$\phi(n) = (p - 1) \, . \, (q - 1) \tag{2}$$

Inisialisasi ϕ(n) yang bernilai hasil kali p - 1 dengan q - 1. Inisialisasi e sebagai sebuah bilangan bulat yang relatif prima terhadap ϕ(n).

$$d \, . \, e = 1 + k \, \phi(n) \tag{3}$$

Inisialisai d yang dapat dihitung dengan persamaan diatas atau dengan menggunakan algoritma Euclidean. k merupakan bilangan bulat terkecil yang dapat menghasilkan d sebagai bilangan bulat.

e dan n merupakan key publik yang dapat dipublikasikan ke umum. Sedangkan d dan n merupakan key privat yang tidak dipublikasikan ke umum dan hanya diketahui oleh pemegang kunci tersebut karena key privat akan digunakan untuk mendekripsi pesan yang telah dienkripsi menggunakan key publik.

Plaintext yang hendak dienkripsi dibagi-bagi menjadi blok-blok dengan ukuran yang sama satu dengan yang lainnya.

$$c_i = m_i^e \bmod n \tag{4}$$

Proses enkripsi dilakukan dengan menghitung nilai masing-masing blok plaintext yang dilambangkan dengan i menggunakan persamaan diatas. Hasil perhitungan tersebut menghasilkan nilai ciphertext.

$$m_i = c_i^d \bmod n \tag{5}$$

Proses dekripsi dilakukan dengan menghitung nilai masing-masing block ciphertext yang dilambangkan dengan i menggunakan persamaan diatas. Hasil perhitungan tersebut akan menghasilkan nilai message yang sama dengan nilai plaintext.

F. Fungsi Hash

Fungsi hash merupakan sebuah fungsi yang digunakan untuk mengkompresi sebuah pesan M berukuran sembarang menjadi sebuah string h yang berukuran *fixed*. [9]

Fungsi hash merupakan sebuah fungsi yang bersifat satu arah. Hasil yang didapatkan setelah melakukan fungsi hash pada sebuah pesan disebut *message digest. Message digest* yang didapatkan tidak dapat dikembalikan menjadi semula karena pada proses hashing, jumlah karakter pada pesan mengalami perubahan dari jumlah aslinya, sehingga *message digest* yang didapatkan tidak dapat dikembalikan menjadi pesan semula. *Message digest* yang didapatkan juga memiliki panjang yang tidak berubah-ubah, meskipun pesan yang dihash memiliki jumlah karakter yang sedikit ataupun jumlah karakter yang banyak.

Terdapat beberapa sifat dari fungsi hash.

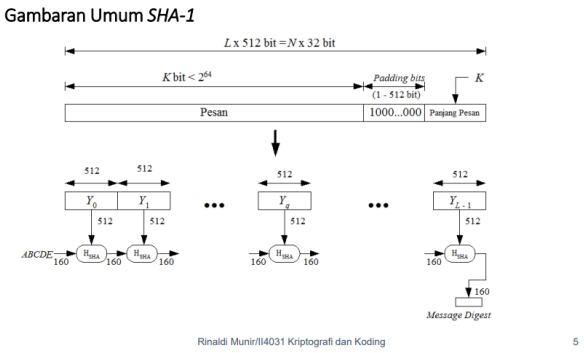
- Collision Resistance: sangat sulit untuk menemukan 2 pesan berbeda yang akan menghasilkan *message digest* yang sama.
- Preimage Resistance: sangat sulit untuk menemukan sebuah pesan yang akan menghasilkan suatu *message digest* sembarang.
- Second Preimage Resistance: sangat sulit untuk menemukan sebuah pesan yang menghasilkan *message digest* yang sama dengan *message digest* yang dihasilkan dari sebuah pesan lain.

Seiring berjalannya waktu, jumlah fungsi hash yang dapat digunakan terus bertambah. Dimulai dari SHA-0, SHA-1, SHA-3, dan fungsi-fungsi hash lainnya, seperti WHIRLPOOL ataupun Grøstl.

G. Fungsi Hash SHA-1

SHA-1 merupakan salah satu varian pada keluarga fungsi hash SHA. SHA-1 memanfaatkan penambahan bit-bit pengganjal / *padding bit* dan penambahan nilai panjang pesan semula. Kemudian melakukan pengolahan pesan dalam ukuran 512 bit dengan menggunakan bit penyangga / bit *buffer*.

Berikut merupakan langkah-langkah penyusun algoritma SHA-1 dengan mengolah pesan M hingga menghasilkan sebuah *message digest.*



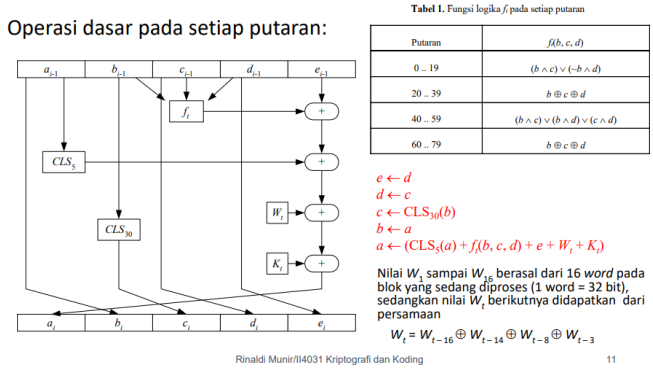
Gambar 5. Gambaran umum proses fungsi hash SHA-1 (sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/19%20-%20Fungsi-hash-SHA-2021.pdf)

Pesan ditambah dengan *padding bit* sehingga hasil bagi panjang pesan dengan 512 menghasilkan 448. *Padding bit* yang ditambahkan terdiri atas bit 1 yang diikuti dengan bit 0.

Setelah pesan ditambahkan dengan *padding bit*, pesan ditambahkan dengan 64 bit tambahan yang bernilai panjang bit semula sehingga panjang bit total habis dibagi 512.

Tahap selanjutnya memerlukan 5 buah penyangga dengan panjang masing-masing 32 bit, sehingga panjang totalnya adalah 160 bit. Penyangga diinisialisasikan dalam bentuk *hexadecimal* dan diberi nama A, B, C, D, dan E.

Pengolahan pesan selanjutnya dilakukan dalam blok yang masing-masing berukuran 512 bit sebanyak 80 kali putaran. Setiap 20 putaran akan menggunakan sebuah bilangan penambah yang berubah-ubah. Bilangan penambah memiliki panjang 32 bit dengan bentuk *hexadecimal*. Berikut merupakan operasi dasar yang akan dilakukan pada setiap putaran.

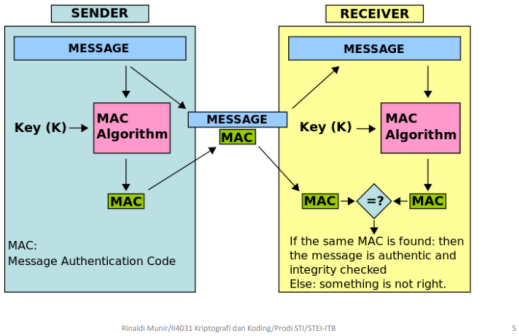


Gambar 6. Operasi dasar pada setiap putaran (sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/19%20-%20Fungsi-hash-SHA-2021.pdf)

H. HMAC

Message Authentication Code (MAC) merupakan sebuah kode yang dihasilkan oleh fungsi hash satu arah yang menggunakan kunci rahasia (secret key) dalam pembangkitan *message digest*-nya. [10]

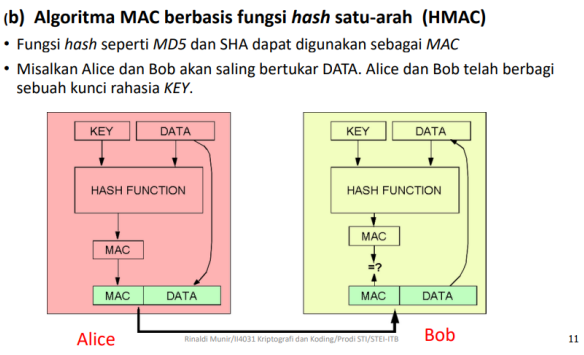
MAC merupakan sebuah kode yang dihasilkan dari pesan yang telah melalui proses algoritma MAC menggunakan kunci K. MAC kemudian dilekatkan dengan pesan semula dan dikirimkan oleh pengirim kepada penerima. Penerima lalu melepaskan MAC dari pesan semula dan melakukan proses algoritma MAC lagi pada pesan yang dikirimkan. Jika kode yang dihasilkan sama dengan MAC yang dilekatkan pada pesan, penerima dapat menyimpulkan bahwa pesan masih orisinil dan tidak mengalami modifikasi apapun.



Gambar 7. MAC (sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/22%20-%20MAC-2021.pdf)

Namun, pengirim juga dapat memanfaatkan fungsi hash yang sudah ada, seperti MD5 ataupun SHA untuk membangkitkan MAC. Dengan menggunakan suatu fungsi hash, key dan pesan dapat diolah dengan fungsi hash untuk menghasilkan suatu *message digest*. *Message digest* tersebut akan bertindak seperti MAC dan dilekatkan pada pesan kemudian dikirimkan ke penerima. Penerima akan melepaskan MAC dari pesan kemudian melakukan ulang fungsi hash menggunakan pesan yang didapatkan dengan key yang sama dengan key yang digunakan oleh pengirim. Jika *message digest* yang didapatkan oleh penerima setelah melakukan fungsi hash sama dengan MAC yang diterima, pengirim dapat memastikan bahwa pesan yang dikirim orisinil dan tidak mengalami modifikasi apapun.

SHA-1 merupakan salah satu varian pada keluarga fungsi hash SHA. SHA-1 memanfaatkan penambahan bit-bit pengganjal / *padding bit* dan penambahan nilai panjang pesan semula. Kemudian melakukan pengolahan pesan dalam ukuran 512 bit dengan menggunakan bit penyangga / bit *buffer*.



Gambar 8. HMAC (sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/22%20-%20MAC-2021.pdf)

I. Digital Signature

Digital Signature merupakan sebuah nilai kriptografis yang bergantung pada isi pesan dan kunci. *Digital Signature* akan selalu berbeda antara satu dokumen dengan dokumen lainnya yang tidak identik. [11]

Terdapat 2 cara untuk melakukan *Digital Signature*, yaitu dengan menggunakan kriptografi kunci simetri, atau dengan menggunakan kriptografi kunci publik. Namun penggunaan kriptografi tidak non-repudiation karena kunci yang digunakan untuk menandatangani diketahui oleh lebih dari 1 pihak. Cara untuk mengatasinya adalah dengan menggunakan pihak ketiga yang dapat dipercaya untuk menengahi kedua belah pihak yang hendak melakukan pengiriman pesan. Pihak ketiga dapat memastikan bahwa pengirim pesan tidak dapat melakukan penyangkalan. Namun, menggunakan pihak ketiga akan memakan lebih banyak usaha yang seharusnya tidak diperlukan jika menggunakan kriptografi kunci publik.

Digital Signature yang menggunakan kriptografi kunci publik memiliki sedikit perbedaan dengan konsep kriptografi kunci publik pada dasarnya. Pada umumnya, kriptografi kunci publik akan menggunakan kunci publik penerima untuk melakukan enkripsi pesan. Namun bila konsep ini diimplementasikan pada *Digital Signature*, bukti otentikasi tidak didapatkan karena kunci publik penerima diketahui oleh semua orang. Dengan membalikan pemanfaatan kunci publik, hasil yang didapatkan akan menjadi berbeda.

Bila *Digital Signature* dilakukan dengan menggunakan kunci privat pengirim untuk melakukan proses enkripsi, kerahasiaan pesan tetap terjaga karena hanya penerima yang menerima pesan dan dapat mendekripsi dengan kunci publik pengirim dan otentikasi didapatkan karena pesan pasti berasal dari pengirim karena hanya pengirim yang mengetahui kunci privatnya.

Digital Signature pada umumnya akan dilekatkan pada pesan semula atau melalui media terpisah yang sama-sama ditujukan kepada penerima. Penerima kemudian mendekripsi *Digital Signature*, kemudian membandingkan hasil dekripsi tersebut dengan pesan yang dikirimkan. Bila hasil dekripsi dan pesan yang dikirim sama, penerima dapat menyimpulkan bahwa pesan orisinil dan tidak mengalami modifikasi sama sekali.

Namun, seringkali kerahasiaan pesan tidak diperlukan, melainkan hanya otentikasi yang diperlukan. Oleh karena itu, dengan memanfaatkan fungsi hash, kerahasiaan pesan tidak perlu dipedulikan dan proses enkripsi menjadi lebih ringan karena pengirim tidak perlu mengenkripsi sebuah pesan dengan ukuran yang sembarang. Dengan menggunakan fungsi hash terlebih dahulu pada pesan, pengirim hanya perlu mengenkripsi *message digest* yang dihasilkan oleh fungsi hash tersebut. Hasil enkripsi yang didapatkan merupakan *Digital Signature* yang kemudian akan dilekatkan pada pesan semula yang tidak perlu dimodifikasi. Penerima kemudian hanya perlu melakukan fungsi hash ulang pada pesan yang diterima dan mendekripsi *Digital Signature* menggunakan kunci publik pengirim. Jika hasil dekripsi *Digital Signature* sama dengan *message digest* yang didapatkan, penerima dapat menyimpulkan bahwa pesan yang dikirimkan otentik dan tidak mengalami modifikasi apapun.

IV. Analisis dan Pembahasan

A. Proses Autentikasi BCA Mobile

Proses autentikasi pada BCA Mobile melalui beberapa tahapan sebelum pengguna dapat menjalin koneksi dengan API BCA dan menggunakan layanan-layanan yang tersedia. Proses autentikasi pada BCA Mobile bernama Authentication SNAP (Secure Network Access Protocol).

Pertama-tama, seorang pengguna perlu melakukan *user registration* untuk melakukan registrasi ke BCA Mobile menggunakan informasi pribadi dan nomor telepon, serta membuat sebuah *username* dan *password*.

Ketika pertama kali seorang pengguna melakukan *login* ke BCA Mobile, pengguna akan menggunakan *username* dan *password*. Ketika pengguna berhasil *login*, Authentication SNAP akan teraktivasi.

Kemudian pengguna akan diminta untuk membuat sebuah PIN yang akan digunakan sebagai proses autentikasi tambahan pada *login-login* lain.

Ketika pengguna hendak melakukan *login* lagi, pengguna akan diminta untuk memasukan PIN yang sebelumnya sudah ditetapkan, sedangkan Authentication SNAP akan menggunakan *credential* lain untuk melakukan proses autentikasinya sendiri.

Jika proses autentikasi PIN dan Autentication SNAP berhasil, pengguna akan mendapatkan akses kepada akun yang telah didaftarkan.

B. Authentication SNAP

Untuk dapat melakukan koneksi, BCA Mobile perlu melakukan Authentication SNAP, yaitu sebuah proses autentikasi yang berbeda dengan proses autentikasi yang dilakukan oleh pengguna. Authentication SNAP akan menggunakan *client_id* yang unik pada setiap *client*. Jika *client_id* ter-*authorized*, *client* akan mendapatkan *access_token* yang bertindak seperti tiket menjalin koneksi bersama API BCA. Ketika sebuah *client* berhasil melakukan *sign in*, *client* akan mendapatkan *client_id* dan juga *client_secret*. *client_secret* merupakan sebuah informasi yang sensitif dan

harus dijaga. Jika *client_secret* diketahui oleh orang lain, pengguna harus sesegera mungkin melakukan *reset client_secret*.

Sebelum *client* mendapatkan *access_token*, terdapat proses *Signature Asymmetric* yang digunakan untuk memastikan bahwa *request access_token* tidak dilakukan oleh penyerang atau penyadap dan *Signature Symmetric* yang digunakan untuk memastikan bahwa *open api service request* tidak dilakukan oleh penyerang atau penyadap.

Terdapat proses validasi HMAC pada proses *Signature Asymmetric*. Berikut merupakan langkah-langkah proses validasi HMAC.

- Mendapatkan *Timestamp* dari *HTTP Header* (X-TIMESTAMP)
- Mendapatkan *Client Key* dari *HTTP Header* (X-CLIENT-KEY)
- Melakukan *lookup API Secret* yang sesuai dengan *key* yang diterima pada *internal store*.
- Mendapatkan HMAC *client* dari *HTTP Header* dengan format *lowercase hexadecimal* (X-SIGNATURE)
- Menghitung HMAC menggunakan *API Secret* sebagai *secret key*
- Membandingkan HMAC *client* dengan HMAC yang telah dihitung

Jika perbandingan HMAC *invalid*, maka *API Gateway* akan mengembalikan *HTTP 401 error code*. Jika perhitungan HMAC sukses dan hasil yang didapatkan sama dengan HMAC *client*, *signature* dianggap *valid*.

SHA256 dengan RSA digunakan untuk membuat *signature* dengan menggunakan *Private Key* sebagai *key*.

X-SIGNATURE = *SHA256withRSA(PrivateKey, StringToSign)* (6)

StringToSign merupakan sebuah *list request* yang dipisahkan oleh sebuah *colon*.

Sama seperti pada *Signature Asymmetric*, *Signature Symmetric* juga memiliki proses validasi HMAC. Proses validasi HMAC pada *Signature Symmetric* sama dengan proses validasi HMAC pada *Signature* Asymmetric.

Namun, proses generasi X-SIGNATURE pada *Signature Symmetric* berbeda dengan *Signature Asymmetric*. Pada *Signature Symmetric*, digunakan SHA512 HMAC dengan *Client Secret* sebagai *key*.

X-SIGNATURE = *HMAC-SHA512(ClientSecret, StringToSign)* (7)

Kemudian, ketika kedua *signature* dinyatakan *valid*, *client* akan mendapatkan *access_token*. Dengan begitu, *client* dapat menjalin hubungan dengan API BCA dan pengguna dapat menggunakan layanan-layanan yang disediakan.

C. Pembahasan

Proses autentikasi pada BCA Mobile sudah memenuhi standar proses autentikasi yang digunakan di berbagai macam sistem pada saat ini. Proses autentikasi pada BCA Mobile memanfaatkan *signature* dan HMAC yang digunakan untuk memastikan bahwa *request* yang diajukan oleh *client* merupakan *request* yang valid dan bukan merupakan sebuah *request* yang diajukan oleh penyerang. Sementara untuk proses penyusunnya, proses autentikasi pada BCA Mobile juga sudah memanfaatkan fungsi hash SHA256 dan SHA512 yang masih menjadi sebuah standar industri bagi keamanan informasi pada sistem. Begitu pula dengan algoritma RSA yang masih merupakan algoritma enkripsi yang paling *reliable* dan paling banyak dipilih karena tingkat keamanannya yang baik.

Dengan memanfaatkan algoritma RSA dan fungsi hash SHA, keamanan data yang digunakan sebelum, selama, dan sesudah proses autentikasi pada BCA Mobile terjaga kerahasiannya. Dengan memanfaatkan *signature* dan HMAC, seluruh proses autentikasi memenuhi sifat autentikasi yang mencerminkan bahwa seluruh proses memastikan data tepat dan menghilangkan celah keamanan informasi sebanyaknya.

Namun seiring berjalannya waktu, teknik-teknik kriptografi yang digunakan oleh BCA Mobile akan kehilangan relevansinya. Hal ini disebabkan oleh munculnya *Quantum Computer* secara komersil di masa depan. *Quantum Computer* dapat memecahkan teknik-teknik enkripsi dan dekripsi seperti yang digunakan oleh RSA. Oleh karena itu, BCA Mobile tetap harus melakukan pengembangan keamanan informasinya. Salah satu contoh teknik kriptografi baru yang dapat digunakan untuk menghadapi kekuatan *Quantum Computer* adalah *Quantum Key Distribution*. Di masa yang mendatang, tidak menutup kemungkinan dan sangat disarankan bagi BCA Mobile untuk mengimplementasikan *Quantum Cryptography* untuk menjaga keamanan informasinya.

KESIMPULAN

Berdasarkan analisis yang telah dilakukan, dapat dibuktikan bahwa proses autentikasi yang dilakukan oleh BCA Mobile telah memenuhi standar keamanan informasi yang digunakan oleh berbagai macam sistem pada saat ini dengan memanfaatkan RSA, SHA256, SHA512, HMAC, dan *signature*.

Proses autentikasi yang terdiri atas berbagai tahapan dengan kompleksitas yang cukup tinggi dan keamanan yang terus terjaga dapat mengartikan bahwa proses autentikasi BCA Mobile cukup aman atau bahkan aman untuk menanggulangi celah-celah keamanan yang kerap terjadi pada zaman ini.

Namun untuk menanggulangi celah keamanan informasi yang mungkin terjadi di masa mendatang, proses autentikasi BCA Mobile masih belum matang. Oleh karena itu, dapat disimpulkan bahwa layanan BCA Mobile relatif terpercaya dan dapat dimanfaatkan oleh siapa saja tanpa perlu mengkhawatirkan banyaknya celah keamanan informasi yang ada karena BCA Mobile telah berhasil menanggulangi mayoritas celah keamanan informasi yang seringkali menjadi masalah.

PENGHARGAAN

Penulis mengucapkan syukur sebesar-besarnya kepada Tuhan yang Maha Esa karena masih memberikan kesehatan dan kesempatan bagi penulis untuk menyelesaikan laporan penelitian ini.

Penulis juga mengucapkan terima kasih atas dukungan keluarga dan teman-teman di sekitar penulis sehingga proses pembelajaran dan penelitian penulis dapat terlaksana.

Terima kasih juga penulis ucapkan kepada Bapak Dr. Ir. Rinaldi Munir, M. T. selaku dosen pengajar mata kuliah II4031 Kriptografi dan Koding STI yang telah berjasa memberikan berbagai macam ilmu pengetahuan selama satu semester ini.

REFERENCES

Berikut merupakan referensi-referensi yang dimanfaatkan dalam proses penyusunan laporan penelitian ini.

[1] A. Shinta and A. Shinta, "Mengenal Kriptografi, Pengertian, Jenis dan Algoritmanya," *Blog Dewaweb*, Apr. 13, 2022. https://www.dewaweb.com/blog/apa-itu-kriptografi/#Pengertian_Kriptografi (accessed May 22, 2023).

[2] "01 -Pengantar Kriptografi Prodi Sistem dan Teknologi Informasi Sekolah Teknik Elektro dan Informatika 2021 Oleh: Rinaldi Munir II4031 Kriptografi dan Koding." Accessed: May 22, 2023. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/1%20-%20Pengantar-Kriptografi-STI-(2021).pdf

[3] "Sejarah Singkat PT Bank Central Asia, Tbk," 123dok.com, 2017. https://text-id.123dok.com/document/wyevr1g1z-sejarah-singkat-pt-bank-central-asia-tbk.html (accessed May 22, 2023).

[4] "tentang-bca," Bca.co.id, 2018. https://www.bca.co.id/id/tentang-bca (accessed May 22, 2023).

[5] "BCA - Syarat dan Ketentuan BCA mobile," www.bca.co.id, 2023. https://www.bca.co.id/id/Syarat-dan-Ketentuan/BCA-mobile#:~:text=m%2DBCA%20(Mobile%20Banking),media%20SMS%20atau%20menggunakan%20menu (accessed May 22, 2023).

[6] Desy, "Ini Perbedaan antara BCA Mobile dan myBCA untuk Transaksi," fortuneidn.com, Mar. 13, 2023. https://www.fortuneidn.com/finance/desy/ini-perbedaan-antara-bca-mobile-dan-mybca-untuk-memudahkan-transaksi?page=all (accessed May 22, 2023).

[7] Aorinka Anendya and Aorinka Anendya, "Apa itu Autentikasi, Cara Kerja dan Fungsinya bagi Keamanan Data," Blog Dewaweb, Oct. 13, 2022. https://www.dewaweb.com/blog/pengertian-autentikasi/#Apa_Itu_Proses_Autentikasi (accessed May 22, 2023).

[8] "Algoritma RSA II4031 Kriptografi dan Koding Oleh: Rinaldi Munir Program Studi Sistem dan Teknologi Informasi Sekolah Teknik Elektro dan Informatika ITB." Accessed: May 22, 2023. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/12%20-%20Algoritma-RSA-2021.pdf

[9] "II4031 Kriptografi dan Koding Oleh: Rinaldi Munir Program Studi Sistem dan Teknologi Informasi Sekolah Teknik Elektro dan Informatika ITB." Accessed: May 22, 2023. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/17%20-%20Fungsi-hash-2021.pdf

[10] R. Munir, "MAC (Message Authentication Code) II4031 Kriptografi dan Koding 1 Rinaldi Munir/II4031 Kriptografi dan Koding/Prodi STI/STEI-ITB." Accessed: May 22, 2023. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/22%20-%20MAC-2021.pdf

[11] "Tanda-tangan Digital II4031 Kriptografi dan Koding Oleh: Rinaldi Munir Program Studi Sistem dan Teknologi Informasi Sekolah Teknik Elektro dan Informatika ITB." Accessed: May 22, 2023. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/21%20-%20Tanda-tangan-digital-2021.pdf [1]

[12] "Dokumentasi," Bca.co.id, 2023. https://developer.bca.co.id/id/Dokumentasi (accessed May 22, 2023).

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, 22 Mei 2023

Brandon Jonathan Latif
18220103