ANALISIS PENGGUNAAN ENKRIPSI *END TO END* PADA APLIKASI *WHATSAPP MESSENGGER*

Gellysa Urva
Program Studi Informatika, Sekolah Tinggi Teknologi Dumai
Jl. Utama Karya Bukit Batrem II Dumai
e-mail: gellysa.urva@gmail.com

Abstrak

Perkembangan teknologi dan komunikasi yang begitu pesat pada era dunia saat ini tidak dapat dipungkiri. Teknologi merupakan alat bantu yang saat ini menjadi salah satu kebutuhan yang harus dipenuhi sebagai pelengkap di kehidupan manusia. Perkembangan *smartphone* berbasis android telah mewarnai dunia dengan pesatnya. Mulai kalangan anak-anak hingga dewasa menuntut kegunaan *smartphone* sebagai teknologi tepat guna untuk digunakan sebagai komunikasi maupun kegunaan-kegunaan lainnya. Salah satu aplikasi android yang paling banyak digunakan adalah *WhatsApp Messenger* yang masih menjadi primadona sebagai aplikasi pesan instan yang digemari oleh banyak orang di dunia. Ada beberapa alasan pemilihan *WhatsApp Messenger* sebagai aplikasi pesan yang digemari yaitu seperti aplikasi yang ringkas, mudah terhubung dalam jaringan, dan tidak perlu memiliki ID pengguna menjadi salah satu keunggulan tersendiri bagi *WhatsApp Messenger*.

WhatsApp Messenger sebagai aplikasi pesan yang banyak digemari oleh banyak orang juga membutuhkan peningkatan keamanan guna menghindari kejahatan-kejahatan dunia *cyber* yang tidak dikehendaki. Mengingat penggunaan aplikasi tersebut berbanding lurus dengan peningkatan tingkat kejahatan yang menggunakan aplikasi pengolah pesan itu. Tidak jarang, aplikasi pengolah pesan digunakan untuk bertukar informasi yang ilegal ataupun tindakan pemerasan. Hal ini membutuhkan penanganan khusus. Dengan penerapan teknik enkripsi *end-to-end* pada *WhatsApp Messenger* maka hanya pengirim dan penerima sajalah yang hanya dapat membuka dan membaca pesan asli yang dikirimkan walaupun pesan terlebih dahulu singgah pada server penyedia layanan. Menariknya, *WhatsApp Messenger* memilih tipe enkripsi *'end-to-end'*. Enkripsi *end to end* ini akan melindungi setiap pesan yang dikirim maupun yang diterima.

Kata kunci : *WhatsApp Messenger*, Enkripsi end to end, Keamanan.

Abstract

The rapid development of technology and communications in the current world era can not be denied. Technology is a currently tool becomes one of the needs that must be met as a complement in human life. The development of android-based smartphone has colored the world by leaps and bounds. Starting from children to adults demanding smartphone usability as the right technology to be used as communication and other uses. One of the most widely use android app is WhatsApp Messenger which is still a primadonna as an instant messaging app favorite by many people in the world. There are several reasons why the WhatsApp Messenger as a

popular messaging app. There are a compact application, easy to connect in the network, and it does not need to have a user ID to be one of its own advantages for WhatsApp Messenger.

WhatsApp Messenger as a messaging app that is popular with many people also requires increased security in order to avoid unwanted cyber world crimes. The relation of application using and the crime rates is directly proportional to. Not infrequently, messaging applications are used to exchange illegal information or extortion measures. This requires special handling. With the application of end-to-end encryption techniques in WhatsApp Messenger, only senders and recipients can open and read the original message that is sent even if the message first drops on the service provider's server. Interestingly, WhatsApp Messenger chooses the 'end-to-end' encryption type. End to end encryption protects every sent or received message.

Keywords : *WhatsApp Messenger*, 'end-to-end' encryption, *communication security*.

Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi secara jauh. Antar kota antar wilayah bahkan negara bukan lagi merupakan suatu kendala dalam melakukan komunikasi dan pertukaran data. Media komunikasi yang digunakan dapat berupa pesan, berkas, gambar, suara atau video. Media komunikasi tersebut menjadi salah satu media yang sering digunakan karena mempermudah dan mempercepat kegiatan komunikasi. Pertukaran informasi yang dilakukan dengan mengirimkan data tanpa melakukan pengamanan terhadap konten yang dikirim mungkin saja tidak aman, karena ketika dilakukan penyadapan maka data dapat langsung dibaca oleh penyadap. Sehingga, informasi yang bersifat penting bahkan rahasia dapat jatuh ke pihak yang tidak berhak.

Seiring dengan itu tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan semakin meningkat. Begitu banyak pengguna seperti Perusahaan, Sekolah, Kampus maupun Individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Teknik ini dapat mengubah pesan yang dianggap rahasia menjadi pesan acak sehingga tidak sesuai dengan pesan yang asli. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan informasi asli atau dikenal dengan sebutan (*plaintext*) ke dalam bentuk informasi yang di acak/di enkripsi (*ciphertext*) yang tidak dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima(*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditransformasikan kembali dalam bentuk *plaintext* agar dapat dikenali. Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses transformasi dari *plaintext* ke *ciphertext* dikenal dengan proses deskripsi. Kedua proses tersebut dilakukan dengan menggunakan algoritma tertentu yang dikenal dengan kunci. Ada empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. 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.
3. 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.
4. Non Repudiasi, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

WhatsApp Messenger adalah aplikasi pesan seluler lintas *platform* yang memungkinkan Anda untuk bertukar pesan tanpa harus membayar SMS. Aplikasi *WhatsApp Messenger* merupakan aplikasi yang diciptakan *WhatsApp Inc* yang didirikan oleh Brian Acton dan Jan Koum pada tahun 2009. Kedua orang tersebut sebenarnya juga merupakan pekerja senior yang pernah bekerja di Yahoo. Ide awal *WhatsApp Messenger* bermula dari Jan Koum yang mempunyai ide untuk membuat suatu aplikasi yang dapat mem*broadcast* status walaupun orang tersebut dalam kondisi yang sulit untuk dihubungi. Ketika itu, Jan Koum melakukan kerja sama dengan Anton. Pada awalnya aplikasi ini hanya menarik sebagian kecil orang, namun setelah menambahkan fitur *messaging* aplikasi ini menjadi semakin populer.

Gambar 1. Logo *WhatsApp Messenger*

Saat ini *WhatsApp Messenger* telah tersedia untuk *iPhone*, *BlackBerry*, *Windows Phone*, *Android*, Nokia serta bisa digunakan di PC maupun *Notebook*. Model penggunaan *WhatsApp Messenger* yang dapat digunakan secara *Free* dalam aktivitasnya. Pengguna *WhatsApp Messenger* dapat membuat grup, saling berkirim gambar, pesan video, dan audio dalam jumlah tidak terbatas. Penggunaanya tidak berbayar hanya berdasarkan paket data internet di *android*. *WhatsApp Messenger* telah meningkatkan sistem keamanan aplikasi ke level yang tertinggi. Teknologi yang digunakan WhatsApp ini berbasis *open source* yang dikembangkan oleh perusahaan bernama *Open Whisper Systems*. Perusahaan ini sudah mengembangkan sistem anti peretasan pesan dan telepon lain seperti *TextSecure*, *RedPhone*, serta *Signal and Flock*. *Whisper Systems* merupakan perusahaan yang telah diakuisisi oleh *Twitter* pada tahun 2011. Kemudian proyek *open source* perusahaan tersebut

dirancang untuk membuat standar enkripsi yang dapat digunakan untuk membuat pesan lebih rahasia dan aman. Moxie Marlinspike, pendiri Open *Whisper Systems* menyatakan Enkripsi diaktifkan secara *default* di *WhatsApp Messenger*, sehingga pengguna tidak perlu melakukan apapun untuk membuatnya bekerja, dan *WhatsApp Messenger* tidak akan dapat membaca pesan dari pengguna. Selain dari pihak *WhatsApp Messenger*, pesan yang akan dikirim kepada antar pengguna juga tidak dapat dibaca oleh server karena tidak memiliki *decryption key*. Sistem enkripsi ini akan menutup peluang pihak-pihak yang tidak bertanggungjawab tidak dapat melacak pesan kamu secara pribadi. Untuk membobol pesan ini, kita harus membuka kunci satu per satu. Dengan mode enkripsi seperti ini tentunya diyakini akan mengurangi kasus pencurian informasi dari pihak yang tidak bertanggung jawab di seluruh dunia. *WhatsApp Messenger End-to-end Encryption* adalah fitur keamanan terbaru *WhatsApp Messenger* dengan metode/cara mengenkripsi konten chat baik teks maupun file gambar gif/JPEG, dokumen pdf/.doc, suara/musik, video, dan lainnya sehingga hanya dapat dibaca oleh pengirim dan penerima pesan dan tidak bisa di akses (tidak terbaca jika disadap) oleh pihak lain termasuk aplikasi pihak ketiga, penjahat (*Hacker*), rezim opresif ataupun penegak hukum (pemerintah), dan bahkan oleh pihak *WhatsApp Messenger*.

Pengiriman pesan tersebut membutuhkan pengamanan yang berupa penyandian pesan sehingga pesan yang dikirimkan merupakan pesan yang telah disandikan. Penerapan menjamin privasi pengguna yang menggunakan aplikasi tersebut. Penulis akan membahas tentang penggunaan pengamanan pesan yang diterapkan oleh *WhatsApp Messenger* dengan menggunakan teknik enkripsi *end-to-end*.

Metode Penelitian

Teknik pengumpulan data yang digunakan dalam penelitian ini menggunakan studi literatur. Dimana Penulis melakukan studi literatur pada buku-buku yang membahas terkait topik penelitian, junal-jurnal ilmiah maupun penelitian-penelitian yang telah dilakukan terlebih dahulu. Selanjutnya menjadi bahan untuk penulis mengembangkan isi maupun alur dari penelitian ini. Adapun yang menjadi acuan bagi penulis sebagai bahan referensi merupakan sumber-sumber yang dapat dipercaya dan sudah dapat diakui tulisan maupun hasil penelitiannya.

Hasil dan Pembahasan

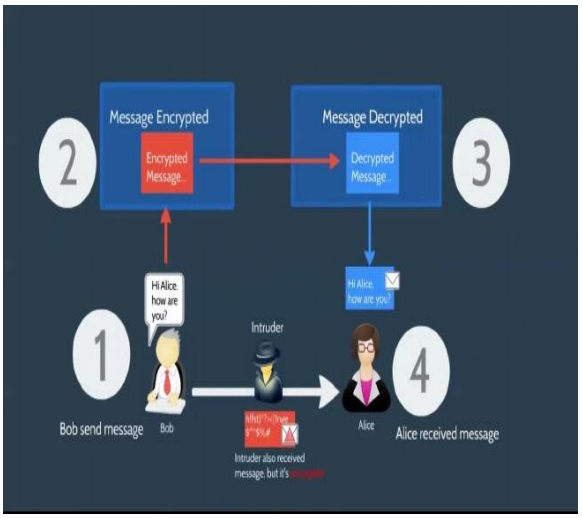
1. Skema Pengamanan Pesan dengan Teknik Enkripsi *End-to-end* pada *WhatsApp Messenger*

WhatsApp Messenger mulai tanggal 6 April 2016 resmi merilis mode keamanan dengan menggunakan teknik enkripsi *End-to-end*. Mode ini membuat setiap pesan yang dikirim terenkripsi secara aman dan hanya bisa dibuka oleh pengirim dan penerima pesan tersebut. Dengan menggunakan teknik ini seluruh pesan yang dikirimkan dan diterima oleh pengguna WhatsApp kini tidak bisa disadap oleh pihak ketiga. Pesan tersebut hanya bisa dibaca oleh penerima yang dituju, termasuk layanan telepon, gambar, video, dan pesan suara.

Teknik enkripsi *End-to-end* merupakan sebuah sistem dimana proses enkripsi terjadi pada saat pesan dikirimkan hanya terdeskripsi pada saat pesan sampai kepada penerima. Bahkan pihak *WhatsApp Messenger* sendiri akan kesulitan untuk menyerahkan rekaman data penggunanya ke pihak yang berwajib, karena sistem enkripsi *end-to-end* dirancang agar tidak bisa dibobol (kriptanalisis) oleh pembuatnya sekalipun.

Dengan sistem enkripsi *end-to-end* ini pengguna *WhatsApp Messenger* tentunya tidak perlu menghawatirkan privasi mereka. Pihak pemerintah ataupun kepolisian juga akan sulit untuk memata-matain percakapan yang dilakukan oleh pengguna karena semua pesan dan data yang dikirimkan merupakan kumpulan kode yang telah terenkripsi dan tidak dapat dimengerti. Kode tersebut hanya dapat dibaca pada perangkat penerima pesannya, sehingga pihak ketiga secara otomatis tidak dapat bisa menyadap percakapan di *WhatsApp Messenger*..

Sebagai ilustrasi pengirim pesan di *WhatsApp Messenger* mengirimkan pesan "Apa Kabar?", pada saat pesan dikirimkan maka pesan tersebut akan dienkripsi secara otomatis menjadi "9XB80FFAH" kemudian akan dideskripsikan kembali menjadi pesan semula "Apa Kabar?". Dengan menggunakan teknik enkripsi *end-to-end* maka segi privasi pengguna aplikasi *WhatsApp Messenger* lebih terjamin.



Gambar 2. Ilustrasi Pengiriman Pesan di *WhatsApp Messenger*

Dengan menggunakan fitur enkripsi *end-to-end* di *WhatsApp Messenger* akan menyulitkan penyidik untuk melakukan penyadapan. Sehingga teknik enkripsi *end-to-end* ini penting untuk melindungi privasi seseorang. Namun disaat yang sama, fitur keamanan tingkat tinggi ini juga dapat dimanfaatkan oleh pelaku kejahatan, termasuk teroris, koruptor dan lain-lain. Salah satu praktisi keamanan internet Indonesia mengatakan fitur enkripsi *end-to-end* di *WhatsApp Messenger* sangat menguntungkan bagi penjahat dalam melakukan setiap perencanaan maupun perwujudan dari perencanaan mereka. Enkripsi *end-to-end* selalu aktif, hanya jika semua orang yang terlibat menggunakan versi terbaru *WhatsApp Messenger* . Tidak ada cara untuk menonaktifkan enkripsi *end-to-end*. Berikut ini

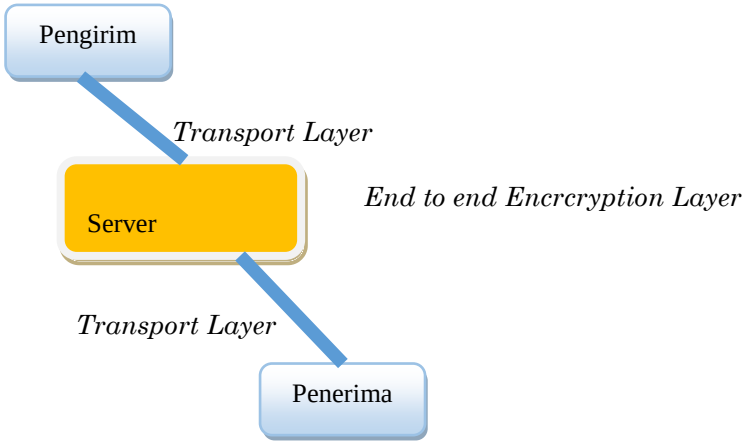
tampilan pemberitahuan penggunaan teknik enkripsi *end-to-end* pada *WhatsApp Messenger* versi terbaru di android.

2. Cara Kerja Enkripsi *End To end* pada *WhatsApp Messenger*

Enkripsi *end-to-end WhatsApp Messenger* memastikan bahwa hanya pengguna dan lawan yang berkomunikasi dengan pengguna sajalah yang dapat membaca apa yang telah dikirimkan, dan tidak ada orang lain, bahkan *WhatsApp Messenger*. Pesan-pesan pengguna diamankan dengan sebuah kunci, dan hanya penerima dan pengguna saja yang memiliki kunci spesial yang diperlukan untuk membuka dan membaca pesan.

Melalui mekanisme *end to end encryption*, aplikasi akan mengenkripsi pesan yang akan dikirim. Pesan yang akan dikirim akan dienkripsi sebelum dikirim ke BTS (*Base Transceiver Station)* sebagai sebuah infrastruktur telekomunikasi yang memfasilitasi komunikasi nirkabel antara piranti komunikasi dan jaringan operator. Untuk keamanan tambahan, setiap pesan yang pengguna kirimkan memiliki kunci yang unik misalnya pesan yang dilindungi dengan *message key* menggunakan AE5256 dalam moda SHA256 untuk otentikasi. Setiap pesan berubah untuk setiap pesan yang dikirimkan dan *messege key* yang dipakai untuk mengenskripsikan sebuah pesan yang tidak bisa di kontruksikan.

Pada sistem kemanan *end-to-end encription* ini semua fitur yang terjadi secara otomatis tidak perlu mengaktifkan pengaturan tertentu atau mengatur sebuah *chat* tertentu yang rahasia untuk mengamankan pesan-pesan yang pengguna kirimkan. Pada setiap *chat* memiliki sebuah kode keamanan yang digunakan untuk memverifikasikan bahwa panggilan dan pesan-pesan yang pengguna kirimkan ke *chat* tersebut terenkripsi secara *end-to-end*. Pada dasarnya fitur ini membungkus data pengguna pada saat dikirim dan dibuka pada saat diterima. Untuk lebih memahami konsep dasar tersebut dapat dilihat pada gambar 6 berikut ini.



Gambar 3. Konsep Dasar Enkripsi *End to end*

Pada gambar 3 ditunjukkan bahwa fitur enkripsi *end-to-end* seolah-olah memiliki jalur sendiri untuk berkomunikasi. Namun jalur tersebut hanyalah perumpaan saja dikarenakan jalur tersebut sebagai pembungkus data pada komunikasi antar pengguna. Pada fitur *end-to-end* enkripsi *WhatsApp Messenger* mengadopsi protokol yang dimiliki oleh aplikasi signal yang di desain berbasis *Open Whisper System*. Sistem ini di desain untuk menghindari serangan dari pihak ketiga dalam mencuri informasi baik berupa data pesan maupun panggilan. Bahkan jika

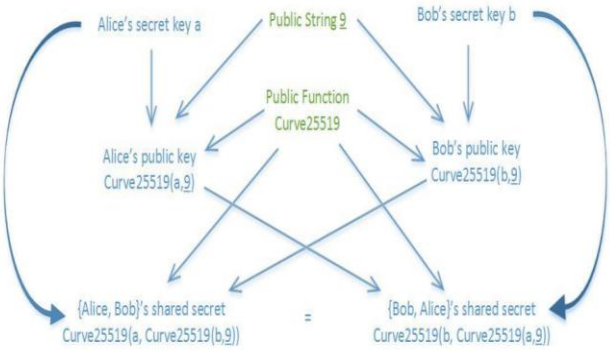
kunci enkripsi suatu pengguna dicuri oleh penyerang, mereka tetap tidak akan bisa mendekripsi pesan yang telah dikirim.

3. Metode Enkripsi *End To end*

a. Tipe Publik *Key*
   1) *Identity Key Pair* adalah pasangan kunci *long-term Curve*25519
   2) *Signed Pre Key* adalah pasangan kunci medium-term *Curve*25519, dibangkitkan pada saat proses instalasi aplikasi, dan akan berubah-ubah dalam waktu tertentu.
   3) *One-Time Pre Keys* adalah barisan pasang kunci Curve25519 yang digunakan hanya satu kali, dibangkitkan pada saat proses instalasi, dan akan muncul pada saat dibutuhkan.

Pada beberapa tipe kunci publik yang digunakan oleh *end-to-end encryption* pada *WhatsApp Messenger* , pasangan kunci yang digunakan berjenis *Curve*25519. *Curve*25519 adalah sebuah *elliptical curve* (ecc) dengan panjang 128 bit yang menggunakan konsep ECDH (*eliptic curve* Diffie-Hellman). Beberapa yang menjadi pertimbangan dipakainya *Curve*25519 adalah dari sisi keamanan yang cukup baik dan beberapa kelebihan dibandingkan dengan algoritma pertukaran kunci lainnya. Pada karya ilmiah Daniel J Bernstein yang berjudul "*Curve*25519: *new Diffie-Hellman speed records*" diakui bahwa *Curve*25519 memiliki kecepatan komputasi yang baik yang dapat diterapkan pada algoritma kriptografi. Hal ini mungkin yang mendasari *WhatsApp Messenger* untuk memakai *curve*25519 pada fitur *end-to-end encryption*. Sebagaimana kita ketahui tiap pengembang aplikasi *mobile* membuat aplikasi harus lebih efisien terutama dari pemakaian memori yang dapat mempengaruhi jalannya aplikasi secara efisien.

Pada konsep dasar *Curve*25519 tiap pengguna memiliki 32 *Byte secret key* dan 32 *Byte public key*. Selain itu, tiap pasangan pengguna memiliki 32 *Byte shared key* yang digunakan untuk mengotentikasi dan mengenkripsi pesan antar 2 pengguna. Untuk memperjelas hal tersebut berikut adalah diagram alur pembangkitan *shared key* :



Gambar 4. Proses Pembangkitan *Shared Secret Key*

Pada gambar 4 adalah proses pembangkitan *shared secret key* yang nantinya akan dijadikan kunci untuk mengenkripsi pesan. Langkah-langkah pembangkitan adalah sebagai Berikut :

1. Kedua *user* yaitu Alice dan Bob harus sama-sama menentukan public string dimana pada gambar *public String* bernilai 9.
2. Lalu masing-masing Alice dan Bob menentukan *secret key*. Pada gambar *secret key* a untuk Alice dan *secret key* b untuk Bob. *Secret key* ini bersifat rahasia.

3. Kemudian Alice dan Bob membangkitkan kunci *public* dengan cara memasukan nilai dari *secret key* (a dan b) dan nilai public string (9) ke dalam fungsi *Curve*25519 yaitu *Curve*25519(a, 9) untuk Alice dan *Curve*25519 (b, 9) untuk Bob.
4. Lalu Alice dan Bob saling bertukar kunci publik yang telah dimasukan ke fungsi *Curve*25519.
5. Terakhir Keduanya dapat menghitung i dengan cara memasukan *public key* yang didapat dan nilai *secret key* masing-masing kedalam *Curve*25519. Sebagai contoh *Curve*25519(a, *Curve*25519(b,9)) untuk *shared key* Alice dan Bob.

Ada beberapa kelebihan dari konsep *Curve*25519 :

1. *Extremely High Speed*
   Dalam sebuah karya ilmiah telah dibuktikan dalam beberapa *Personal Computer* (PC) bahwa *Curve*25519 memiliki kecepatan yang mampu untuk sebuah proses.
2. *No Time Variability*
   *Curve*25519 telah diriset tahan terhadap *timing attack, hyperthreading attack*, dan *cache timing attack.*
3. *Short Secret Key*
   Pada *Curve*25519 hanya memiliki 32 *Byte secret key.*
4. *Short Public Key*
   Pada *Curve*25519 memiliki 32 *Byte public key.*

b. Tipe Kunci Sesi
   1) Root Key adalah sebuah nilai dengan panjang 32 Byte yang digunakan untuk membangkitkan Chain Keys.
   2) Chain Key adalah sebuah nilai dengan panjang 32 Byte yang digunakan untuk membangkitkan Message Keys.
   3) Message Key adalah sebuah nilai dengan panjang 80 Byte yang digunakan untuk mengenkripsi isi pesan. Dari 80 Byte, 32 Byte digunakan sebagai kunci AES-256.

c. Registrasi Pengguna (*Client Registration*)

Pada waktu awal registrasi, penguna mengirimkan P*ublic Identity Key, Signed Pre Key* (beserta s*ignature* nya), dan sejumlah *public One-Time Pre Key* ke server aplikasi. Server *WhatsApp Messenger* menyimpan *public key* ini beserta identitas pengguna tersebut.

d. Inisialisasi Pembentukan Sesi

Dalam berkomunikasi dengan pengguna lain, pertama-tama user harus menyiapkan sebuah sesi untuk berkomunikasi yang aman (terenkripsi). Sesi dibentuk hanya satu kali. Jika suatu saat komunikasi ingin dilakukan kembali dengan pengguna yang sama maka tidak perlu membuat sesi yang baru sampai suatu saat sesi yang telah dibentuk hilang dikarenakan *install* ulang aplikasi atau perpindahan pengguna ke perangkat lain. Berikut adalah proses pembentukan sesi :

1. Inisiator adalah user yang pertama kali meminta komunikasi dengan pengguna lain. Inisiator meminta *public Identity Key, public Signed Key, dan single public One-Time Pre Key* milik pengguna lain (*recipient*).
2. Server mengembalikan permintaan dengan suatu nilai *public key*. Satu *One-Time Pre Key* yang hanya bisa digunakan satu kali, jadi setelah dikirim dan diterima inisiator maka *One-Time Pre Key* tadi akan otomatis dihapus dari *storage server.*
3. Inisiator menyimpan *Identity Key* milik penerima (*recipient*) sebagai *Irecipient* , *Signed Pre Key* sebagai *Srecipient* , dan *One-Time Pre Key* sebagai *Orecipient* .

4. Lalu inisiator membangkitkan pasangan kunci *ephemeral Curve*25519 sebagai *Einitiator*.
5. *Inisiator* mengisi *Identity Key* dengan I .
6. Kemudian, *inisiator* menghitung *master secret* yaitu *master_secret* = ECDH (*Iinitiator ,Srecipient*) | | ECDH (*Einitiator , Irecipient*) | | ECDH (*Einitiator , Srecipient*) | | ECDH (*Einitiator , Orecipient*).
7. *Inisiator* menggunakan HKDF untuk membangkitkan *Root Key* dan *Chain keys* dari *master_secret*.

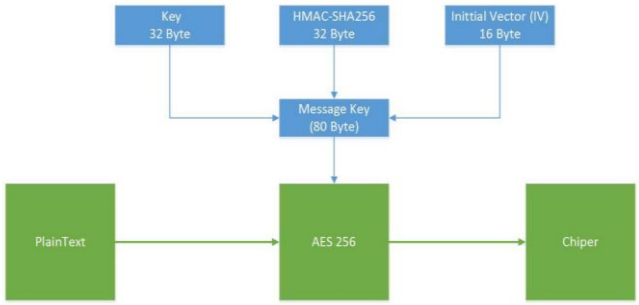
e. Pengaturan Sesi Penerimaan (*Receiving Session Setup*)

Setelah dilakukannya pembentukan sesi enkripsi, *inisiator* dapat langsung memulai pengiriman pesan ke penerima, bahkan jika penerima dalam keadaan *offline*. Sampai respon diberikan oleh penerima, *inisiator* termasuk informasi yang dikirim yang dibutukan oleh penerima, membentuk *corresponding session*. Dalam hal ini termasuk *Einitiator* dan *Iinitiator* . Ketika penerima menerima pesan, penerima akan menghitung *master_secret* dengan menggunakan *private key* dan *public key* yang terpasang pada *header* paket informasi yang didapat. Kemudian penerima menghapus *One-Time Pre Key* yang digunakan oleh *inisiator*. Selanjutbya *inisiator* menggunakan HKDF untuk mendapatkan *Root Key* dan *Chain Keys* dari *master_secret*.

f. Pertukaran Pesan (*Exchanging Messages*)

Dalam berkomunikasi, pertama kali yang dilakukan adalah menyiapkan sesi. Setelah sesi telah terbentuk dengan baik, pertukaran pesan dapat dilakukan. Pada *WhatsApp Messenger* pertukaran pesan antar klien dilindungi dengan *Message Key* dengan menggunakan enkripsi AES256 pada mode CBC (*Chiper Block Chining*) serta menggunakan HMAC-SHA256 sebagai integritas data.

Message Key akan selalu berbeda pada tiap paket yang kirim karena bersifat ephemeral (penggunaan secara singkat). Seperti halnya *Message Key* yang telah mengenkripsi pesan tidak dapat mengenkripsi ulang. *Message Key* diadapatkan dari *Chain key* pengirim/inisiator dimana akan bangkit secara berkesinambungan dan akan kembali ke suatu titik tertentu "*ratchets method*". Berikut adalah blok diagram proses enkripsi pesan, ditunjukkan pada gambar 8 :



Gambar 5. Enkripsi *end to end* pada *WhatsApp Messenger*

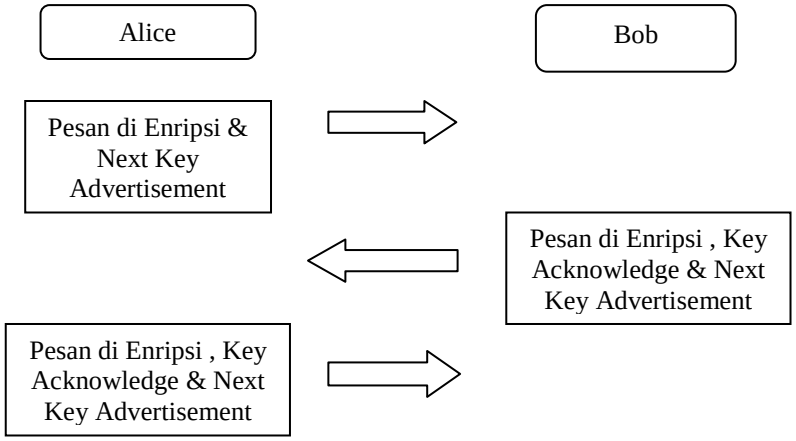
Pada gambar 5 ditunjukkan bahwa algoritma enkripsi yang digunakan berupa AES-256. Untuk kunci (*Message Key*) dari AES-256 sepanjang 80 *Byte* yang terdiri dari 32 *Byte* kunci, 32 *Byte* HMAC-SHA256, dan 16 *Byte initial vector* (iv). Pada prosesnya pembangkitan *Message key* diperoleh dari Chain key (32Byte). *Message Key* dibutuhkan setiap waktu oleh pengirim / inisiator untuk mengenkripsi data. Gambar berikut adalah

blok diagram pembentukan *Message* .

Gambar 6. Proses Pembangkitan *Message Key*

Berikut cara dalam mendapatkan nilai *Message Key* :
1. *Message Key* = HMAC-SHA256 (*Chain Key*, 0x01)
2. *Chain key* kemudian di*update* dengan proses penghitungan *Chain Key* = HMAC-SHA256 (*Chain Key*, 0x02).

Pada enkripsi pesan yang dilakukan pada saat komunikasi, kunci (*Message key*) yang didapatkan dari *Chain Key*. *Chain Key* yang dibangkitkan berjumlah 32 *Byte* yang bersifat "*rachets*". Metode *rachets* dibuat oleh open *whisper system* yang digunakan untuk mengatasi masalah pertukaran kunci publik enkripsi yang sama pada waktu tertentu. Metode ini memastikan kunci publik yang dikirimkan berbeda-beda pada tiap pengiriman paket. Fitur ini adalah *protocol* keamanan modern yang digunakan untuk mencegah penyerang yang biasa melakukan *sniffing*/ mengendus jaringan, yang nantinya akan mencoba melakukan dekripsi karena hanya menggunakan satu kunci saja. Selain itu dengan metode pertukaran kunci singkat (*ephemeral key exchange*) akan menyulitkan bagi penyerang untuk mendapatkan kunci selanjutnya dikarenakan kunci hanya disimpan di memori hanya sementara dan dalam waktu singkat. Gambar berikut dapat mengilustrasikan konsep metode "*ephemeral key exchange*".



Gambar 7. Proses *Ephemeral Key Exchange* pada *Ratchet*

Pada gambar 7 adalah proses "*ephemeral key exhange*" yang dilakukan pada saat sesi telah dibangun. Tiga langkah pada gambar dijelaskan sebagai berikut :

4. Alice mengirimkan pesan terenkripsi kepada Bob. Bersamaan dengan isi dari pesan yang sebenarnya, Alice juga mengirikan kunci "*advertises*" yang digunakan sebagai kunci pada pengiriman pesan selanjutnya.

5. Bob mengirimkan pesan terenkripsi kepada Alice. Pada saat bersamaan, Bob juga mengirimkan "*acknowledges*" kunci yang diberikan oleh alice, dan mengirimkan kunci Bob untuk dipakai pada komunikasi selanjutnya.
6. Alice akan menggunakan kunci *advertised* dan *acknowledged* pada pengiriman pesan selanjutnya.

g. Konsep Grup (*Grouping Message*)

Pada dasarnya beberapa aplikasi *chating* memiliki fitur "*grouping*" dimana fitur ini dapat membuat suatu ruangan yang bisa di isi oleh beberapa orang yang kita inginkan. Pada prosesnya teknis pengiriman data pada fitur ini terbagi menjadi 2, yaitu *server-side fan out* dan *client-side fan out*. Untuk perbedaannya terdapat pada proses pengirimannya. Misalnya untuk *server-side fan-out*, pengirim akan mengirimkan suatu pesan ke dalam suatu grup. Didalam sistem, pesan tersebut tidak langsung dikirimkan ke grup/seluruh anggota yang ada di dalam grup, melainkan pesan akan dikirim terlebih dahulu ke server. Lalu server yang akan meneruskan pesan terenkripsi ke dalam grup / seluruh anggota (N *times*). Lain halnya dengan *client-side fan out*. Metode ini mengharuskan pesan yang dikirim akan langsung dikirimkan ke seluruh anggota yang ada didalam grup (N *times*) itu sendiri. Hal ini menyebabkan beban yang berat yang harus ditanggung oleh pengirim dan akan menyebabkan proses menjadi lambat dikarenakan keterbatasan spesifikasi perangkat *mobile* itu sendiri.

Proses *grouping* pada *WhatsApp Messenger* menggunakan suatu pasangan sesi terenkripsi untuk mendukung efisiensi *server-side fan-out*. Hal ini menggunakan "*Sender key* ", yaitu komponen yang berasal dari *Signal Messaging Protocol*. Berikut ini adalah proses inisialisasi dimana suatu anggota grup akan mengirim suatu pesan ke grup itu sendiri :

1. Pengirim Membangkitkan nilai acak / random sepanjang 32 *Byte Chain Key*.
2. Pengirim membangkitkan bilangan acak pasangan *Curve*25519 *Signature Key*.
3. Pengirim mengkombinasikan 32 *Byte Chain Key* dan *public key* dari *Signature key* kedalam pesan *Sender Key* .
4. Pengirim akan mengenkripsi *Sender Key* secara pribadi untuk dikirimkan ke setiap anggota grup.

Setelah proses inisialisasi selesai maka proses pengiriman pesan oleh suatu pengguna ke dalam suatu grup adalah sebagai berikut :

1. Pengirim akan memperoleh *Message Key* yang berasal dari *Chain Key*, serta *update* dari *Chain Key* sebelumnya.
2. Pengirim mengenkripsi pesan menggunakan AES256 pada mode CBC.
3. Pengirim menandai chipertext menggunakan *Signature Key*.
4. Pengirim mengirim pesan terenkripsi ke server, dan server meneruskan ke seluruh anggota grup.

h. *Call Setup*

Pada fitur *end-to-end encryption WhatsApp Messenger* juga terdapat pada mode panggilan. Ketika kedua pengguna *WhatsApp Messenger* sedang melakukan komunikasi jalur yang dipakai ternyata sudah terenkripsi dengan metode SRTP (*Secure Real-Time Transport Protocol*). SRTP khusus didesain untuk pengiriman suara atau video secara real-time. Fitur yang dimiliki oleh protkol ini antara lain menjaga kerahasiaan data (*confidentiality*), Autentikassi pesan, serta perlindungan umpan balik dati trafik RTP. Berikut ini adalah proses panggilan yang dilakukan pengguna pada *WhatsApp Messenger* :

1. Inisiator membentuk sebuah sesi yang terenkripsin dengan penerima (*recipient*), jika sesi belum terbentuk sebelumnya.
2. Inisiator membangkitkan nilai acak (*random*) 32 *Byte* SRTP *master secret*.

3. Inisiator mengirim pesan terenkripsi kepada penerima berupa tanda panggilan masuk, dan berisi SRTP *master secret*. Jika penerima merespon / menjawab panggilan, SRTP secara otomatis mengenkripsi panggilan.

Kesimpulan

Pengiriman data maupun informasi yang dilakukan pada komunikasi via *WhatsApp Messenger* di android bersifat rahasia karena telah melalui proses enkripsi. Fitur enkripsi *end-to-end WhatsApp Messenger* berguna dalam pencegahan pihak ketiga (*attacker*) dalam mencuri data maupun informasi. Karena data dan informasi bersifat rahasia (*confidential*). Begitu juga dalam mencegah perubahan data maupun informasi, karena fitur ini juga menjaga keaslian (integritas).

Enkripsi *end-to-end* ini juga memakai metode-metode yang telah teruji dari berbagai sisi. Seperti halnya algoritma yang dipakai untuk enkripsi pesan dan algoritma pertukaran kunci yang dipakai. Hal ini dikarenakan aplikasi *WhatsApp Messenger* berbentuk aplikasi *mobile* dimana memerlukan komputasi yang efisien sehingga proses pengiriman bisa cepat.

Daftar Pustaka

Advanced Cryptographic Ratcheting. (2016). Retrieved from Open Whisper Systems website https://whispersystems.org/blog/advanced-ratcheting/

C. Anglano, ,(2014) "Forensic Analysis of WhatsApp Messenger on Android," Elsevier.

Mazen Tawfik Mohammed, Alaa Eldin Rohiem and Ali El-moghazy, (2014) “Confidentiality Enhancement of Secure Real Time Transport Protocol”, Computer Engineering Conference (ICENCO), 2012 8th International, pp 43-48

Mehdi Asnaashari, (2008) “Method and system for encryption of information stored in an external nonvolatile memory”, United States, WO2008127408 A2

Ruth Nelson,(1989) “End-to-End Encryption at the Network Layer”, Computer Security Applications Conference ,Fifth Annual, 1989, pp. 28

Vasily Sidorov and Wee Keong Ng, (2015) “Transparent Data Encryption for Data-in-Use and Data-at-Rest in a Cloud-Based Database-as-a-Service Solution”, IEEE World Congress on Services, 2015, pp. 221-228

WhatsApp Encryption Overview. (2016). Retrieved from Whatsapp official website:https://www.whatsapp.com/security/WhatsApp-Security Whitepaper.pdf