Peran Kriptografi dalam aplikasi WhatsApp

Agil Sjech Abubakar, Rizki Alrasyid Kaisupy
Universitas Amikom Yogyakarta
Agilbsa10@gmail.com
Universitas Amikom Yogyakarta
rkaisupy@gmail.com

ABSTRAK

Tujuan dilakukannya penelitian ini agar kita bisa mengetahui lebih dalam tentang kriptogafi dan bagaimana perannya dalam aplikasi bertukar pesan yang paling banyak digunakan oleh masyarakat pada saat ini yaitu aplikasi WhatsApp, seperti yang kita ketahui bahwa aplikasi WhatsApp merupakan sebuah aplikasi bertukar pesan yang paling banyak digunakan oleh masyarakat pada saat ini dan label aplikasi bertukar pesan seperti ini tidak pernah lepas dari pihak-pihak yang ingin mengetahui pesan dari pengguna aplikasinya tersebut oleh karena itu harus ada fitur khusus yang mampu untuk mengatasi masalah tersebut. Fitur yang akan kita bahas adalah fitur enkripsi yang mana akan menjadi tolak ukur bagaimana kriptografi dapat berperan dalam aplikasi WhatsApp. Dengan adanya tolak ukur yang kita dapatkan dalam aplikasi WhatApp diharapkan kita dapat mengetahui dengan detail peran kriptografi serta algortima kriptogafi yang paling berperan dalam meggamankan aplikasi WhatsApp melalui fitur enkripsi WhatsApp

Kata Kunci : kriptografi, enkripsi, WhatsApp

ABSTRACT

The purpose of this study is so that we can find out more about cryptographic and how its role in the message exchange application is most widely used by the community today, namely the WhatsApp application, as we know that the WhatsApp application is a message exchange application that is most widely used by the community at this time and the application label exchanging messages like this has never been separated from the parties who want to know the message from the user of the application, therefore there must be a special feature that is able to solve the problem. The feature that we will discuss is the encryption feature which will be a benchmark for how cryptography can play a role in the WhatsApp application. With the benchmark we get in the WhatsApp application, it is expected that we can find out the details of the cryptographic role and cryptographic functions that have the most role in securing WhatsApp applications through the WhatsApp encryption feature.

Keywords : cryptographic, encryption, WhatsA

PENDAHULUAN

Kriptogarfi sebenarnya sudah menjelaskan banyak hal tentang bagaimana merahasiakan ataupun menggamankan data yang kita miliki namun dalam konteks kali ini kita akan dihadapkan dengan sebuah aplikasi bertukar pesan yang paling populer di masyarakat pada saat ini yaitu aplikasi WhatsApp, oleh karena itu kita akan menelaah lebih dalam tentang kriptografi sehingga kita dapat menemukan sebuah metode dari kriptografi sehingga kita dapat menemukan detail peran kriptografi itu sendiri. Secara umum kita perlu ketahui bahwa kriptografi itu sendiri juga memiliki banyak metode maupun algoritma yang digunakan untuk mengenkripsikan sebuah data dan hal itu yang menjadi dasar penelitian kita untuk dapat menetapkan dengan tepat dan akurat dasar metode yang paling pas pada fitur enkripsi yang ada pada aplikasi WhatsApp oleh karena itu kita perlu untuk mejabarkan unsur-unsur yang terdapat pada kriptografi dan unsur-unsur yang terdapat pada aplikasi WhatsApp sampai kebagian dimana unsur-unsur tersebut memiliki kesinambungan sebagai bagian yang berperan dan bagian yang merasakan peran tersebut agar dalam proses penetapan tidak terjadi permasalah dikarenakan tidak adanya kesinambungan antara kriptogarfi dengan aplikasi WhatsApp yang berakibat pada kurangnya keterkaitan antara kriptografi dengan aplikasi WhatsApp maka dari itu kita akan menjabarkan unsur-unsur yang terdapat pada kriptogarfi dan unsur-unsur yang terdapat pada aplikasi WhatsApp.

Kriptografi

Bagian inilah yang mejadi dasar paling penting dalam proses penelitian ini karena kriptografi adalah dasar dari terciptanya judul yang kami buat dan merupakan metode paling dasar yang digunakan untuk mengenkripsikan sebuah data yang kemudian dijadikan sebagai dasar untuk mencari perannya terhadap fitur enkripsi yang ada pada aplikasi WhatsApp oleh karen itu kita perlu untuk menjabarkan lagi bagian-bagian kecil yang terdapat pada kriptografi yang sekiranya mampu dijadikan dasar terciptanya fitur enkripsi pada aplikasi WhatsApp tersebut yang akan dijabarkan sampai ke bagian dasarnya. namun sebelum kita menjabarankan sampai kebagian sandi-sandinya kita harus tau kalau sandi yang terdapat pada kriptografi berdasar pada metode subtisusi dan metode transposisi. Banyak sandi yang terdapat di dalam kriptografi namun disini kita akan menjelaskan mengenai beberapa sandi dasar yang terdapat di dalam kriptografi sehingga mempermudah kita dalam mencari hubungannya dengan fitur enkripsi pada aplikasi WhatsApp.

Algoritma kriptografi klasik

Kriptografi yang satu ini menjadi awal mula lahirnya algortima-algoritma yang bertugas untuk mengamankan sebuah data dan merupakan algoritma kriptogarfi yang telah lahir sejak berabad abad yang lalu, untuk prosesnya sendiri terbilang sederhana dan tidak membutuhkan media yang terlalu canggih, untuk pembuatannya sendiri juga tidak perlu menggunakan computer. Dari kriptografi klasik ini kita akan mendapatkan beberapa metode yang akan digunakan untuk mendapatkan sandi-sandi yang akan diterapkan untuk mengamankan sebuah data, metode-metode tersebut adalah sebagai berikut

1. Kriptografi subtitusi

Metode ini secara singkat berperan dalam mengenkripsikan data melalui proses perubahan data, baik itu perubahan data tunggal maupun secara menyeluruh. Metode ini akan melahirkan beberapa sandi pada kriptografi sebagai berikut

1. Sandi Ceasar
2. Sandi Subtitusi
3. Sandi Affine
4. Sandi Vigenere
5. Sandi Hill
6. Sandi One Time Pad
7. Sandi Rotor

2. Kriptografi transposisi

Metode ini secara singkat memiliki peran yang sama dengan metode subtitusi namun dari segi proses terdapat perbedaan yaitu metode ini memiliki proses pemindahan posisi antara suatu data yang akan dienkripsikan. Metode ini akan melahirkan beberapa sandi pada kriptografi sebagai berikut

1. Sandi Transposisi Columnar
2. Sandi Permutasi

Algoritma kriptografi modern

Kriptografi yang satu ini merupakan bentuk baru yang lahir dari kriptografi klasik yang kemudian melahirkan algoritma-algoritma baru dari hasil pembaruan yang bertujuan untuk memperkuat keamanan yang dihasilkan dari algoritma-algoritma yang terdapat pada kriptografi klasik. Dari kriptografi modern ini akan lahir metode baru lagi yang akan berperan untuk lebih mengamankan data. Metode tersebut sebagai berikut

1. Kriptografi simetris

   Metode ini merupakan sebuah metode pengenkripsian data yang hanya membutuhkan 1 kunci baik itu untuk enkripsi maupun deskripsinya. Secara umum metode algoritma simetris ini akan melahirkan beberapa metode aplikasi yang dapat digunakan untuk mengamankan data yang kita miliki, aplikasi tersebut sebagai berikut

   1. DES *(Data Encryption Standart)*
   2. AES *(Advance Encryption Standart)*
   3. IDEA *(Internasional Data Encryption Algorithm)*
   4. A5
   5. RC4
2. Kriptografi asimetris

   Metode ini merupakan perbaikan dari metode sebelumnya yaitu metode simetris karena metode tersebut hanya berisikan 1 kunci sehingga memiliki keamanan yang lebih rendah meskipun kita ketahui bahwa antara metode simetris dan asimetris sama sama memiliki keamanan yang sudah mumpuni. Dari metode asimetris ini akan melahirkan algoritma-algoritma baru sebagai berikut

   1. Algoritma RSA
   2. Algoritma Knapsack Merkle-Hellman
   3. Algoritma ElGamal
   4. Algoritma fungsi hash satu arah
   5. Algoritma DMDC (DES-*like Message Digest Computation*)
   6. MD-5
   7. ECC (*Elliptic Curve Cryptosystem*)

WhatsApp

WhatsApp adalah salah satu aplikasi bertukar pesan yang paling banyak diminati oleh masarakat sampai saat ini tentunya banyak pihak yang akan menyoroti bagaimana bisa aplikasi ini mampu untuk berkembang dengan sangat pesat. Salah satu faktor yang mempengaruhi perkembangan WhatsApp itu sendiri terdapat di keamanannya, seperti yang kita ketahui bahwa WhatsApp dengan percaya diri meghadirkan fitur mereka yang mampu menjawab semua pertanyaan masarakat mengenai keamanan pesan yang mereka kirim ke sesama pengguna WhatsApp melalui fitur enkripsi mereka

Fitur enkripsi WhatsApp

Fitur ini seakan menjadi jawaban dari semua keresahan masarakat dalam bertukar pesan secara aman seperti yang kita ketahui bahwa WhatsApp menerapakan ketentuan untuk aplikasi mereka sebagai berikut

1. Fitur enkripsi end to end

METODE PENELITIAN

Dalam metode penelitian ini kita akan memulainya dengan mengamati terlebih dahulu bagian-bagian yang telah kita jabarkan pada pembahasan sebelumnya tentang kriptografi dan WhatsApp sehingga kita dapat meneliti peran kriptografi itu sendiri namun sebelum itu kita harus menentukan poin manakah yang akan diamati terlebih dahulu. Dalam penelitian ini yang menjadi poin paling utama untuk diamati adalah aplikasi WhatsApp itu sendri dengan pertimbangan kemudahan mencocokan antara poin-poin yang terdapat dalam kriptografi dengan poin-poin yang terdapat dalam aplikasi WhatsApp karena sudah kita ketahui bahwa dari pembahasan sebelumnya poin-poin yang terdapat didalam kriptografi terlalu banyak sehingga akan mempersulit proses pencocokan dan akan memperlama proses penelitian. Untuk aplikasi WhatsApp sendiri seperti yang telah dibahas sebelumnya bahwa dalam aplikasi ini terdapat sebuah fitur yang mampu untuk mengamankan pesan yang terdapat dalam aplikasi tersebut sehingga tidak dapat dilihat oleh pihak ketiga selain sang pengirim dan sang penerima pesan yang berupa teks, foto, suara maupun video. Fitur yang dimaksud adalah fitur enkripsi pesan pada aplikasi WhatsApp. Dari fitur yang telah kita teliti ini terdapat kata enkripsi yang merupakan suatu proses perahasiaan data sehingga data tidak dapat dilihat dengan mudah oleh pihak ketiga

Fitur enkripsi pada WhatsApp sendiri menerapkan metode enkripsi end to end yang merupakan metode terbaru yang lahir dari kriptografi modern atau yang lebih spesifik lagi yaitu kriptografi modern yang terdapat pada metode asimetris seperti yang kita ketahui pada pembahasan sebelumnya bahwa metode asimetris merupakan turunan dari kriptografi modern sehingga dari segi keamanan data metode asimetris pada kriptografi modern ini memiliki keamanan tertinggi dari metode simetris pada kriptografi modern maupun metode-metode lain yang terdapat pada kriptografi klasik. Jadi jika dilihat dari segi kecocokan, fitur enkripsi end to end yang terdapat pada aplikasi WhatsApp dengan kriptografi sendiri dapat terbilang sangat cocok dan sangat berkaitan antara satu dengan yang lain dan untuk penelitian kita bias kita pastikan poin-poin antara fitur enkripsi end to end dengan metode asimetris pada kriptografi modern adalah poin penghubung antara aplikasi WhatsApp dengan kriptografi.

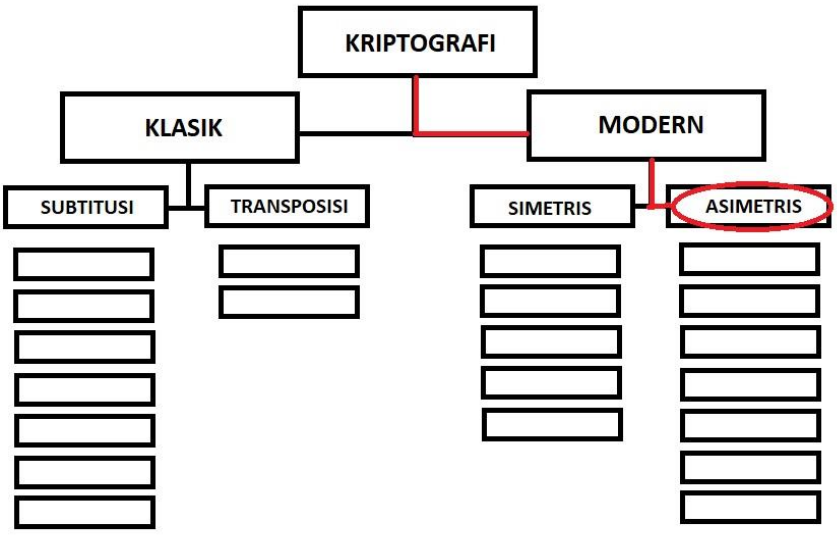
HASIL DAN PEMBAHASAN

Dari hasil penelitian yang telah kami lakukan terdapat beberapa poin penting yang sangat menentukan titik dimana pembahasan antara kriptografi dengan WhatsApp terlihat lebih masuk akal ketika dibahas secara berdampingan karena telah kita buktikan bahwa kriptografi tidak akan pernah lepas dengan sesuatu yang berkaitan dengan pengenkripsian sebuah data dan WhatsApp sendiri secara terang terangan mengatakan bahwa aplikasi mereka telah memiliki sebuah fitur yang mampu untuk mengamankan isi pesan yang terdapat didalam percakapan pengguna aplikasi ini. Dari kata mengamankan isi pesan saja kita sudah bisa membayangkan bahwa hal tersebut tidak akan pernah lepas dengan proses enkripsi data yang akan sangat berperan penting dalam pengamanan isi pesan yang terdapat dalam aplikasi WhatsApp. Belum lagi dari pihak WhatsApp sendiri sudah memperjelas bahwa mereka akan menggunakan fitur enkripsi end to end yang bertujuan agar isi pesan hanya bisa didapat oleh kedua pihak yang saling berkomunikasi tanpa harus diganggu oleh pihak ketiga.

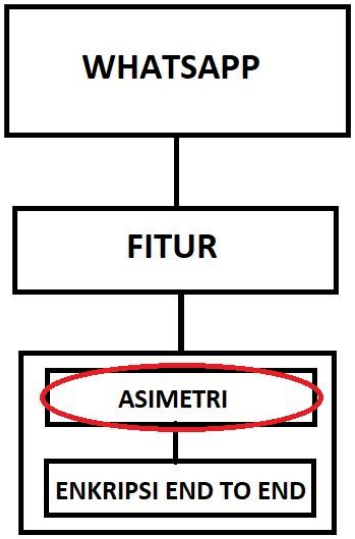
Sturktur keterkaitann

Dalam pembahasan sebelumnya kita telah menjelaskan secara rinci bagian-bagian kecil yang terdapat didalam kriptografi maupun yang terdapat didalam aplikasi WhatsApp kemudian kita telah menemukan dengan bagian yang saling berkaitan yang membuktikan bahwa kriptografi merupakan dasar yang sangat penting dalam penerapan fitur enkripsi pada aplikasi WhatsApp. Namun disini akan kami terangkan secara singkat menggunakan struktur dan menampilkan beberapa gambar penunjang sebagai berikut.

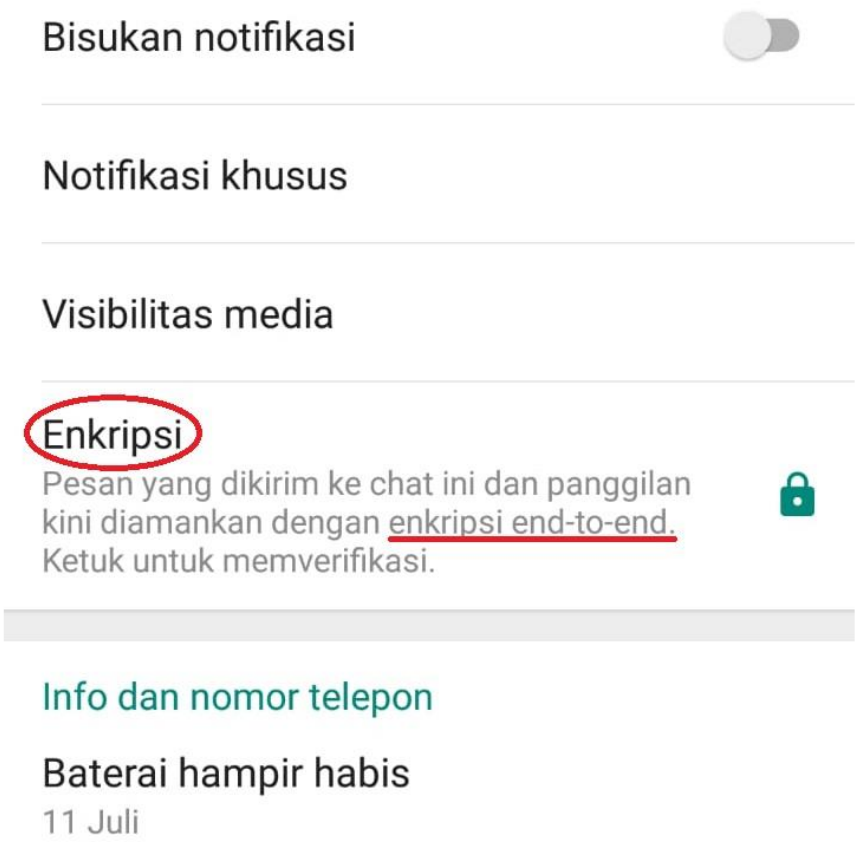
Struktur 1. Keterkaitan kriptografi dengan aplikasi WhatsApp.



Struktur 2. Keterkaitan kriptografi dengan aplikasi WhatsApp



Fitur enkripsi end to end pada WhatsApp



KESIMPULAN

1. Dalam aplikasi WhatsApp pesan yang dikirim dan panggilan akan diamankan dengan enkripsi end-to-end. Perusahaan WhatsApp.Inc memilih untuk menggunakan pengamanan ini agar pengguna lebih merasa aman saat mengirim pesan didalam aplikasi WhatsApp.

2. Algoritma kriptografi modern memiliki tingkat pengaman yang tinggi karena merupakan pengembangan atau terlahir dari algoritma kriptografi klasik

3. Kriptografi yang digunakan oleh WhatsApp adalah kriptografi modern metode Asimetris yang dimana metode kriptografi Asimetris ini lebih rumit daripada metode kriptografi Simetris namun lebih aman untuk digunakan dalam sebuah aplikasi pertukaran pesan yang banyak digunakan oleh masyarakat seperti WhatsApp ini.

REKOMENDASI

Di penelitian ini kami melihat bahwa dalam untuk melakukan pengriman pesan sangat disarankan untuk melakukan pengamanan atau pesan itu di rahasiakan agar tidak pesan itu tidak jatuh ke orang lain atau tangan yang tidak bertanggung jawab, disini WhatsApp hadir dengan fitur pengamanan enkirpsi end-to-end dari aplikasi WhatsApp ini sangat aman dan sangat cocok untuk dipakai untuk mengirim pesan.

UCAPAN TERIMAKASIH atau CATATAN

Dalam penyusunan tugas Matematika Diskret ini tidak terlepas beberapa dukungan dari berbagai pihak, dengan ini kami berdua ingin menyampaikan terima kasih sebesar–besarnya kepada :

1. Allah SWT dengan segala rahmat dan karunia-Nya yang memberikan kami kekuatan dan kesehatan agar bisa mengerjakan tugas.
2. Kepada kedua orang tua kami yang tercinta yang selama ini telah membantu kami dengan bentuk doa, kasih sayang, serta semangat yang tiada hentinya, doa dan kasih sayang itu menjadi salah satu motivasi kita berdua untuk mengerjakan tugas ini.
3. Kepada Universitas Amikom Yogyakarta sebagai tempat kita menimbah ilmu di pergurusn tinggi ini.
4. Kepada Bapak Ferry Wahyu Wibowo, S.Si, M.Cs sebagai pengajar yang telah memberikan kami materi yang semoga menjadi suatu ilmu yang bermanfaat
5. Kepada Bapak Bernadhed, M.kom yang telah memberikan kita motivasi agar tetap tenang dan jangan panik.
6. Kepada Satrio Yudho Pangestu sebagai salah satu mahasiswa Universitas Amikom yang telah membantu kami berdua dalam mengerjakan tugas ini
7. Kepada Aldi Alfiansyah sebagai mahasiswa Universitas Amikom yang telah membantu kami dalam penyusnan kata-kata.
8. Kepada Afochar dan Gilang wahyudi yang telah membantu kami dalam penyusunan tugas ini.
9. Kepada Jihan Ardhyatami Tueka yang telah membantu kami dalam bentuk doa dan semangat yang menjadi suatu motivasi kepada kami.
10. Kepada Bluehole Studio yang telah membuat game PUBG Mobile, dimana kami akan beristirahat untuk memikirkan tugas tugas dengan bermain game PUBG Mobile.
11. Kepada semua pihak yang berpartisipasi dalam penyusunan tugas ini namun sempat tersebutkan.

REFERENSI

Dari hasil pengerjaan tugas penilitian ini kami mendapatkan beberapa refernsi dari berbagai pihak, referensi tersebut kami cantumkan dalam paper ini agar tidak terlibat dalam tindakan plagiatisme, referensi itu adalah sebagai berikut

Buku:

Rifki Sadikim (2012) Kriptografi Jaringan dan Implementasi nya dalam Bahasa Java: Yogyakarta: C.V ANDI OFFSET

Dony Ariyus (2006) Kriptografi Keamanan Data dan Komunikasi : Yogyakarta: Penerbit Graha Ilmu

Internet:

(https://bacaiptek.blogspot.com/2016/09/mengenal-apa-itu-fitur-enkripsi-end-to-end.html), dipublikasikan pada Sabtu, 24 September 2016

(http://gilang-kurniawan.blogspot.com/2012/05/kriptografi-2-macam-macam-algoritma.html) dipublikasikan oleh Gilang Kurinawan pada tanggal 16 Mei 2012

(https://www.slideshare.net/likut101010/kriptografi-klasik-42155874?next_slideshow=1) dipublikasikan pada 29 November 2014

(https://pojokteknologi.com/id/2017/02/16/kriptografi/) dipublikasikan oleh Irvan pada 16 February 2017

(https://www.pcplus.co.id/2016/04/fitur/beginilah-cara-kerja-whatsapp-end-to-end-encryption/) dipublikasikan oleh Wiwiek Juwono pada 12 April 2016

(https://www.posciety.com/apa-itu-end-to-end-encryption/) dipublikasikan oleh Malik Al pada tahun 2017