# SIMULASI ALGORITMA KRIPTOGRAFI A5/3

**Ellyana Kusdiarti Walang[1], Maman Abdurohman[2], Andrian Rakhmatsyah[3]**

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

**Abstrak**

**Algoritma A5/3 merupakan algoritma versi terbaru dari algoritma A5 yang digunakan untuk enkripsi suara dari mobile phone ke Base Transceiver Station (BTS). Algoritma ini dibuat berdasarkan algoritma KASUMI, yaitu sebuah blok cipher yang menghasilkan 64 bit input dari 64 bit output di bawah control kunci 128 bit. Keluaran dari algoritma ini yaitu dua buah blok 114 bit yang akan digunakan untuk enkripsi/dekripsi pada uplink dan downlink. Aplikasi algoritma A5/3 dibuat sebagai suatu simulator untuk mensimulasikan algoritma tersebut. Avalanche effect, waktu proses, dan perubahan besar file, dijadikan sebagai parameter untuk mengukur ketahanan algoritma ini. Berdasarkan pengujian avalanche effect yang dihasilkan oleh algoritma A5/3 adalah 51.053% untuk kasus beda satu bit kunci dengan plainteks yang sama. Sedangkan, untuk kasus beda satu bit plainteks dengan kunci yang sama nilainya adalah 0.877%. Waktu proses bertambah sebanding dengan ukuran file, di mana makin besar file maka makin lama waktu prosesnya. Pada aplikasi ini, ukuran file output sama dengan ukuran file input. Hal itu sesuai dengan algoritma A5/3 yang merupakan algoritma stream cipher.**

**Kata Kunci : A5/3, enkripsi, dekripsi, avalanche effect, waktu proses, besar file**

**Abstract**

**A5/3 algorithm is a new version of A5 algorithm. It is used to encrypt voice and data from mobile phone to Base Transceiver Station (BTS). This algorithm based on KASUMI algorithm, that produces 64 bit output from 64 bit input with 128 bit key. Output from this algorithm are two blocks contain each 114 bit. That blocks is used for encrypt/decrypt on uplink and downlink. Application of algorithm A5/3 is made as simulator to simulate that algorithm. Avalanche effect, process time, and changing of file size are parameter to measure strength of algorithm. Based on this experiments, result of avalanche effect is 51.053% for case that flipping single bit of key with same plaintext. The other hand, avalanche effect for the case that flipping one bit plaintext with same key is 0.877%. The process time increase as same as increasing of file size. So, the large file size need much time to process. The output file size as same as input file size. Therefore, it same as behavior of A5/3 algorithm that a stream cipher.**

**Keywords : A5/3, encrypt, decrypt, avalanche effect, time process, file size**

# 1. Pendahuluan

## 1.1 Latar belakang

*Global System for Mobile Communication* atau biasa disingkat dengan GSM merupakan standar global komunikasi bergerak digital yang dispesifikasikan oleh *Groupe Speciale Mobile* di Eropa. Sekarang ini, jaringan berbasis GSM digunakan oleh lebih dari 130 negara di dunia. GSM mendukung layanan komunikasi suara dan data yang beroperasi pada frekuensi 900 MHz, 1800 MHz, dan 1900 MHz. Masalah keamanan komunikasi menjadi satu faktor penting yang harus diperhatikan pada jaringan GSM karena medium komunikasi berbasis *wireless* cenderung lebih rentan terhadap berbagai serangan. Salah satu cara untuk menjaga keamanan tersebut adalah dengan menerapkan proses kriptografi. Algoritma yang digunakan untuk mengenkripsi trafik suara dan data *user* antara *mobile station* dan *base station* adalah algoritma A5. Algoritma ini diimplementasikan pada *mobile station* dan *Base Station Subsystem* (BSS).

Algoritma A5 terdiri dari tiga versi yaitu A5/1, A5/2 dan A5/3. Algoritma A5/1 dan A5/2 merupakan algoritma yang umum digunakan pada GSM. Namun, pada tahun 2006 Elad Barkan, Eli Biham dan Nathan Keller telah mendemonstrasikan serangan terhadap A5/1 dan A5/2 di mana penyerang dapat menyadap percakapan melalui *mobile phone* kemudian mendekripsikannya baik secara *real time* atau pun tidak [5]. Sejak 1 Juli 2006, GSM *Association* mengamanatkan kepada GSM *Mobile Phone* untuk tidak menggunakan *cipher* A5/2 lagi [2].

Algoritma A5/3 diperkenalkan oleh GSM *Association* dan 3GPP pada tahun 2002 dengan maksud untuk dijadikan algoritma enkripsi standar pada GSM. Algoritma A5/3 merupakan *stream cipher* yang berdasarkan algoritma Kasumi, yaitu suatu blok *cipher* yang memproduksi sebuah *output* 64-bit dari sebuah *input* 64-bit dengan sebuah kunci 128-bit. Algoritma ini memproduksi dua *keystream* 114-bit yang digunakan untuk enkripsi/dekripsi pada *uplink* dan *downlink*. Algoritma A5/3 ini dikatakan lebih kuat dibandingkan dua versi pendahulunya [13]. Oleh karena itu, pada tugas akhir ini akan dibuat suatu aplikasi yang dapat mensimulasikan algoritma A5/3 dan kemudian menganalisis hasilnya.

## 1.2 Perumusan masalah

Berdasarkan uraian latar belakang tersebut, maka pada tugas akhir ini dapat dirumuskan masalah sebagai berikut:

1. Bagaimana membuat aplikasi yang dapat mensimulasikan algoritma A5/3 untuk proses kriptografi.
2. Bagaimana menganalisis hasil dari percobaan pada aplikasi tersebut sehingga dapat diukur kemampuan dari algoritma kriptografi A5/3 berdasarkan tingkat *avalanche effect*, waktu proses, dan perubahan besar file.

Selain rumusan masalah, pada tugas akhir ini juga ditetapkan batasan-batasan sebagai berikut:

1. Tidak mengimplementasikan hasil aplikasi dalam bentuk *hardware.*

2. Tidak memperhatikan layanan pengamanan lain yang ada pada jaringan GSM seperti proses otentikasi dan verifikasi dengan menggunakan algoritma kriptografi A3 dan A8.
3. Tidak memperhatikan bagian perangkat baik *software* dan *hardware* yang ada pada jaringan GSM antara *mobile station* dan *Base Transceiver Station* (BTS).

## 1.3 Tujuan

Adapun tujuan dari tugas akhir ini adalah:
1. Membuat suatu aplikasi untuk simulasi algoritma kriptografi A5/3.
2. Menganalisis kemampuan dari aplikasi algoritma kriptografi A5/3 berdasarkan parameter *avalanche effect*, waktu proses, dan perubahan besar file.

## 1.4 Metodologi penyelesaian masalah

Metodologi penyelesaian masalah yang akan diterapkan pada tugas akhir ini adalah:
1. Studi literatur
   Mempelajari literatur yang relevan dengan permasalahan yakni spesifikasi algoritma A5/3 dan proses kriptografi pada jaringan GSM. Literatur-literatur yang ada tersebut digunakan untuk membantu dalam membuat aplikasi.
2. Analisis dan perancangan model aplikasi yang akan dibuat.
   Pada tahap ini akan dianalisis apa saja kebutuhan sistem, baik *input, output,* atau pun proses dari Algoritma A5/3 dan akan dimodelkan dengan menggunakan *Data Flow Diagram* (DFD).
3. Implementasi aplikasi
   Pada tahap ini akan diimplementasikan aplikasi yang sesuai dengan spesifikasi sebelumnya ke dalam bahasa pemrograman. Implementasi dilakukan dengan menggunakan DELPHI 7.0.
4. Pengujian pada aplikasi
   Pengujian dilakukan untuk mengetahui proses enkripsi/dekripsi yang ada pada aplikasi dan hasilnya yang akan dianalisis.
5. Analisis hasil percobaan
   Menganalisis semua percobaan yang dilakukan berdasarkan parameter yang telah ditentukan yakni tingkat *avalanche effect* dan waktu proses.
6. Penarikan kesimpulan berdasarkan hasil analisis dan penyusunan laporan.

# 5. Kesimpulan dan Saran

## 5.1 Kesimpulan

Dari hasil pengujian dan analsis yang sudah dilakukan maka dapat ditarik beberapa kesimpulan yakni:

1. Waktu proses pada proses dekripsi dan enkripsi relatif sama. Selain itu, waktu prosesnya juga memenuhi standar pada jaringan GSM.
2. Ukuran file input tidak terlalu berpengaruh pada proses enkripsi atau dekripsi.
3. *Avalanche effect* yang didapatkan dari dua jenis kasus yaitu beda 1 bit painteks menghasilkan nilai yang jauh dari ideal, tetapi pada kasus beda 1 bit kunci menghasilkan *avalanche effect* yang bagus karena berada pada range 45-60%.
4. Perubahan besar file tidak terjadi setelah proses enkripsi ataupun proses dekripsi.

## 5.2 Saran

Adapun saran untuk pengembangan TA ini selanjutnya antara lain adalah:

1. Mencoba untuk melakukan optimasi terhadap algoritma ini khususnya pada fungsi KGCORE sehingga bisa lebih baik dari segi kecepatan.
2. Mencoba untuk menganalisis algoritma A5/3 dari parameter keamanan.

# Daftar Pustaka


[1] Avalanche Effect, 2007, http://en.wikipedia.org/wiki/Avalanche_Effect, didownload pada tanggal 29 November 2007.

[2] A5/3, 2006, http://en.wikipedia.org/wiki/A5/3, didownload pada tanggal 9 Februari 2007.

[3] A5/3 dan GEA3 Specifications, 2003, http://www.3gpp.org, didownload pada tanggal 16 Januari 2007.

[4] A. Menezes, P. van Oorschot, S. Vanstone, 1996, "Handbook of Applied Cryptography", CRC Press.

[5] Barkan Elad, Biham Eli, Keller Nathan, 2006, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, http://www.gsm-security.net, 22 Januari 2007.

[6] GSM Association Specification for A5/3,.2000, http://3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_13_Yokohama/Docs/PDF/S3-000362.pdf, didownload pada tanggal 16 Januari 2007.

[7] GSM Security, 2003, http://www.gsm-security.net, didownload pada tanggal 9 Februari 2007.

[8] KASUMI Specification, 1999, http://www.3gpp.org, didownload pada tanggal 8 Februari 2007.

[9] Kristanto, Andri, 2003, "Keamanan Data Pada Jaringan Komputer", Gava Media.

[10] Kurniawan, Yusuf, Ir., MT., 2004, "Kriptografi Keamanan Internet dan Jaringan Telekomunikasi", Informatika Bandung.

[11] Mobile Communication, 2001, http://www.informatik.uni-reiburg.de/~softech/teaching/ws01/itsec/, didownload pada tanggal 31 Agustus 2007.

[12] Munir, Rinaldi, 2006, "Kriptografi", Informatika.

[13] Quirke, Jeremy, 2004, Security in the GSM System, http://www.ausmobile.com, didownload pada tanggal 21 Januari 2007.

[14] Schafer, Gunter, 2003, "Security in Fixed and Wireless Networks", John Wiley & Sons, Inc.

[15] Schneier, Bruce, 1996, "Applied Cryptography", John Wiley & Sons, Inc.

[16] Survey Pelanggan Operator Seluer, 2007, http://wordpress.com/tag/mentari/Feed, didownload pada tanggal 4 Desember 2007.

[17] Wahana Komputer, 2003, "Memahami Model Enkripsi dan Security Data", ANDI Yogyakarta.