Pengaruh Penggunaan Jaringan Wifi dan 3G Pada Aplikasi Telepon Anti Sadap

Effect of the Use of Wifi and 3G Networks in Secure Phone Call Application

Ryan Ari Setyawan, Selo, Bimo Sunafri Hantono
Laboratorium Sistem Elektronis, Jurusan Teknik Elektro dan Teknologi Informasi, Fakultas Teknik, Universitas Gadjah Mada
Jl. Grafika No.2 Yogyakarta Indonesia - 55281
e-mail: ryan.ari.mti13@mail.ugm.ac.id

Naskah diterima: 23-09-2014, direvisi: 22-10-2014, disetujui: 21-11-2014

Abstrak

Aplikasi telepon anti sadap merupakan suatu aplikasi layanan telepon internet yang dibuat dan telah terdapat algoritma enkripsi TEA, algoritma enkripsi tersebut digunakan agar pihak ketiga tidak dapat melakukan proses penyadapan atau serangan. Namun aplikasi telepon anti sadap tidak terlepas dari jaringan yang digunakan. Tujuan dari penelitian ini adalah melakukan pengujian terhadap penggunaan jaringan wifi dan 3G sebagai konektivitas aplikasi telepon anti sadap. Hasil ujicoba menunjukkan bahwa jaringan wifi-wifi memiliki *delay* 0,003391 *seconds* dan *troughput* sebesar 126,173 kbps sehingga aplikasi telepon anti sadap dapat berjalan dengan baik apabila konektivitas jaringan yang digunakan adalah jaringan Wifi.

Kata kunci: android, enkripsi, *tiny encryption algorithm, voice over internet protocol*.

Abstract

Secure phone call application is an internet phone service application that has been developed and had a TEA encryption algorithm, the encryption algorithm is used so that third parties can not conduct any tappings or attacks. However, the application can not be separated from the network used. The purpose of this study is to test the use of wifi and 3G networks connectivity applications as secure phone call. Results of the trial indicate that the wifi-wifi network has 0.003391 seconds delay and throughput of 126.173 kbps so the secure phone call application can run well when network connectivity used is the Wifi network.

Keywords: *android, encryption, tiny encryption algorithm, voice over internet protocol*

PENDAHULUAN

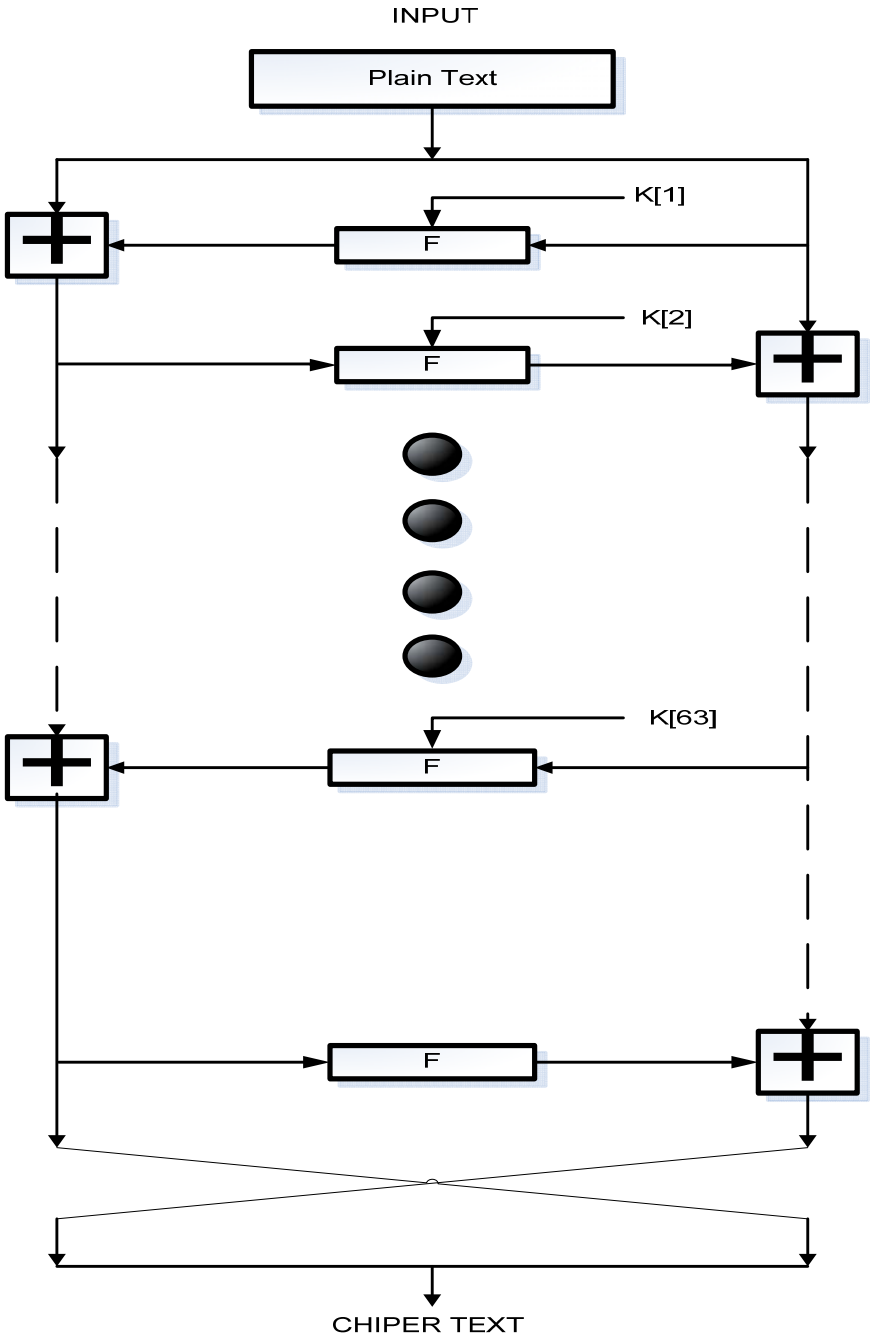
Teknik enkripsi secara *end-to-end* merupakan salah satu solusi yang dibutuhkan untuk keamanan dalam berkomunikasi secara *real-time* melalui telepon (I. Burns, dkk, 2011). Hal tersebut dilakukan untuk meminimalisir proses penyadapan. Berbagai penelitian telah dilakukan mengenai algoritma kriptografi enkripsi untuk keamanan data pada saat melakukan telepon seperti penggunaan algoritma *Elliptic-Curve Diffie-Hellman* (ECC) dan penggunaan kunci dinamis yang tujuannya agar tidak dapat dilakukan proses penyadapan, baik berupa serangan terhadap jaringan maupun melalui kriptoanalisis (C.-H. Wang & Y.-S. Liu, 2011). Penggunaan algoritma RC4 juga dilakukan untuk keamanan data suara dalam jaringan *voice over internet protocol* (VoIP) (M. S. Kumar & M. Sudhakar, 2013), hasil yang didapatkan adalah bahwa algoritma enkripsi menggunakan algoritma RC4 dapat dilakukan meskipun masih memiliki kelemahan algoritma tersebut dipecahkan oleh kriptanalisis dengan teknik *bruto force* (N. Couture and K. B. Kent). Penelitian berikutnya penggunaa algoritma *ephimeral Diffie-Hellman* untuk sistem keamanan jaringan VoIP di *platform android* (Saruchi Kukar, 2012), tujuannya adalah memberikan rekomendasi algoritma dan perancangan keamanan *VoIP* di *android*.

Dalam penelitian ini algoritma yang digunakan adalah *tiny encryption algorithm* (TEA). TEA merupakan algoritma enkripsi modern yang menjadi kandidat lima terbesar algoritma *advance encryption system* (AES) (J. Nechvatal, dkk, 2001). Algoritma TEA dipilih dalam penelitian ini karena memiliki karakteristik yang sangat efisien untuk diimplementasikan pada *platform* berbasis *mobile device* serta memiliki keunggulan memaksimalkan kecepatan dan meminimalkan memori (S. A. Y. Hunn, dkk, 2012) dibandingkan dengan algoritma kriptografi yang lain. Algoritma tersebut nantinya akan ditanamkan pada aplikasi telepon VoIP. Teknik enkripsi yang dilakukan terhadap telepon anti sadap tersebut tidak lepas dari suatu konektivitas jaringan yang digunakannya, walaupun teknik enkripsi yang digunakan memakai algoritma yang memiliki tingkat keamanan yang sangat tinggi namun konektivitas jaringan juga sangat mempengaruhi baik atau buruknya komunikasi yang dihasilkan.

Melihat situasi tersebut, penelitian ini akan melakukan ujicoba pengaruh konektivitas jaringan terhadap aplikasi telepon anti sadap. Tujuannya untuk mengetahui komunikasi yang dihasilkan pada aplikasi telepon anti sadap apabila menggunakan jaringan yang berbeda. Jaringan yang digunakan untuk ujicoba dalam penelitian ini yakni menggunakan *Wifi* dan *3G*. *Paper* ini akan membahas lebih lanjut mengenai algoritma TEA, desain sistem serta implementasi dan ujicoba aplikasi telepon anti sadap di jaringan *Wifi* dan *3G*.

Tiny Encryption Algoritma (TEA) adalah Algoritma yang cepat dan sederhana serta memiliki feistel berbasis *block chiper* dirancang menjadi salah satu algoritma kriptografi tercepat dan paling efisien dibandingkan dengan algoritma lain seperti RC4 dan ECC (S. A. Y. Hunn, dkk, 2012). TEA diperkenalkan oleh Roger M. Needham dan David J. Wheeler pada tahun 1994. TEA dirancang untuk *mobile system* dengan karakteristik meminimalkan memori dan memaksimalkan kecepatan dengan membuat operasi dasar yang sangat mudah dan sederhana.

Operasi dasar algoritma TEA sangat mudah dan sederhana untuk dipelajari. Dimulai dengan masukan pada algoritma enkripsi pada dasarnya adalah sebuah blok *plaintext* dan K (Kunci). *Plaintext* diwakili oleh P dimana dapat dibagi menjadi dua bagian Kiri [0] dan Kanan [0] sementara *teks cipher* diwakili oleh C (Kiri[64], Kanan [64]) (S. A. Y. Hunn, dkk, 2012). Sebagian dari *plaintext* P digunakan untuk mengenkripsi, sebagian lainnya mengalami proses 64 putaran dan kemudian digabungkan bersama-sama menghasilkan *chiper* blok teks. Skema algoritma TEA diperlihatkan pada Gambar 1.



Gambar 1. Skema Algoritma TEA
(Sumber: S. A. Y. Hunn, dkk, 2012)

```
void code(long* v, long* k) {
      unsigned long y=v[0],z=v[1], sum=0, /* set up */
                        delta=0x9e3779b9, /* penjadwalan kunci
                        n=64 ;

      while (n-->0) { /* mulai proses perputaran */
                  sum += delta ;
                  /* proses XOR
                  y += ((z<<4)+k[0]) ^ (z+sum) ^ ((z>>5)+k[1]) ;
                  z += ((y<<4)+k[2]) ^ (y+sum) ^ ((y>>5)+k[3]) ;
      } /* end cycle */
      v[0]=y ; v[1]=z ; }
```

Gambar 2. *Pseudocode* TEA

Untuk sistem penyandian TEA menggunakan proses *feistel network* dengan menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik. Pergeseran dua arah (ke kiri dan ke kanan) menyebabkan semua bit kunci dan data bercampur secara berulang ulang. TEA memproses 64-bit *input* sekali waktu dan menghasilkan 64-bit *output*. TEA menyimpan 64-bit *input* kedalam L_0 (kiri) dan R_0 (kanan) masing masing 32-bit. Sedangkan 128-bit kunci disimpan kedalam k(0), k(1), k(2), dan k(3) yang masing masing berisi 32-bit. Sedangkan kinerja algoritma TEA dijelaskan pada Gambar 2. *pseudocode*.

Gambar 2. memperlihatkan *pseudocode* algoritma TEA dengan langkah sebagai berikut :

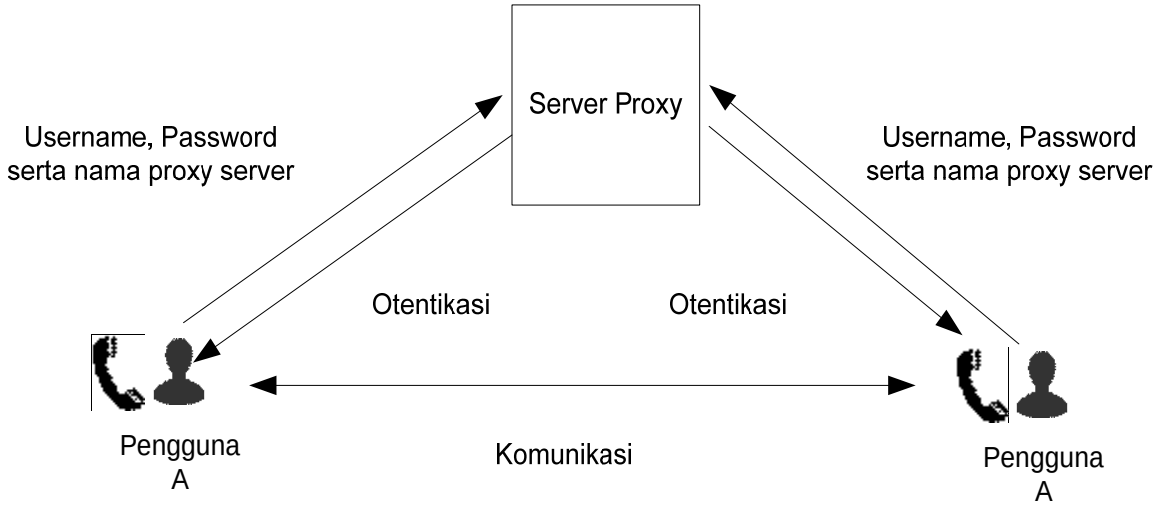
1. Pergeseran (*Shift*)
   Block teks terang pada kedua sisi masing-masing sebanyak 32-bit akan digeser ke kiri sebanyak empat (4) kali dan digeser ke kanan sebanyak lima (5) kali.

2. Penambahan
   Langkah selanjutnya setelah digeser ke kiri dan ke kanan, maka Y dan Z yang telah digeser akan ditambahkan dengan kunci K[0]-K[3]. Sedangkan Y dan Z awal akan ditambahkan dengan *sum* (delta).

3. Proses *XOR*
   Proses selanjutnya setelah dioperasikan dengan penambahan pada masing-masing *register* maka akan dilakukan proses *XOR*. Hasil penyandian dalam satu *cycle* satu blok teks terang 64-bit menjadi 64-bit teks sandi adalah dengan menggabungkan Y dan Z. Untuk penyandian pada *cycle* berikutnya Y dan Z ditukarkan posisinya, sehingga Y_1 menjadi Z_1 dan Z_1 menjadi Y_1 lalu dilanjutkan proses seperti langkah-langkah diatas sampai 16 *cycle* (32 *round*).

4. *Key Schedule*
   Algoritma TEA menggunakan *key schedule*-nya sangat sederhana yaitu kunci k[0] dan k[1] digunakan *round* ganjil sedangkan kunci k[2] dan k[3] konstan digunakan untuk *round* genap.

5. Deskripsi dan Enkripsi
   Proses dekripsi sama halnya seperti pada proses penyandian yang berbasis *feistel chiper* lainnya. Yaitu pada prinsipnya adalah sama pada saat proses enkripsi. Hal yang berbeda adalah penggunaan teks sandi sebagai *input* dan kunci yang digunakan urutannya dibalik.



Gambar 3. Proses Penggunaan SIP

Sedangkan protokol yang digunakan dalam penelitian ini yakni *Session Intitiation Protocol* merupakan protokol pada *Voice over Internet Protocol* (VoIP) (Jaber, dkk, 2013) atau dapat dikatakan *protocol signaling* lapisan aplikasi yang menggunakan berbasis *text message* untuk membangun, memodifikasi, dan mengakhiri komunikasi multimedia antara dua pengguna atau lebih (Johnston, dkk, 2012).

Mekanisme penggunaan SIP adalah yang pertama *user* terlebih dahulu mendaftar di *Server* SIP, prosesnya dapat dilihat pada Gambar 2, kemudian setelah mendapatkan akun *user* dapat melakukan panggilan ke sesama pengguna SIP. Untuk dapat menggunakan aplikasi telepon internet gratis melalui SIP tersebut *use*r cukup memasuk *username*, *password*, serta nama *server* yang digunakan.

METODE

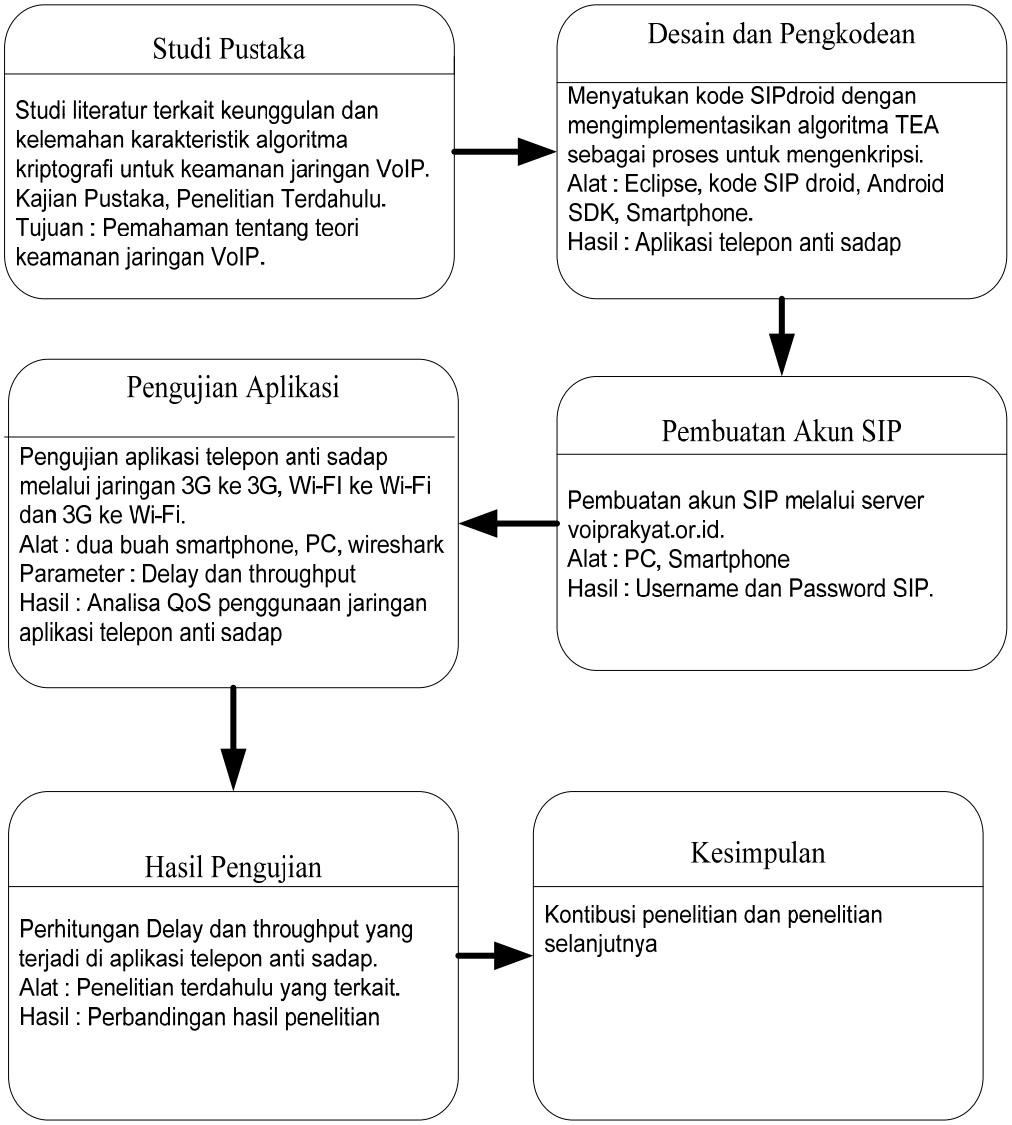
Metode yang dilakukan meliputi materi serta alat yang digunakan, dan tahapan penelitian yang dilakukan. Dalam pembuatan aplikasi telepon anti sadap ini diperlukan penganalisaan kebutuhan perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan agar aplikasi ini dapat berjalan seperti yang direncanakan.

Perangkat keras yang digunakan dalam penelitian ini merupakan kebutuhan sistem utama dari sebuah sistem komputer secara fisik, yang terdiri dari komponen-komponen yang saling terkait yaitu berupa masukan, proses dan keluaran. Perangkat keras yang digunakan dalam penelitian ini adalah satu unit laptop dengan spesifikasi Prosesor Intel® Core™ i3-3110M CPU @2.40Ghz, *Harddisk* 500 GB, RAM 2,00 GB, kabel data. *Smartphone* berbasis android, untuk menjalankan program aplikasi yang dibuat dengan spesifikasi sebagai berikut, sistem Operasi : Android 4.3 (*Jelly Bean*), dual-core 1.2 Ghz, 4GB, 1GB RAM. Kabel data serial *port*, fungsi dari kabel data ini adalah untuk menghubungkan antara komputer dengan *smartphone.*

Sedangkan perangkat lunak yang digunakan dalam penelitian ini yakni bahasa pemrograman menggunakan *java development kid* (jdk) 1.6 dan *java runtime environment* (jre), sistem operasi windows 7 (32-bit), *integrated development environment* (ide) eclipse kepler, *android software development kit* (android sdk), *android development tools* (adt), dan wireshark.

Aplikasi yang berjalan di dalam sistem operasi Android terdapat beberapa keterbatasan pada perangkat berbasis Android. Sehingga sebelum melakukan pengujian maka perlu diperhatikan untuk mengembangkan aplikasi diantaranya :

a. Sumber daya memori yang terbatas, hingga saat ini perangkat Android yang banyak beredar memiliki kapasitas memori terbatas sehingga dalam hal ini yang digunakan adalah algoritma yang sesuai dengan karakteristik *smartphone*.
b. Sumber daya baterai yang secara efektif hanya mampu bertahan selama kurang lebih 6 jam, dengan penggunaan secara terus-menerus dan kurang lebih 200 jam dalam keadaan *standby.*
c. Tampilan antar muka aplikasi sangat berpengaruh terhadap waktu tunggu hingga aplikasi benar-benar siap diguna-



Gambar 4. Tahapan Penelitian

kan, semakin banyak komponen yang digunakan akan semakin lama pula waktu tunggu yang dibutuhkan.

d. Konektivitas jaringan dapat tergantung dari *basestation* disekitar apabila menggunaka jaringan 3G dan tergantung dari *access point* apabila menggunakan jaringan wifi.

Tahapan penelitian yang dilakukan dalam penelitian ini diperlihatkan pada Gambar 4.

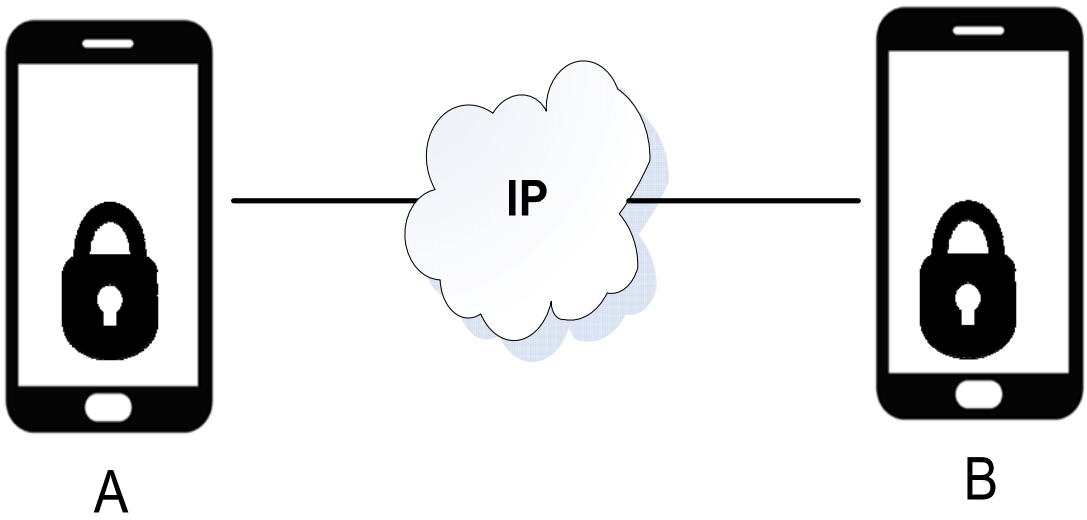
Gambar 4 menjelaskan bahwa alur dari penelitian ini yakni studi literatur dengan membaca referensi baik melalui buku, jurnal, dan karya ilmiah penelitian sebelumnya mengenai karakteristik keunggulan dan kelemahan algoritma kriptografi, hasilnya adalah rekomendasi algoritma kriptografi untuk pengembangan aplikasi telepon anti sadap. Kemudian melakukan proses desain sistem yang dilanjutkan pengkodean dengan mengimplementasikan algoritma kriptografi ke kode SIPdroid. Proses selanjutnya melakukan pendaftaran akun SIP di *server* voiprakyat.or.id untuk dapat melakukan pensinyalan (*signaling*) serta proses pengujian aplikasi di jaringan wi-fi dan 3G dianalisis menggunakan *software wireshark*, kemudia melakukan perhitungan hasil pengujian serta pengambilan kesimpulan.

Desain sistem aplikasi telepon anti sadap yang dibuat menggunakan *smartphone android,* untuk mekanisme kerja aplikasi telepon anti sadap lebih rinci dijelaskan pada Gambar 5 .

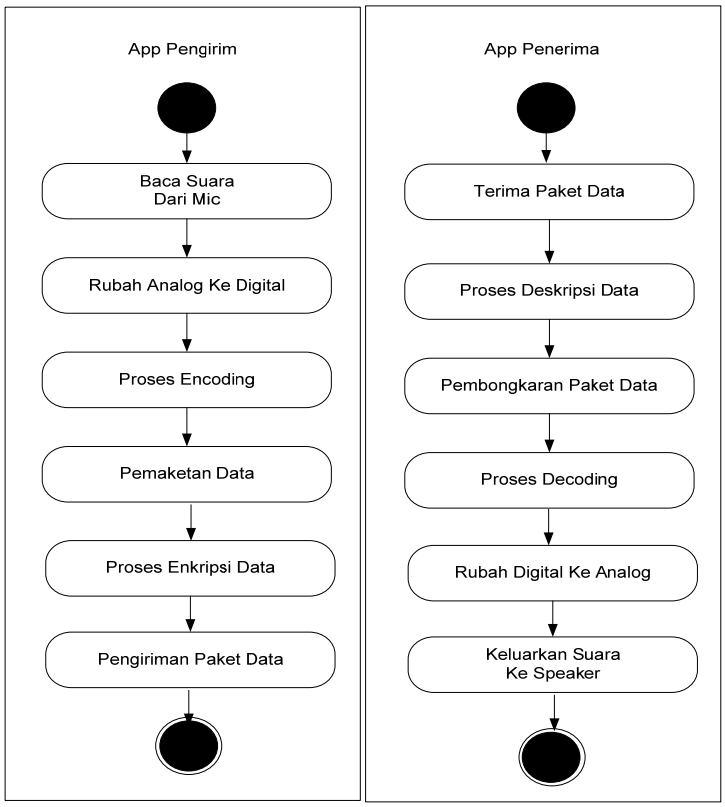
Gambar 5. Menjelaskan pada *smartphone* A dan *smartphone* B telah terdapat aplikasi telepon anti sadap yang masing-masing sudah memiliki kunci untuk enkripsi-deskripsi pada data suara sehingga paket data dijaringan sudah diacak. Penjelasan mengenai mekanisme kinerja aplikasi telepon anti sadap adalah sebagai berikut :

a. Pensinyalan : *Session Intitiation Protokol* (SIP)
   → *SIPsecure*
   → *Transport Layer Security* digunakan untuk protokol kriptografi.
b. Data Suara : *Real-time Transport Protokol* (RTP).
   → *Secure Real-time Transport Protokol*
   → Algoritma TEA

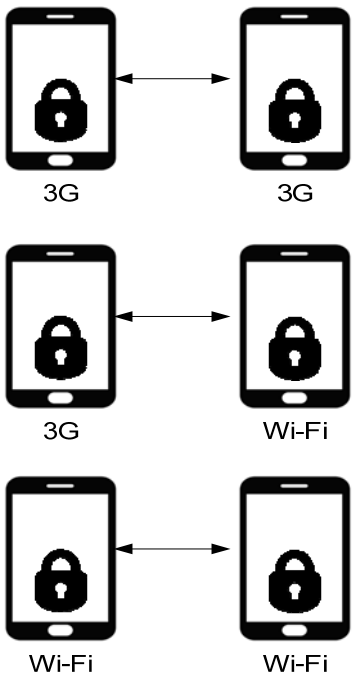
Untuk mekanisme proses enkripsi-deskripsi yang terjadi pada aplikasi telepon anti sadap dapat dijelaskan melalui diagram aktivitas pada Gambar 6.



Gambar 5. Mekanisme Telepon Anti Sadap



Gambar 6. Proses enkripsi-dekripsi aplikasi telepon anti sadap



Gambar 7. Desain Pengujian Jaringan

Gambar 7. Memperlihatkan proses enkripsi dan dekripsi aplikasi dimana proses enkripsi terjadi pada *payload* saja yang merupakan segmen-segmen dari datagram TCP/IP kemudian dienkapsulasi dengan menggunakan *header* IP dari protokol IP. Untuk proses dekripsi kinerjanya terbalik dari proses enkripsi.

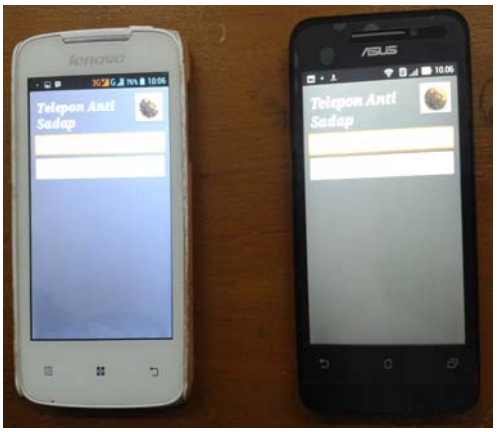
Desain pengujian dilakukan untuk melakukan pengujian terhadap penggunaan jaringan di aplikasi telepon anti sadap dilakukan melalui penggunaan jaringan wifi dan 3G, adapun skema pengujian dapat dilihat pada Gambar 7. Sesuai dengan Gambar 7 proses pengujian aplikasi telepon anti sadap diuji menggunakan berbagai konektivitas jaringan yakni dari 3G ke 3G, 3G ke *Wi-Fi*, dan *Wi-Fi* ke *Wi-Fi* dengan menggunakan dua buah *smartphone* berbasis android.

Skenario Pengujian dilakukan saat melakukan implementasi aplikasi, hasil ujicoba dianalisis dan kemudian melakukan perhitungan terhadap *troughput* dan *delay* yang terjadi saat melakukan komunikasi percakapan pada aplikasi telepon anti sadap.

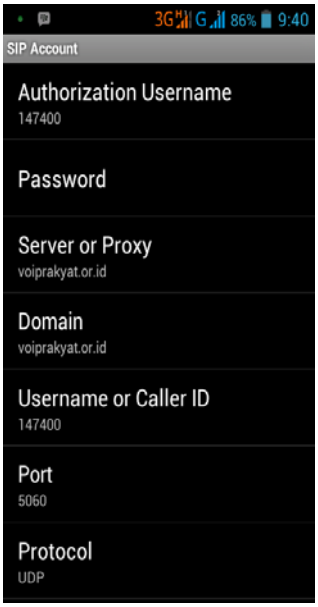
1. Mengatur koneksi jaringan pada masing-masing *smartphone* dengan perlakuan :
   - Untuk pengujian yang pertama *smartphone* A dan B sama-sama menggunakan koneksi jaringan 3G.
   - Untuk pengujian yang kedua salah satu *smartphone* diubah koneksi-nya memakai *Wifi*.
   - Untuk pengujian yang ketiga *smartphone* A dan B sama-sama menggunakan koneksi *Wifi*.
2. Memasukan *username* dan *password* sesuai dengan akun SIP yang didapatkan dari *server* SIP voiprakyat.or.id
3. Setelah itu menunggu akun SIP masing-masing *smartphone* telah terotentikasi oleh *server* SIP sampai siap digunakan.
4. Salah satu dari *smartphone* tersebut masukan *Caller ID* atau no telepon yang akan dituju.
5. Lakukan percakapan yakni hanya dengan mengucapkan kata “hallo”.
6. Amati paket data dan dianalisis dengan *wireshark*.

HASIL DAN PEMBAHASAN

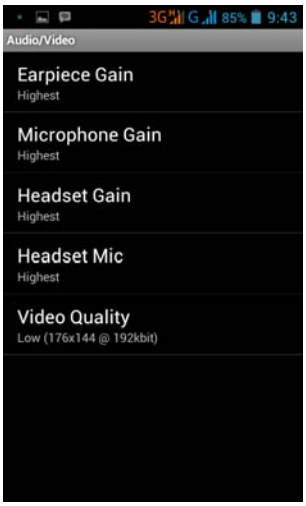
Pengujian menggunakan dua *smartphone* android yang masing-masing telah terdapat aplikasi telepon anti sadap seperti pada Gambar 8.



Gambar 8. Aplikasi Telepon Anti Sadap



Gambar 9. Konfigurasi SIP



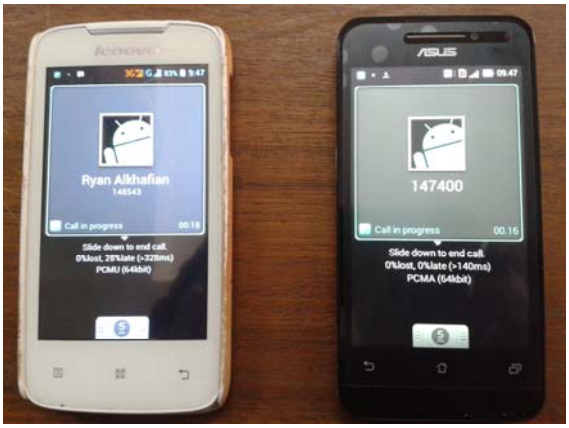
Gambar 10. Konfigurasi Audio

Namun sebelum melakukan panggilan percakapan melalui aplikasi telepon anti sadap terlebih dahulu melakukan langkah-langkah sebagai berikut :

a. Konfigurasi SIP
   Masukan *username, password*, nama *server* dan penggunaan jaringan pada aplikasi seperti Gambar 9.
b. Konfigurasi Audio
   Untuk mendapatkan hasil yang baik maka masing-masing konfigurasi audio pada *smartphone* di *set* ke *level highest* semua kecuali pada *video quality* seperti pada Gambar 10.

Setelah itu tunggu sampai proses otentikasi *server* selesai dan jika selesai seperti Gambar 11.

Gambar 11. Otentikasi SIP



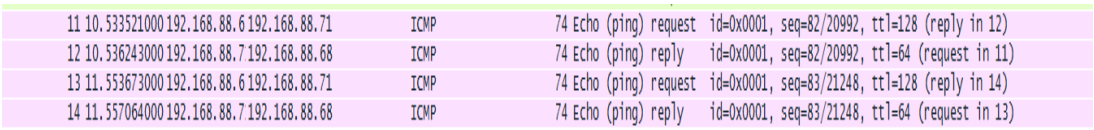
Gambar 12. Komunikasi Telepon Anti Sadap

c. Lakukan Panggilan
   Lakukan panggilan dengan cara memasukan *Caller ID* yang dituju.
d. Pengujian aplikasi ke jaringan
   Aplikasi diuji melalui jaringan Wi-Fi dan 3G sesuai dengan desain pengujian. Pengujian aplikasi dilakukan selama 10 kali pengujian. Hal tersebut dilakukan untuk mendapatkan prosentase komunikasi yang dihasilkan pada Tabel 1.

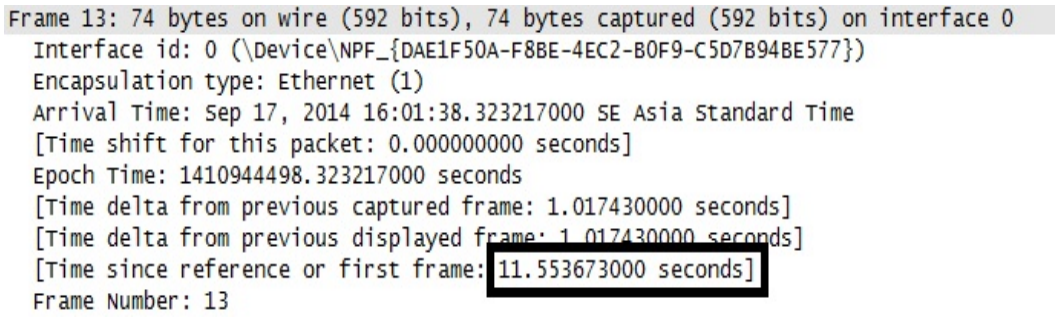
Tabel 1. Memperlihatkan bahwa proses komunikasi yang terjadi pada penggunaan jaringan 3G memiliki prosentase komunikasi putus-putus dan delay yang besar. Namun dari hasil pengujian tersebut diperlukan analisis lebih lanjut untuk mengetahui delay dan *troughput* yang terjadi pada saat komunikasi. *Bandwith* yang digunakan dalam penelitian ini yakni wifi sebesar 2 Mbps dan 3G sebesar 1,06 Mbps. Maka analisis lebih lanjut tersebut adalah sebagai berikut :

Tabel 1. Hasil Pengujian Jaringan

Jaringan	Delay	Komunikasi Putus-Putus
3G dan 3G	85%	87%
3G dan Wifi	83%	68%
Wifi dan Wifi	10 %	12%



Gambar 13. Hasil ICMP *wireshark*



Gambar 14. *Time since reference*

Tabel 2. Delay

Koneksi	Paket dikirim (s)	Paket diterima(s)	Delay (s)
3G-3G	168,011820000	168,019601000	0,007781
3G-Wifi	328,065653000	328,068768000	0,003115
Wifi-Wifi	11,553673000	11,557064000	0,003391

Delay

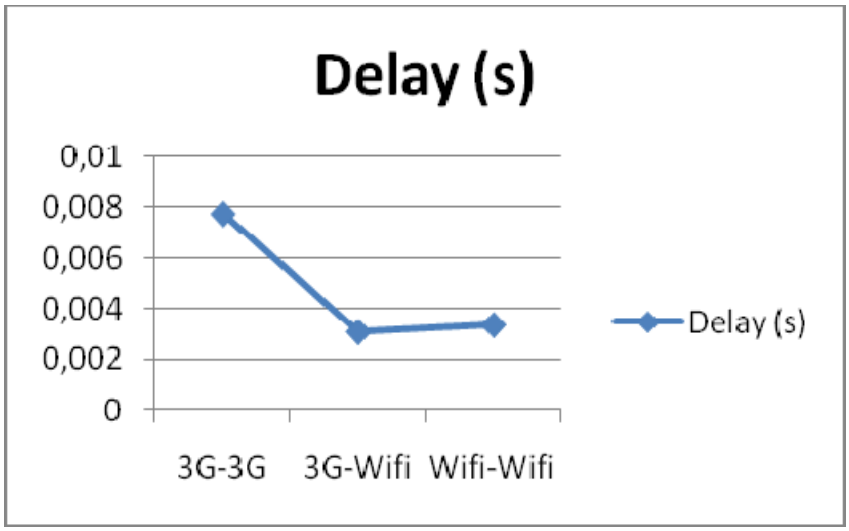
Untuk mengukur *delay* yang terjadi pada aplikasi telepon anti sadap yakni :

1. Melalui command prompt melalukan ping 192.168.88.6 yang merupakan ip salah satu *smartphone* saat ujicoba.
2. Melalui *software* wireshark muncul ICMP seperti pada Gambar 13.
3. Selanjutnya mengukur delay dengan mengambil *time since reference* pada ICMP *request* sebagai waktu paket dikirimkan dan *time since reference* pada ICMP *reply* sebagai waktu paket diterima. *Time since reference* dipelihatkan pada Gambar 14.
4. Kemudian melakukan perhitungan menggunakan persamaan

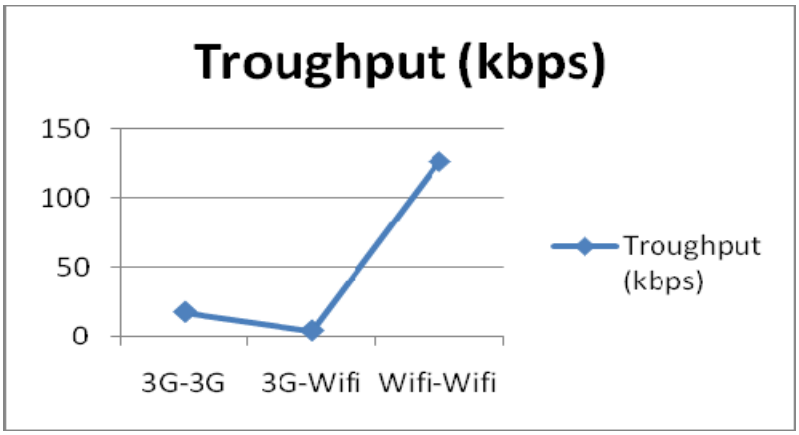
Delay = waktu paket diterima–waktu paket dikirim

5. Untuk mengukur waktu delay paket pada pengunaaan jaringan wifi-3G serta 3G-3G juga dengan menggunakan langkah yang sama.
6. Sehingga dari langkah-langkah pengukuran tersebut didapatkan hasil pada Tabel 2.

Dari Tabel 2 menjelaskan koneksi aplikasi menggunakan 3G-3G memiliki *delay* yang cukup besar sedangkan dari 3G-W*ifi* dan *Wifi-Wifi* hampir memiliki waktu *delay* yang sama yakni dengan beda *delay* 0,000276 *seconds*. Sehingga dapat diperlihatkan seperti pada grafik Gambar 15.



Gambar 15. Grafik *Delay*



Gambar 16. Grafik *Troughput*

Troughput

Untuk mengukur *troughput* yang terjadi pada aplikasi telepon anti sadap yakni dengan meng*capture* paket data dengan *wireshark* saat komunikasi terjadi kemudian membuka *statistics* → *summary* seperti diperlihatkan pada Gambar 16. Dari hasil *capture* tersebut kemudian mengambil nilai *avg.Mbit/sec*. atau dapat menggunakan persamaan

Troughput = jumlah data yang dikirim / waktu pengiriman

Dimana :

Average Byte/sec = jumlah data

Time between first & last packet (sec) = waktu

Untuk penggukuran *troughput* pada penggunaan jaringan 3G-3G, wifi-3G dan wifi-wifi menggunakan langkah yang sama sehingga didapatkan hasil pengukuran pada Tabel 3.

Tabel 3. Troughput

Koneksi	Jumlah data (Byte/s)	Waktu (s)	Troughput (kbps)
3G-3G	596,554	34,57	17,526
3G-Wifi	706,104	164,217	4,2998
Wifi-Wifi	1276,509	10,074	126,173

Tabel 3 memperlihatkan bahwa kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data yang terjadi pada aplikasi telepon anti sadap paling cepat yakni melalui *wifi-wifi* dengan *troughput* 126,173 kbps seperti diperlihatkan pada grafik Gambar 16.

Grafik pada Gambar 16 memperlihatkan *troughput* paling besar pada jaringan *wifi*, ini membuktikan bahwa koneksi aplikasi telepon anti sadap menggunakan jaringan *wifi-wifi* dapat berjalan dengan baik, sehingga direkomendasikan bahwa agar komunikasi dapat berjalan dengan lancar tidak terdapat putus-putus atau *delay* minimal koneksi yang tepat yakni menggunakan jaringan *wifi-wifi* ketika menggunakan aplikasi telepon anti sadap.

PENUTUP

Berdasarkan implementasi dan pengujian aplikasi telepon anti sadap terhadap jaringan wifi dan 3G maka dapat disimpulkan bahwa aplikasi telepon anti sadap dapat berjalan dengan baik apabila aplikasi telepon anti sadap menggunakan koneksi jaringan di *smartphone* yakni 3G-*Wifi* dan *Wifi-Wifi*, sebab pada hasil pengujian dijelaskan koneksi jaringan menggunakan 3G-*Wifi* memiliki *delay* 0,003115 *seconds* serta memiliki *troughput* 4,2298 kbps, namun apabila koneksi pada aplikasi telepon anti sadap menggunakan *wifi-wifi* memiliki *delay* 0,003391 *seconds* dan *troughput* 126,173 kbps. *Troughput* yang dihasilkan oleh penggunaan jaringan *wifi-wifi* lebih besar karena kemampuan sebenarnya pada jaringan *wifi* lebih baik dalam mengirimkan data meskipun bandwith yang digunakan dalam penelitian ini besar namun *troughput* bersifat dinamis tergantung trafik yang terjadi. Sehingga komunikasi percakapan melalui aplikasi telepon anti sadap direkomendasikan menggunakan jaringan *wifi-3G* atau *wifi-wifi* agar komunikasi percakapan yang dilakukan selain aman juga dapat berjalan dengan baik.

Faktor lain yang mempengaruhi performa atau kinerja dari aplikasi telepon anti sadap agar dapat berjalan dengan baik. Peneliti merekomendasikan dieksplorasi pada penelitian selanjutnya.

DAFTAR PUSTAKA

Barker, E. Roback, J. Nechvatal, J. Foti, L. Bassham, M. Dworkin, and W. Burr, "*Report on the development of the Advanced Encryption Standard (AES)*," *J. Res. Natl. Inst. Stand. Technol.*, vol. 106, no. 3, pp. 511–577, 2001.

Coulibaly and Lian Hao Liu, "Security of Voip networks," presented at the Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, 2010, vol. 3, pp. V3–104.

Elbayoumy and S. J. Shepherd, "A Comprehensive Secure VoIP Solution.," *IJ Netw. Secur.*, vol. 5, no. 2, pp. 233–240, 2007.

Hendra, "*Analisis Perbandingan Kinerja Algoritma Twofish Dan Tea (Tiny Encryption Algorithm) Pada Data Suara*," *J. Ilm. Mat. Terap.*, vol. 7, no. 1, 2012.

Johnston, B. Rosen, H. Kaplan, J. D. Rosenberg S. A. Baset, and V. K. Gurbani "*The session initiation protocol (SIP): An evolutionary study,*" *J. Commun.*, vol. 7, no. 2, pp. 89–105, 2012.

Jaber, Supriyanto, S. Manickam, and S. Ramadass, "*Highly effective filtration and prevention framework for secure incoming VoIP calls,*" *Int. J. Control Autom.*, vol. 6, no. 3, pp. 95–102, 2013.

Setiawan, A. Fatchur Rochim, and R. R. Isnanto, "Voice over Internet Protocol (VoIP) Menggunakan Asterisk Sebagai Session Initiation Protocol (SIP) *Server*," Jurusan Teknik Elektro Fakultas Teknik Undip, 2011.

Wang and Y.-S. Liu, "*A dependable privacy protection for end-to-end VoIP via Elliptic-Curve Diffie-Hellman and dynamic key changes*," *J. Netw. Comput. Appl.*, vol. 34, no. 5, pp. 1545 – 1556, 2011.