PROTOTIPE PENGAMANAN DATA PADA APLIKASI LAPOR POLISI BERBASIS ANDROID DENGAN ALGORITMA BLOWFISH DAN ALGORITMA DIFFIE-HELLMAN

Dyas Yudi Priyanggodo
Program Studi Informatika
Fakultas Teknik Universitas Muhammadiyah Tangerang
Jl. Perintis Kemerdekaan 1/33 Cikokol Kota Tangerang
priyanggodo.15@gmail.com

Abbstract - On lately appeared a whole range of applications Android-based Police Report maintained by the Polres each region.The Police Report on the application of the data that is sent plain text.It is dangerous because it allows hackers or unauthorized persons can read or change information that report.To secure the data report on applications Android-based Police Report writer uses the concept of merging cryptographic algorithms Blowfish and key exchange method Diffie-Hellman for encryption of data transmitted at the time of report.Implementation of the Blowfish algorithm and Diffie-Hellman algorithms on Android-based applications use memory is nothing more than a memory allocation provided by the Android operating system.

Keyword : Cryptography, Blowfish, Diffie-Hellman, Android

I. PENDAHULUAN

Perkembangan teknologi informasi saat ini semakin pesat, dibuktikan dengan banyaknya macam-macam alat elektronik berteknologi tinggi. Salah satu teknologi informasi yang saat ini terus berkembang adalah *smartphone.* Saat ini pengguna *smartphone* di Indonesia terus meningkat. Sebuah lembaga riset menyebutkan bahwa Indonesia berada di peringkat keempat daftar pengguna *smartphone* terbesar di dunia setelah China, India, dan Amerika Serikat. Data tersebut dilansir oleh Steven Millward melalui web techinasia.com. Pengguna *smartphone* di Indonesia pada tahun 2016 mencapai 69.400.000 (id.techinasia.com, 2016).

Di sisi lain, akhir-akhir ini banyak kejadian-kejadian kriminal. Untuk mencegah kejadian kriminal tersebut, Polri meminta masyarakat ikut berperan aktif menjaga keamanan lingkungan sekitarnya dengan cara segera melaporkan hal-hal yang dianggap mencurigakan kepada Polisi. Diberbagai daerah juga bermunculan aplikasi-aplikasi Lapor Polisi yang dikelola secara independen di daerah masing masing. Aplikasi tersebut berfungsi untuk melaporkan tidak kriminal kepada polisi secara detail lengkap dengan peta kejadian sehingga polisi dapat dengan mudah menuju tempat kejadian (Haorrahman, 2016). Dalam menjalankan aplikasi Lapor Polisi tersebut memanfaatkan teknologi dalam bidang komunikasi yang dapat digunakan untuk mengirimkan data digital (transmisi data). Data digital tersebut berupa data laporan tindak kriminal yang bersifat *privacydata*. Untuk menjaga supaya data dapat sampai ke pihak Kepolisian,dibutuhkan suatu sistem pengamanan untuk mengamankan data laporan yang dikirimkan oleh pelapor pada saat data tersebut di transmisikan. Dari masalah tersebut melalui konsep penggabungan algoritma kriptografi Blowfish dengan algoritma penukaran kunci Diffie-Hellman diharapkan dapat berhasil mengamankan data saat diterapkan Lapor Polisi bebasis Android. Namun yang perlu diperhatikan pada saat proses development aplikasi berbasis Android adalah batasan-batasan yang tidak ditemukan pada aplikasi *server-side* yaitu terbatsnya alokasi memori. Untuk itu perlu juga diadakan

pengujian terhadap alokasi memori yang disediakan oleh sistem Operasi Android.

II. TINJAUAN PUSTAKA

A. Algoritma Blowfish

Blowfish adalah cipher blok 64-bit yang memiliki sebuah kunci yang panjangnya variabel. Algoritma blowfish terdiri dari dua bagian yaitu *key expansion* dan enkripsi data. Blok diagram enkripsi algoritma Blowfish dapat dilihat pada gambar 2.3. *Key expansion* mengkonversikan sebuah kunci sampai 448 bit ke dalam beberapa array subkey dengan total 4168 byte. Enkripsi data terdiri dari sebuah fungsi yang sederhana dengan iterasi 16 kali. Semua operasi, penjumlahan dan XOR pada word 32-bit. Blowfish menggunakan sejumlah subkey yang besar. Key ini harus dihitung awal sebelum enkripsi atau dekripsi.

B. Algoritma Diffie-Hellman

Algoritma Deffie Hellman pertama kali dikenalkan oleh peneliti universitas Stanford yaitu Whitfield Diffie dan Martin Hellman pada tahun 1975. Mereka memperkenalkan algoritma ini untuk memberi solusi atas pertukaran informasi secara rahasia. Dasar dari algoritma ini adalah matematika dasar dari aljabar eksponen dan aritmatika modulus. Jumlah pengguna yang ingin menggunakan pertukaran kunci menggunakan algoritma Diffie-Hellman ini tidak dibatasi. Hal ini hanya berlaku jika memenuhi 2 prinsip yang harus dilakukan yaitu:

1. Bilangan *p* dan *g* yang telah disetujui oleh semua anggota.
2. Setiap anggota harus melakukan pertukaran data yang diperlukan oleh anggota lainnya sehingga semua data dapat didapatkan secara merata $\mathbf{g^{abc….n}}$

Tingkat keamanan dari algoritma ini tinggi, jika nilai *p* dan *g* dipilih secara benar. Karena untuk mengetahui atau menebak nilai rahasia yang dimiliki oleh penerima dan pengirim harus menyelesaikan persamaan Diffie-Hellman terlebih dahulu. Ini merupakan masalah logaritma diskrit yang perhitungan tersebut tidak dapat diselesaikan untuk nilai bilangan *p* yang sangat besar. Menghitung logaritma diskrit dari bilangan modulo *p* memakan waktu yang kurang lebih sama seperti dengan memfaktorkan bilangan non prima menjadi faktor primanya, seperti yang digunakan di algoritma RSA. Oleh karena itu, algoritma ini tingkat keamanannya setingkat dengan dengan algoritma RSA.

C. Android

Android tersedia tersedia secara *open source* bagi manufaktur perangkat keras untuk memodifikasi sesuai kebutuhan. Meskipun konfigurasi perangkat Android tidak sama antara satu perangkat dengan perangkat lainnya. Yang perlu diperhatikan pada saat proses development aplikasi berbasis Android adalah batasan-batasan yang tidak ditemukan pada aplikasi *server-side*. Salah satunya adalah terbatasnya RAM (*Random Access Memory*) pada aplikasi yang sedang berjalan (Ihsannudin, 2016). Ketika aplikasi sedang melakukan alokasi RAM, tetapi perangkat tidak memiliki resource yang dapat diberikan, maka pesan eror out of memory akan muncul dan mengakibatkan berhentinya aplikasi yang sedang dijalankan (Ihsannudin, 2016).

D. Laporan

Definisi Laporan dapat kita lihat di dalam Pasal 1 angka 24 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ("KUHAP"), yaitu:

"Laporan adalah pemberitahuan yang disampaikan oleh seorang karena hak atau kewajiban berdasarkan undang-undang kepada pejabat yang berwenang tentang telah atau sedang atau diduga akan terjadinya peristiwa pidana".

Dari pengertian di atas, laporan merupakan suatu bentuk pemberitahuan kepada pejabat yang berwenang bahwa telah ada atau sedang atau diduga akan terjadinya sebuah peristiwa pidana/kejahatan. Artinya, peristiwa yang dilaporkan belum tentu perbuatan pidana, sehingga dibutuhkan sebuah tindakan penyelidikan oleh pejabat yang berwenang terlebih dahulu untuk menentukan perbuatan tersebut merupakan tindak pidana atau bukan. Kita sebagai orang yang melihat suatu tidak

kejahatan memiliki kewajiban untuk melaporkan tindakan tersebut.

E. Tempat Melapor

Dalam hal ini tempat untuk melapor polisi adalah kantor kepolisian terdekat pada lokasi peristiwa pidana tersebur terjadi. Adapun daerah hukum kepolisian sesuai Pasal 4 ayat [1] Peraturan Pemerintah Nomor 23 Tahun 2007 tentang Daerah Hukum Kepolisian Negara Republik Indonesia – PP 23/2007 meliputi :

1. Daerah hukum kepolisian Markas Besar (MABES) POLRI untuk wilayah Negara Kesatuan Republik Indonesia;
2. Daerah hukum kepolisian Daerah (POLDA) untuk wilayah Provinsi;
3. Daerah hukum kepolisian Resort (POLRES) untuk wilayah Kabupaten/kota;
4. Daerah hukum kepolisian Sektor (POLSEK) untuk wilayah kecamatan.

Untuk wilayah administrasi kepolisian, daerah hukumnya dibagi berdasarkan pemerintahan daerah dan perangkat sistem peradilan pidana terpadu (Pasal 2 ayat [2] PP 23/2007). Sebagai contoh jika Anda melihat ada tindak pidana di suatu kecamatan, maka pelapor dapat melaporkan hal tersebut ke Kepolisian tingkat Sektor (POLSEK) di mana tindak pidana itu terjadi. Akan tetapi, pelapor juga dibenarkan/dibolehkan untuk melaporkan hal tersebut ke wilayah administrasi yang berada di atasnya misal melapor ke POLRES, POLDA atau MABES POLRI.

Pada saat pelapor berada di Kantor Polisi, pelapor menuju ke bagian SPKT (Sentra Pelayanan Kepolisian Terpadu) yang merupakan unsur pelaksana tugas pokok di bidang pelayanan kepolisian. SPKT memiliki tugas memberikan pelayanan terhadap laporan/pengaduan masyarakat. Hal ini sebagaimana ketentuan Pasal 106 ayat (2) Peraturan Kepala Kepolisian Negara Republik Indonesia No. 23 Tahun 2010 tentang Susunan Organisasi dan Tata Kerja Pada Tingkat Kepolisian Resor dan Kepolisian Sektor, yang berbunyi.

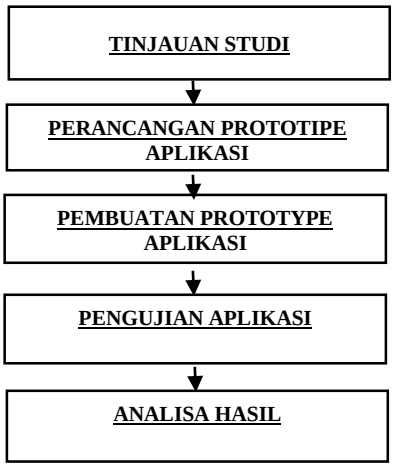
SPKT bertugas memberikan pelayanan kepolisian secara terpadu terhadap laporan/pengaduan masyarakat, memberikan bantuan dan pertolongan, serta memberikan pelayanan informasi

III. METODOLOGI PENELITIAN

Dalam penelitian ini digunakan metode studi pustaka yang dilakukan dengan cara mengumpulkan literatur dan referensi yang berhubungan dengan algoritma kriptografi Blowfish dan metode penukaran kunci Diffie Helman. Selain itu peneliti juga mengumpulkan literature dan referensi yang berhubungan dengan pengembangan aplikasi Android. Referensi atau data-data yang telah terkumpul disortir sesuai dengan bidang pembahasan mengenai algoritma kriptografi Blowfish serta metode penukaran kunci Diffie Hellman yang akan digunakan untuk mengenkripsi data laporan dalam aplikasi Lapor Polisi pada saat proses pengiriman data.

Dalam proses pengamanan data hal pertama yang dilakukan adalah menerapkan algoritma penukaran kunci Diffie-Hellman untuk menentukan kunci yang dipakai algoritma Blowfish dalam me-enkripsi data. Dalam proses penukaran kunci, mula-mula sistem menentukan dua bilangan prima yang disepakati oleh aplikasi pelapor, penerima laporan dan server. Selanjutnya masing-masing meng-*generate* secara acak bilangan bulat. Bilangan hasil *generate* merupakan bilangan yang rahasia, dan tidak akan dikirim dalam transmisi data. Setelah itu antara dua bilangan yang disepakati dan satu bilangan hasil *generate* acak diproses menggunakan algoritma Diffie Hellman. Maka akan menghasilkan bilangan bulat yang selanjutnya akan dikirimkan kepada lawan komunikasi dalam. Selanjutnya setelah menerima bilangan dari lawan komunikasi, masing-masing aplikasi melanjutkan proses lagi untuk menentukan kunci yang dipakai untuk meenkripsi dan mendeskripsi pesan menggunakan algoritma kriptografi Blowfish.

Dalam pembuatan aplikasi Lapor Polisi ini keseluruhan proses harus melalui beberapa tahapan. Langkah-langkah pada tahapan penelitian adalah sebagai berikut:

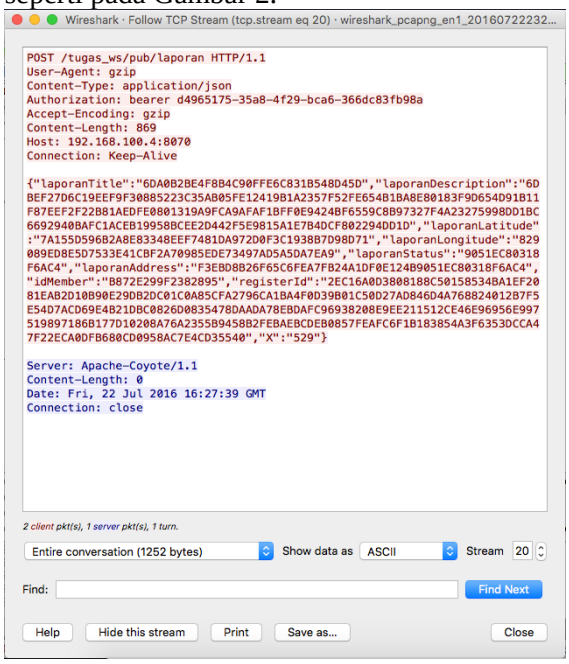


Gambar 1 Langkah-langkah Penelitian

IV. HASIL DAN PEMBAHASAN

A. Pengujian Keamanan Data

Pengujian keamanan data pada saat transmisi dilakukan menggunakan aplikasi Wireshark yang berjalan pada komputer. Dengan melakukan penelusuran pada paket data dari aplikasi lapor polisi maka didapatkan seperti pada Gambar 2.



Gambar 2. Penelusuran Paket Data Laporan

Selanjutnya tahap pengujian ini dilakukan pengujian terhadap keamanan data setelah dienkripsi. Pengujian dilakukan menggunakan metode Brute Force Attack untuk mendapatkan kunci yang dihasilkan oleh algoritma Diffie-Hellman yang selanjutnya digunakan untuk proses enkripsi menggunakan algoritma Blowfish. Selain itu pengujian juga membandingkan antara waktu proses Brute Force Attact menemukan kunci dengan waktu tempuh Polisi menuju ke tempat kejadian. Untuk menentukan waktu Brute Force Attact menemukan kinci menggunakan *tool* "Brute Force Calculator" yang terdapat pada website http://calc.opensecurityresearch.com/.

Percobaan waktu jarak tempuh dilakukan dengan cara melakukan simulasi pelaporan secara acak pada lima tempat berbeda di daerah Kota Bekasi. Selanjutnya menghitung jarak tempuh Polsek yang menerima dengan tempat kejadian dan menentukan waktu tempuh yang diperlukan untuk menuju ke tempat kejadian. Data hasil percobaan dapat dilihat pada Tabel 1.

Tabel. 1 Tabel Hasil Pengujian Brute Force

No	Panjang Kunci	Waktu yang dibutuhkan Brute Force *	Jarak Polsek - Lokasi Kejadian	Waktu Tempuh Polsek - Lokasi Kejadian **
1	7	3 jam 32 menit 51 detik	8,6 KM	28 Menit
2	8	1 hari 11 jam 28 menit 33 detik	2,6 KM	9 Menit
3	7	3 jam 32 menit 51 detik	5,6 KM	17 Menit
4	8	1 hari 11 jam 28 menit 33 detik	5,8 KM	20 Menit
5	8	1 hari 11 jam 28 m	6,2 Km	16 Menit

	enit 33 d etik

* *Key per second* berdasarkan OpenBSD Blowfish (870 k/s) dan *charset numeric*.
** Diasumsikan bahwa pihak Polisi langsung menanggapi laporan dengan langsung menuju ke tempat kejasdian.

Dari tabel 1 dapat dilihat bahwa *attacker* membutuhkan waktu 3 jam 32 menit 51 detik untuk dapat menemukan kunci yang digunakan untuk enkripsi dengan panjang 7 digit dan 1 hari 11 jam 28 menit 33 detik untuk dapat menemukan kunci yang digunakan untuk enkripsi dengan panjang 8 digit. Pada percobaan penghitungan waktu mendapatkan *private key*, kecepatan uji coba per kunci berdasarkan OpenBSD Blowfish dengan kecepatan 870 k/s untuk setiap kunci. OpenBSD Blowfish adalah metode *hashing* yang menggunakan algoritma Blowfish dan diterapkan pada sistem operasi *open source* dari Berkeley Software Distribution(BSD).

Carset numeric menyatakan bahwa *pivate key* tersusun atas angka saja. Sedangkan waktu yang dibutuhkan untuk Polisi menuju ke tempat kejadian setalah mendapatkan laporan didapatkan rata-rata 18 menit dengan waktu paling lama 28 menit dan waktu paling singkat 9 menit. Setelah Polisi sampai ke tempat kejadian maka data laporan tersebut dapat dinyatakan tidak perlu dirahasiakan lagi.
Dari Tabel 1 didapatkan fakta percobaan bahwa waktu yang dibutuhkan untuk mendapatkan *private key* lebih lama dibandingkan waktu tempuh Polisi ke tempat kejadian. Dari hasil tersebut maka dinyatakan bahwa enkripsi data menggunakan algoritma kriptografi Blowfish dengan metode penukaran kunci Diffie-Hellman dinyatakan aman.

Algoritma kriptografi dikatakan aman apabila usaha untuk membongkar kunci rahasia tersebut memerlukan waktu yang sangat lama, sehingga usaha pembongkaran tersebut baru akan berhasil setelah pesan sudah tidak berlaku lagi (Prasetya, 2011).

B. Pengujian Terhadap Alokasi Memori

Pada pengujian ini dilakukan beberapa percobaan untuk membandingkan pemakaian memori yang digunakan untuk membentuk kunci menggunakan algoritma Diffie-Hellman dan enkripsi maupun dekripsi data menggunakan algoritma Blowfish dengan alokasi memori yang disediakan. Percobaan ini bertujuan untuk mengetahui apakah proses yang dijalankan masih dapat dilakukan dengan alokasi memori yang disediakan. Percobaan dilakukan dengan menggunakan beberapa smartphone dengan spesifikasi ram berbeda yang beredar dipasaran. Hasil percobaan dapat dilihat pada Table 2.

Tabel 2. Hasil Pengujian Aplikasi Terhadap Alokasi Memori

No	RAM	Alokasi Memori	Memori Aplikasi	Penggunaan Memori Saat Enkripsi
1	512 MB	11.49 MB	5.00 MB	6.13 MB
2	1 GB	11.51 MB	5.05 MB	5.09 MB
3	2 GB	11.49 MB	5.00 MB	6.12 MB
4	4 GB	11.50 MB	5.02 MB	6.11 MB
Rata-rata		11.4975 MB	5.02 MB	5.86 MB

Dari Tabel 2 didapatkan data bahwa aplikasi Lapor Polisi disediakan alokasi memori sebesar 11.4975 MB dengan penggunaannya sebesar 10.88 MB. 10.88 MB tersebut terdiri dari 5.0175 MB penggunaan memori sebelum melakukan enkripsi dan 5.8625 MB penggunaan memori saat enkripsi.

Dari data tersebut dapat diambil kesimpulan bahwa proses pengamanan data dengan menggunakan algoritma kriptografi Blowfish dan metode penukaran kunci Diffie-Hellman dapat diterapkan pada aplikasi Lapor Polisi berbasis android dengan tidak melebihi alokasi memori yang disediakan.

V. KESIMPULAN

Penerapan konsep algoritma kriptografi Blowfish dengan metode penukaran kunci Diffie-Hellman berhasil dierapkan pada aplikasi Lapor Polisi berbasis Android dengan tidak

melebihi alokasi memori yang disediakan. Pada aplikasi Lapor Polisi Berbasis Android disediakan alokasi memori sebesar 11.4975 MB dengan penggunaannya sebesar 10.88 MB. 10.88 MB tersebut terdiri dari 5.0175 MB penggunaan memori sebelum melakukan enkripsi dan 5.8625 MB penggunaan memori saat enkripsi.

Kekuatan dari konsep tersebut adalah menghasilkan enkripsi *end-to-end* hanya aplikasi Lapor Polisi yang mengirimkan laporan dan aplikasi penerima laporan yang dituju yang dapat mendeskripsikan data. Penggunaan algoritma kriptografi Blowfish dengan metode penukaran kunci Diffie-Hellman dinyatakan aman karena waktu yang dibutuhkan untuk *hacker* menemukan *private key* lebih lama dibandingkan waktu yang dibutuhkan Polisi untuk sampai ke tempat kejadian. Hal tersebut didasarkan dengan percobaan dengan metode Brute Froce Attact untuk menemukan *private key*.

Hasil Percobaan tersebut didapatkan waktu menemukan *private key* 3 jam 32 menit 51 detik untuk dapat menemukan *private key* yang digunakan untuk enkripsi dengan panjang 7 digit dan 1 hari 11 jam 28 menit 33 detik untuk dapat menemukan *private key* yang digunakan untuk enkripsi dengan panjang 8 digit. Sedangkan waktu yang dibutuhkan untuk Polisi menuju ke tempat kejadian setalah mendapatkan laporan didapatkan rata-rata 18 menit dengan waktu paling lama 28 menit dan waktu paling singkat 9 menit.

REFERENSI

[1]Amriel, R.I. (2015). PNomor Darurat 110 dan Kepercayaan Publik. http://kriminalitas.com/nomor-darurat-110-dan-kepercayaan-publik/.

[2]Canavan, John E. (2001). Fundamentals of Network Security. London: Artech House.

[3]Chechik, D. (2013). Look What I Found: Moar Pony!. https://www.trustwave.com/Resources/SpiderLabs-Blog/Look-What-I-Found---Moar-Pony!/.

[4]Gunawan, M. I. (2013). Penggunaan Algoritma Diffie-Hellman dalam Melakukan Pertukaran Kunci.

[5]Hendarsyah, D. (2011). Implementasi Protokol Diffie-Hellman Dan Algoritma RC4 Untuk Keamanan Pesan SMS, *5*(1), 14–25.

[6]Jeske, T. (2012). Floating Car Data from Smartphones: What Google and Waze Know About You and How Hackers Can Control Traffic. *Media.Blackhat.Com*, 12. Retrieved from https://media.blackhat.com/eu-13/briefings/Jeske/bh-eu-13-floating-car-data-jeske-wp.pdf

[7]Kasim, A. A. (2010). Implementasi Kriptosistem Kurva Eliptik Dengan Pertukaran Kunci Diffie-Hellman Pada Data Audio Digital. *Jimt*, *7*(2), 35–42. Retrieved from http://jurnal.untad.ac.id/jurnal/index.php/JIMT/article/view/135

[8]Kautzar, M. G. (2009). Pesan Instan Java Dengan Algoritma Blowfish. *Program*.

[9]Kusuma, I. W., & Adi, P. S. (2012). SISTEM OTENTIKASI SINGLE SIGN-ON MENGGUNAKAN ALGORITMA DIFFIE-HELLMAN DAN MENGGUNAKAN DATABASE PARALLEL DENGAN MENGGUNAKAN RMI (REMOTE METHOD INVOCATION), *2012*(Semantik), 336–342.

[10]Permana, A. D., & St, S. (2013). Pengamanan Sistem Login Aplikasi Menggunakan Protokol ID Based Diffie-Hellman Key Agreement, (70), 9–13.

[11]Pressman, R. S. (1994). *Software Engineering*. http://doi.org/10.1036/0071406204

[12]Schneier, B.(1995).The Blowfish Encription Algorithm. Dr. Dobb 's Journal.

[13]Sitinjak, S., & Fauziah, Y. (2010). Aplikasi Kriptografi File Menggunakan Blowfish, *2010*(semnasIF), 78–86.

[14]Stiawan, A. F. K. and R. (2002). PERANGKAT LUNAK UNTUK PROSES ENKRIPSI DESKRIPSI MESSAGE EMAIL DENGAN ALGORITMA BLOWFISH STIKOM.

[15]Wahyuni, A. (2011). Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid :Diffie-Hellman dan RSA, 15–23.

[16]Wardoyo, S., Imanullah, Z., & Fahrizal, R. (2016). ENKRIPSI DAN DEKRIPSI FILE DENGAN ALGORITMA BLOWFISH PADA PERANGKAT MOBILE BERBASIS ANDROID, (1).

[7]Yuliana, C. T. E. (2005). Implementasi Algoritma Kriptografi Blowfish dan Metode Steganografi End Of File (EOF) untuk Keamanan Data. *Journal of Chemical Information and Modeling*, *53*, 160. http://doi.org/10.1017/CBO9781107415324.004