ISSN 2303 - 1425

J-INTECH

Journal of Information and Technology

Volume 05 Nomor 01, Juni Tahun 2017

STIKI

SEKOLAH TINGGI INFORMATIKA & KOMPUTER INDONESIA
Jl. Raya Tidar 100 Malang, 65146
Telp. (0341)560823, Fax (0341)562525

J-INTECH

Volume 05 Nomor 01, Juni Tahun 2017

ISSN 2303 - 1425

J-INTECH

Journal of Information and Technology

Volume 05 Nomor 01, Juni Tahun 2017

LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT

STIKI

SEKOLAH TINGGI INFORMATIKA & KOMPUTER INDONESIA

Jl. Raya Tidar 100, Malang; Phone: 0341-560823; Fax: 0341-562525; http://www.stiki.ac.id; mail@stiki.ac.id

PENGANTAR REDAKSI

J-INTECH merupakan jurnal yang diterbitkan oleh Sekolah Tinggi Informatika dan Komputer Indonesia Malang guna mengakomodasi kebutuhan akan perkembangan Teknologi Informasi serta guna mensukseskan salah satu program DIKTI yang mewajibkan seluruh Perguruan Tinggi untuk menerbitkan dan mengunggah karya ilmiah mahasiswanya dalam bentuk terbitan maupun jurnal online.

Pada edisi ini, redaksi menampilkan beberapa karya ilmiah mahasiswa yang mewakili beberapa mahasiswa yang lain, yang dianggap cukup baik sebagai media pembelajaran bagi para lulusan selanjutnya.

Tentu saja diharapkan pada setiap penerbitan memiliki nilai lebih dari karya ilmiah yang dihasilkan sebelumya sehingga merupakan nilai tambah bagi para adik kelas maupun pihak-pihak yang ingin studi atau memanfaatkan karya tersebut selanjutnya.

Pada kesempatan ini kami juga mengundang pihak-pihak dari PTN/PTS lain sebagai kontributor karya ilmiah terhadap jurnal J-INTECH, sehingga Perkembangan IPTEK dapat dikuasai secara bersama- sama dan membawa manfaat bagi institusi masing-masing.

Akhir redaksi berharap semoga dengan terbitnya jurnal ini membawa manfaat bagi para mahasiswa, dosen pembimbing, pihak yang bekerja pada bidang Teknologi Informasi serta untuk perkembangan IPTEK di masa depan.

REDAKSI

ISSN 2303 - 1425
J-INTECH
Journal of Information and Technology
Volume 05 Nomor 01, Juni Tahun 2017

DAFTAR ISI

ISSN 2303 - 1425

J-INTECH

Journal of Information and Technology

Volume 05 Nomor 01, Juni Tahun 2017

Implementasi Algoritma Kriptografi Elgamal pada Data Text

Binantara Parmadi
Program Studi Teknik Informatika Sekolah Tinggi Informatika & Komputer Indonesia STIKI Malang
Email: chrysoberyl_burgundy@yahoo.com

ABSTRAK

Keamanan data merupakan syarat wajib yang harus diterapkan seseorang ataupun kelompok dalam menjaga privasinya. Karena tidak sedikit pihak yang tidak berwenang mencuri data tersebut yang seharusnya menjadi privasi digunakan untuk kepentingan pribadi maupun kepentingan tertentu. Implementasi keamanan data adalah salah satu cara efektif dalam mengamankan data demi menjaga privasi tersebut. Dengan melakukan implementasi algoritma Elgamal sebagai keamanan pada data, pihak yang tidak berwenang diharapkan tidak dapat dengan mudah mengetahui isi data yang telah diamankan.

Kata kunci: *Elgamal, keamanan, data, delphi.*

1. PENDAHULUAN

Untuk menjaga keamanan yang mempunyai informasi-informasi rahasia penting, maka digunakanlah salah satu teknik pengaman informasi dengan menggunakan algoritma penyandian data. Pada sistem ini akan menggunakan algoritma penyandian data/kriptografi ElGamal yang akan diimplementasikan pada sebuah aplikasi. Menurut jurnal *A Public Key Cryptosystem and a SignatureScheme Based on Discrete Logarithms* menyebutkan bahwa kekuatan Algoritma Kriptografi Elgamal terletak pada kalkulasi tanda tangan digital yang menekankan pada perhitungan algoritma diskrit sehingga tanda tangan digital atau kunci rahasia tersebut tidak dapat di kriptalis.

2. ANALISA DAN PERANCANGAN

a. Analisa Masalah

Permasalahan

Untuk menjaga keamanan yang mempunyai informasi-informasi rahasia penting, maka digunakanlah salah satu teknik pengaman informasi dengan menggunakan algoritma penyandian data. Pada sistem ini akan menggunakan algoritma penyandian data/kriptografi ElGamal yang akan diimplementasikan pada Aplikasi Client untuk mengenkripsi sebuah data text.

Identifikasi Masalah

1. Dibutuhkah sebuah enkripsi yang kuat agar tidak dapat dikriptalis.
2. Bagaimana membangkitkan bilangan acak (prima dan tidak prima) untuk menjadi kunci dalam sistem kriptografi?

Solusi Pemecahan

Dari penelitian ini dihasilkan sebuah program aplikasi enkripsi dan dekripsi elgamal yang dibangun menggunakan Delphi. Aplikasi ini dapat digunakan oleh user secara umum. User hanya diberi batasan file bebentuk txt dan ektensi khusus yang dibuat penulis. Hasil dari penelitian akan menghasilkan sebuah program aplikasi yang:

1. Dapat mengubah file atau text asli menjadi file yang terenkrikpsi di mana isi file tidak dapat dibaca.
2. Dapat mengembalikan file atau text yang tidak bisa dibaca menjadi file aslinya dengan metode elgamal tanpa merusak dan merubah isi file tersebut.
3. Dapat mengubah pesan asli berupa plaintext menjadi chipertext yaitu berupa kode-kode yang tidak bisa terbaca.

Analisa Kebutuhan Input

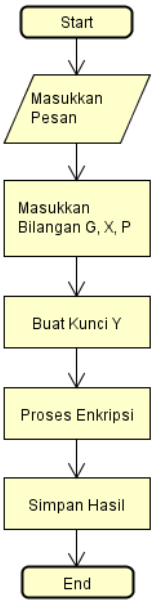
Kebutuhan input pada aplikasi ini adalah:

1. Input untuk memasukkan bilang G, X dan P.
2. Input untuk menuliskan pesan.
3. Tombol Enkripsi dan Deskripsi.
4. Tombol untuk membuka file yang akan dienkripsi atau file yang telah dienkripsi.
5. Tombol untuk menyimpan file hasil enkripsi.

3. PERANCANGAN DAN IMPLEMENTASI

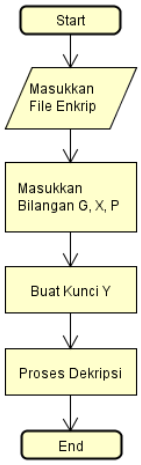
a. Perancangan

Flowchart Enkripsi



Gambar 1. Flowchart Enkripsi

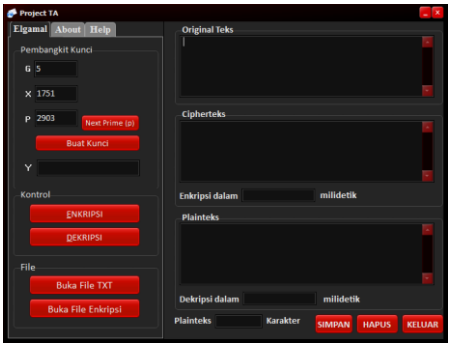
Flowchart Enkripsi



Gambar 2. Flowchart Enkripsi

b. Implementasi

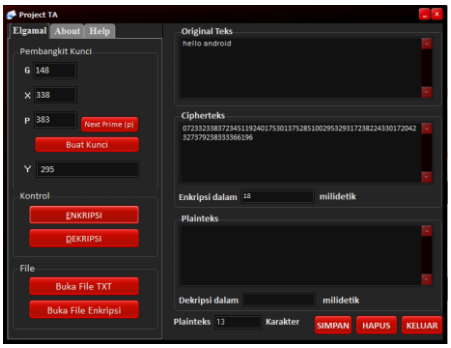
Implementasi merupakan salah satu proses penting yang harus dijelaskan dalam sebuah perancangan project. Pada perancangan kali ini, akan dijelaskan beberapan tahapan implementasi. Berikut adalah desain keseluruhan:



Gambar 3. Form Utama

Gambar 4. Tombol Pembangkit Bilangan Prima (Next Prime)

Gambar 5. Tombol Pembuat Kunci



Gambar 6. Tombol Enkripsi

Contoh kasus dekripsi:
Pesan (plaintext): hello android
Nilai (p,g,y,x): (383, 148, 295, 338)
Nilai k: k1 = 319, k2= 259, k3 = 353, k4 = 105, k5 = 267, k6= 279,k7 = 190, k8 = 252, k9 = 60, k10 = 87, k11 = 360, k12 =139,k13 = 48

Proses Pembentukan Kunci:
Misalkan penulis memilih $p = 2903, g = 5$, dan $x = 1751$. Kemudian menghitung: $y = g^x \bmod p = 5^{1751} \bmod 2903 = 771$

Diperoleh kunci publik $(y, g, p) = (771, 5, 2903)$ dan kunci privatnya $x = 1751$. Kunci publik $(771, 5, 2903)$ inilah yang diberikan penerima kepada pemberi pesan. Kunci rahasia tetap dipegang oleh penerima dan tidak boleh ada yang mengetahui selain dirinya sendiri.

Proses Enkripsi:
Langkah-langkah penyelesaian proses enkripsi secara manual adalah sebagai berikut:
Diketahui:
Plaintext: "hello android"
Nilai $p = 383, g = 148$ dan $y = 295$.

Nilai $k1 = 319, k2 = 259, k3 = 353, k4 = 105, k5 = 267, k6 = 279, k7 = 190, k8 = 252, k9 = 60, k10 = 87, k11 = 360, k12 = 139, k13 = 48$

Penyelesaian:
Ubah pesan asli (plaintext) ke dalam ASCII h=104, e=101, l=108, l=108, o=111, spasi=32, a=97, n=110, d=100, r=114, o=111, i=105, d=100
sehingga nilai pesan ASCII adalah sebagai berikut:
m1=104, m2=101, m3=108, m4=108, m5=111, m6=32, m7=97, m8=110, m9=100, m10=114, m11=111, m12=105, m13=100

Hitung gamma (γ) dengan rumus $\gamma = g^k \bmod p$
$\gamma 1 = 148^{319} \bmod 383$
$\gamma 2 = 148^{259} \bmod 383$
$\gamma 3 = 148^{353} \bmod 383$
$\gamma 4 = 148^{105} \bmod 383$
$\gamma 5 = 148^{267} \bmod 383$
$\gamma 6 = 148^{279} \bmod 383$

Sehingga Hasilnya:
γ1 = 197 γ8 = 31
γ2 = 122 γ9 = 168
γ3 = 85 γ10 = 37
γ4 = 379 γ11 = 38
γ5 = 340 γ12 = 356
γ6 = 269 γ13 = 144
γ7 = 339

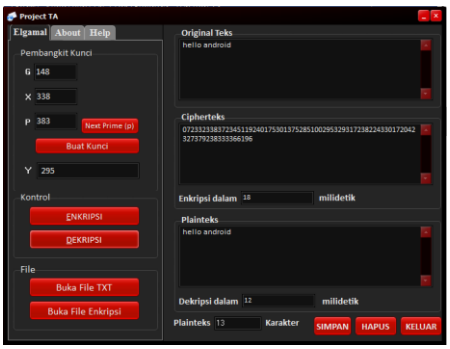
Hitung delta dengan rumus $\delta = y^k .m \bmod p$
$\delta 1 = 295^{319} .104 \bmod 383 = 158$
$\delta 2 = 295^{259} .101 \bmod 383 = 2$
$\delta 3 = 295^{353} .108 \bmod 383 = 300$
$\delta 4 = 295^{105} .108 \bmod 383 = 336$

Hasilnya:
δ1 = 158 δ7 = 99
δ2 = 2 δ8 = 153
δ3 = 300 δ9 = 292
δ4 = 336 δ10 = 113
δ5 = 250 δ11 = 367
δ6 = 98 δ12 = 345
δ13 = 8

Susun hasil perhitungan gamma (γ) dan delta (δ)
Ciphertext: 197, 158, 122, 2, 85, 300, 379, 336, 340, 250, 269, 98, 339, 99, 31, 153, 168, 292, 37, 113, 38, 367, 356, 345, 144, 8

Tabel 1. Hasil Perhitungan Chiperteks

i	m_i	k_i	$\gamma = 148^k \bmod 383$	$\delta = 295^k .m \bmod 383$
1	104	319	197	158
2	101	259	122	2
3	108	353	85	300
4	108	105	379	336
5	111	267	340	250
6	32	279	269	98
7	97	190	339	99
8	110	152	31	153
9	100	60	168	292
10	114	87	37	113
11	111	360	38	367
12	105	139	356	345
13	100	48	144	8



Gambar 7. Tombol Dekripsi

Proses dekripsi:
Langkah-langkah penyelesaian proses dekripsi secara manual adalah sebagai berikut:
Diketahui:
Ciphertext : 197, 158, 122, 2, 85, 300, 379, 336, 340, 250, 269, 98, 339, 99, 31, 153, 168, 292, 37, 113, 38, 367, 356, 345, 144, 8
Nilai p = 383, x = 338.

Penyelesaian:
Pisahkan nilai gamma dan delta pada pesan rahasia (ciphertext).

γ = Ciphertext urutan ganjil.
δ = Ciphertext urutan genap.
Nilai gamma γ1 = 197, γ2 = 122, γ3 = 85, γ4 = 379, γ5 = 340, γ6 = 269, γ7 = 339, γ8 = 31, γ9 = 168, γ10 = 37, γ11 = 38, γ12 = 356, γ13 = 144

Nilai delta δ1 = 158, δ2 = 2, δ3 = 300, δ4 = 336, δ5 = 250, δ6 = 98, δ7 = 99, δ8 = 153, δ9 = 292, δ10 = 113, δ11 = 367, δ12 = 345, δ13 = 8

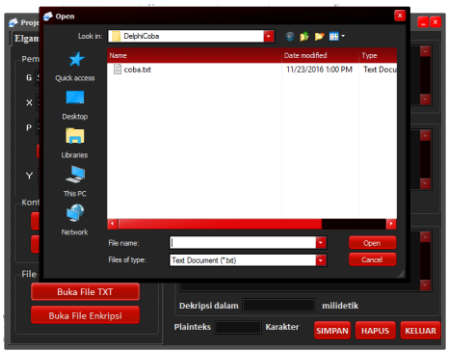
Pisahkan nilai gamma dan delta pada pesan rahasia (ciphertext).
Hitung m (pesan asli) dengan rumus:
$m = \delta . \gamma^{(p-1-x)} \bmod p$
$m1 = 158.197^{(383-1-338)} \bmod 383 = 104$
$m2 = 2.122^{(383-1-338)} \bmod 383 = 101$
$m3 = 300.85^{(383-1-338)} \bmod 383 = 108$
$m4 = 336.379^{(383-1-338)} \bmod 383 = 108$

sehingga hasilnya sebagai berikut:
m1 = 104, m2 = 101, m3 =108, m4 = 108 , m5 = 111, m6 = 32, m7 = 97, m8 = 110, m9 = 100, m10 = 114, m11 = 111, m12 = 105, m13 = 100

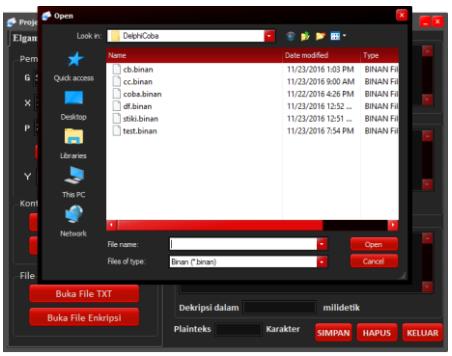
Hasil dari penyusunan inilah yang merupakan pesan asli (plaintext) yang dihasilkan pada proses dekripsi. plaintext: "hello android". Hasil proses perhitungan enkripsi dekripsi dengan program aplikasi dan secara manual adalah sama. Selain itu plaintext setelah dekripsi sama dengan nilai plaintext sebelum di enkripsi.

Tabel 2. Hasil Dekripsi

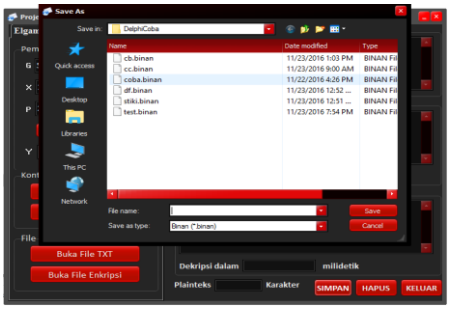
i	δ	γ	$m_i = \delta_i . \gamma_i^{(383-1-338)} \bmod 383$	Karakter m_i
1	158	197	104	h
2	2	122	101	e
3	300	85	108	l
4	336	379	108	l
5	250	340	111	o
6	98	269	32	<spaci>
7	99	339	97	a
8	153	31	110	n
9	292	168	100	d
10	113	37	114	r
11	367	38	111	i
12	345	356	105	o
13	8	144	100	d



Gambar 8. Tombol Buka File TXT



Gambar 9. Tombol Buka File Enkripsi



Gambar 10. Tombol Buka File Enkripsi

4. KESIMPULAN

a. Kesimpulan

Setelah melakukan analisis, perancangan, implementasi beserta pengujian yang telah dilakukan, maka dapat diperoleh kesimpulan sebagai berikut:

1. Algoritma asimetris memiliki kunci enkripsi yang berbeda dengan kunci dekripsi. Kunci untuk enkripsi disebut kunci publik dan kunci untuk dekripsi disebut kunci rahasia.
2. Algoritma ElGamal merupakan salah satu algoritma asimetris dalam kriptografi. Algoritma ini memiliki kunci publik yang terdiri atas 3 bilangan dan kunci rahasia yang terdiri atas sebuah bilangan.
3. Tingkat keamanan algoritma ini didasarkan pada kesulitan pemecahan masalah logaritma diskret pada penggandaan bilangan bulat modula prima yang besar.
4. Cipherteks yang dihasilkan dari plainteks dengan menggunakan algoritma ElGamal dapat berbeda-beda karena adanya penggunaan bilangan acak pada pengenkripsian plainteks. Akan tetapi, ketika didekripsikan, plainteks yang dihasilkan sama.

5. Penggunaan blok-blok cipherteks pada algoritma ElGamal menyebabkan panjang cipherteks menjadi dua kali panjang dari plainteks

b. Saran

Berikut merupakan beberapa saran untuk pengembangan di masa yang akan datang, berdasar pada hasil perancangan, implementasi, dan uji coba yang telah dilakukan.:

1. Menambah karakter Unicode sehingga range kunci x juga bertambah besar, dan menambah keamanan kriptografi ElGamal.
2. Menyempurnakan algoritma Enkripsi dalam kasus mengenali "\n" sebagai spasi.
3. Pembuatan antarmuka aplikasi berupa aplikasi Web Service, sehingga aplikasi ini bisa diakses dari berbagai macam platform.

5. REFERENSI

[1] ElGamal, Taher. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.

[2] Hegelson, Melissa. (2011). Security and Applications of ElGamal's Encryption Algorithm.

[3] Jacobsson, Markus. (2010). Security of Signed ElGamal Encryption.

[4] Mousa, Allam. (2005). Security and Performance of EIGamal Encryption Parameters.