

# Perancangan Aplikasi Penyandian Agenda Pribadi Menggunakan Algoritma Kunci Public Elgamal

Dharma Yudistira

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia

Email: <sup>1</sup>dharmayudis@gmail.com

Email Penulis Korespondensi: dharmayudis@gmail.com

**Abstrak**—Pada proyek akhir ini dibuat sebuah enkripsi yang diintegrasikan dengan aplikasi penyandian agenda yang sudah ada untuk menambah keamanan pada proses pengamanan pada perangkat mobile tersebut. Dengan menggunakan metode enkripsi ElGamal, diharapkan proses enkripsi yang dilakukan melalui perangkat Mobile menjadi lebih aman. Karena, adanya public key dan private key yang hanya diketahui oleh pengguna. Output yang dihasilkan merupakan cipherteks yang mana ketika pengguna ingin membacanya, perlu untuk melakukan proses dekripsi. Selain itu, proses enkripsi pada plainteks yang sama diperoleh cipherteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks yang sama. Sehingga, membuat agenda menjadi lebih aman dibanding sebelumnya.

**Kata Kunci:** Algoritma; Elgamal; Enkripsi; Dekripsi; Agenda

**Abstract**—In this final project, an encryption is created that is integrated with the existing agenda encoding application to add security to the security process on the mobile device. By using the ElGamal encryption method, it is hoped that the encryption process carried out through mobile devices will be more secure. Because, there is a public key and a private key that is only known by the user. The resulting output is ciphertext which when the user wants to read it, it is necessary to carry out the decryption process. In addition, in the encryption process for the same plaintext, different ciphertexts are obtained, but in the decryption process, the same plaintext is obtained. Thus, making the agenda safer than before.

**Keywords:** Algorithm; Elgamal; Encryption; Decryption; Agenda

## 1. PENDAHULUAN

Perkembangan teknologi komputasi mobile telah meningkat pesat, hal ini ditandai dengan semakin banyaknya fungsi pada perangkat *mobile*. Ini menjadi sebuah evolusi perangkat *mobile* dalam hal ini adalah handphone yang ditandai lahirnya teknologi *smartphone* yang kemampuannya hampir mirip dengan sebuah personel komputer. *Smartphone* merupakan kelas baru dari teknologi telepon selular yang bisa memfasilitas akses dan pemrosesan data dan pengamanan data dengan kekuatan komputasi yang signifikan.

*Smartphone* adalah salah satu sarana yang memudahkan keseharian seseorang. Mengabadikan momen merupakan suatu hal yang biasa dilakukan oleh seseorang menggunakan *smartphone*. Mengelompokkan beberapa momen menjadi satu akan memudahkan seseorang dalam mengorganisir banyak kegiatan. Tetapi banyak agenda yang rumit cara pengoperasiannya karena terlalu banyak fitur-fitur. Dengan adanya permasalahan di atas, maka diperlukan sebuah agenda pribadi yang lebih *use able* untuk bisa diakses dengan cepat dan mudah melalui perangkat *mobile*. Agenda pribadi merupakan aplikasi *mobile* berbasis android yang memberikan kemudahan dalam merancang dan membantu manajemen keseharian seseorang. Adapun Salah satu cara pemberian *solusinya* untuk mengatasi hal tersebut adalah menyandikan teks agenda tersebut sehingga bentuk teks menjadi teracak, sehingga apabila jatuh ke tangan yang tidak diinginkan, teks tersebut juga tidak dapat digunakan. Salah satu metode penyandian untuk tujuan di atas adalah menggunakan teknik penyandian *Elgamal*.

Perancangan Sistem Informasi Manajemen Agenda Kegiatan Pertemuan USNI Berbasis Berbasis Mobile dengan metode Elgamal. Selama ini banyak kegiatan yang dilakukan seperti agenda pribadi. Oleh karena itu, dibuatlah suatu Aplikasi mobile Agenda Kegiatan Pertemuan dengan metode Elgamal. Algoritma kriptografi ElGamal merupakan salah satu algoritma kriptografi kunci asimetris yang menggunakan sepasang kunci yang berbeda, satu kunci enkripsi dan satu kunci dekripsi. Hasil dari aplikasi ini mampu mengenkripsi file dengan format docx. Algoritma ElGamal memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima dan dua buah bilangan acak. Algoritma kriptografi ElGamal menggunakan beberapa persamaan untuk melakukan proses *generate key*, proses enkripsi dan proses dekripsi.

Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data pada agenda pribadi, Adapun yang diterapkan dalam pengamanan pada *agenda pribadi* ini adalah dengan teknik penyandian menggunakan algoritma *Elgamal* karena untuk menjaga kerahasiaan suatu data salah satunya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *ciphertext*. Sedangkan suatu proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan biasa (yang mudah dibaca) disebut dekripsi. Ditengah kesibukan sehari-hari dengan jadwal yang berbeda-beda, membutuhkan sebuah agenda yang tepat. Agenda tersebut dapat berupa perjanjian dan pertemuan berdasarkan lokasi tertentu. Melihat jumlah kegiatan pertemuan yang semakin padat, maka *tools* pengingat agenda menjadi sangat dibutuhkan oleh masyarakat. Pengingat agenda yang dimaksud tentunya tidak hanya berisi waktu, tempat kegiatan tersebut dilakukan, serta keterangan saja, tetapi juga diperlukan lokasi (dalam bentuk peta) dari kegiatan tersebut. Untuk itu *tools* pengingat yang dimaksud tidak hanya berorientasi pada waktu tetapi juga berorientasi pada lokasi pengguna berada. Secara khusus *tools* (dalam hal ini adalah software aplikasi) pengingat agenda dan lokasi dapat haruslah memiliki Informasi yang perlu disimpan, meliputi nama pertemuan, waktu, lokasi, prioritas dari pertemuan, serta keterangan lain yang dibutuhkan pada saat pertemuan tersebut berlangsung.

## 2. METODOLOGI PENELITIAN

### 2.1 Keamanan

Keamanan merupakan salah satu aspek terpenting dari sebuah system informasi. Masalah keamanan sering kurang mendapatkan perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering beradadi urutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting [3].

Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. Keamanan merupakan topik yang luas termasuk keamanan nasional terhadap serangan teroris, keamanan komputer terhadap *hacker*, keamanan rumah terhadap maling dan penyusup lainnya, keamanan financial terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya. *Host* komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar dari pada *host* yang tidak berhubungan kemana-mana. Dengan mengendalikan *network security* resiko tersebut dapat dikurangi [5].

### 2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu *kripto* dan *graphia*. *Kripto* berarti *secret* (rahasia) *graphia* berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan akan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint*) [5].

### 2.3 Metode ElGamal

Metode ElGamal merupakan beberapa persamaan untuk melakukan proses *generate key*, proses enkripsi dan proses dekripsi [2]. Algoritma ElGamal memerlukan sepasang kunci yang dibangkitkan dengan memilih bilangan prima  $p$  dan dua buah bilangan acak (*random*)  $g$  dan  $x$ , dengan syarat bahwa nilai  $g$  dan  $x$  lebih kecil dari  $p$  yang memenuhi persamaan.

$y = g^x \text{ mod } p$  Dari persamaan tersebut nilai  $y$ ,  $g$  dan  $p$  merupakan pasangan kunci public sedangkan  $x$ ,  $p$  merupakan pasangan kunci pribadi [2]. Besaran-besaran yang digunakan dalam algoritma kriptografi *ElGamal* adalah :

- Bilangan prima  $p$  bersifat tidak rahasia.
- Bilangan acak  $g$  ( $g < p$ ) bersifat tidak rahasia
- Bilangan acak  $x$  ( $x < p$ ) bersifat rahasia.
- Bilangan  $y$  bersifat tidak rahasia.
- $m$  (*plaintext*) bersifat rahasia merupakan pesan asli yang digunakan untuk data
- sumber dalam proses enkripsi dan merupakan data hasil pada proses dekripsi.
- $a$  dan  $b$  (*ciphertext*) bersifat tidak rahasia.

Metode ini memproses enkripsi dilakukan dengan memilih bilangan acak  $k$  yang berada dalam himpunan  $1 \leq k \leq p-2$ . Setiap blok *plaintext*  $m$  dienkripsi dengan persamaan. [2] :

$$a = g^k \text{ mod } p \quad (1)$$

$$b = y^k \text{ mod } p \quad (2)$$

Proses dekripsi menggunakan kunci pribadi  $x$  dan  $p$  untuk mendekripsi  $a$  dan  $b$  menjadi *plaintext*  $m$  dengan persamaan [2] :

$$(ax)^{-1} = a^{p-1-x} \text{ mod } p \quad (3)$$

$$m = b * a^x \text{ mod } p \quad (4)$$

Sehingga *plaintext* dapat ditemukan kembali dari pasangan *ciphertext*  $a$  dan  $b$ .

## 3. HASIL DAN PEMBAHASAN

Dalam hal ini yang diamankan adalah sebuah file agenda pribadi seperti halnya bahkan banyak yang menyimpan catatan-catatan yang menjadi privasi, dengan alasan agar mudah melihatnya kembali. Hal ini sangat beresiko ketika smartphonenya dicuri atau hilang. Sehingga catatan dapat dilihat orang dan hal-hal yang tidak diinginkan bisa saja terjadi, bahkan kemungkinan terburuknya dapat dimanfaatkan oleh orang lain. Salah satu solusi yang dapat digunakan untuk menangani permasalahan tersebut adalah dengan teknik kriptografi, dengan mengubah file menjadi *chiptexts* disebut juga dengan teknik enkripsi dengan menggunakan metode ElGamal.

Dalam mengamankan file agenda pribadi pada handphone android menguraikan dari suatu sistem yang utuh kedalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan-permasalahan dan kebutuhan-kebutuhan yang diharapkan sehingga dapat dilakukan perbaikannya atau pemecahan masalahnya. *smartphone* berbasis android yang open source membuat para programmer berlomba-lomba untuk membuat mobile aplikasi berbasis android yang dapat menarik minat banyak pengguna. Namun disadari atau tidak kebanyakan pengguna *smartphone* memasang aplikasi catatan agenda dan menggunakannya untuk pengingat. Bahkan banyak yang

menyimpan catatan-catatan yang menjadi privasi. Dengan alasan agar mudah melihatnya kembali. Hal ini sangat beresiko ketika smartphonenya dicuri atau hilang. Sehingga catatan dapat dilihat orang dan hal-hal yang tidak diinginkan bisa saja terjadi, bahkan kemungkinan terburuknya dapat dimanfaatkan oleh orang lain.

### 3.1 Penerapan Metode Elgamal

Proses yang dilakukan adalah *plainteks* terlebih dahulu akan dienkripsi berdasarkan algoritma *Elgamal* sehingga menghasilkan *cipherteks*. Kemudian *cipherteks* yang dihasilkan akan didekripsi kembali berdasarkan algoritma *Elgamal* hingga dihasilkan *plainteks*. Dalam penerapan kriptografi yang sedang penulis bahas yaitu mengenai penyandian sebuah file pada agenda pribadi dengan menggunakan algoritma Kunci Public Elgamal. Sebagaimana gambaran pada analisa masalah, maka solusi atau pemecahan dari masalah yang ada adalah dengan membuat suatu sistem atau alat bantu yang mampu memberikan kenyamanan dan rasa aman dikala seseorang menyimpan sebuah catatan yang menjadi rahasia pribadinya pada sebuah smartphone berbasis android dengan menerapkan kriptografi Kunci Public Elgamal.

Dalam agenda pribadi atau *plainteks* dengan nama "DHARMA" sebelum melakukan proses enkripsi, ubah terlebih dahulu ke ASCII dari setiap huruf, Adapun nilai numerik "DHARMA": ASCII (68, 72, 65, 82, 77, 65)

Enkripsi Metode Elgamal

Input teks : DHARMA

Proses Pembangkitan Kunci :

$$P = 257 ; g = 7 ; x = 2$$

Hitung  $y = g^x \text{ mod } p$

$$y = 7^2 \text{ mod } 257$$

$$y = 49 \text{ mod } 257$$

$$y = 49$$

Berdasarkan proses pembangkit kunci, maka diperoleh :

Kunci PRIVATE = (x,y)  $K_{\text{public}} = (2, 257)$

Kunci PUBLIC = (p,g,y)  $K_{\text{public}} = (257,7,49)$

Plaintek = DHARMA

Nilai k yang dipilih harus berada dalam himpunan  $1 \leq k \leq p-2$ .

Nilai k untuk P1 = 4

$$a = g^k \text{ mod } p$$

$$a = 7^4 \text{ mod } 257$$

$$a = 2401 \text{ mod } 257 = 88$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^4 \text{ mod } P_1) \text{ mod } 257$$

$$= 5764801 * 68 \text{ mod } 257$$

$$= 392006468 \text{ mod } 257$$

$$= 256$$

Nilai k untuk P2 = 2

$$a = g^k \text{ mod } p$$

$$a = 7^2 \text{ mod } 257$$

$$a = 49 \text{ mod } 257 = 49$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^2 \text{ mod } P_2) \text{ mod } 257$$

$$= 2401 * 72 \text{ mod } 257$$

$$= 172872 \text{ mod } 257$$

$$= 168$$

Nilai k untuk P3 = 3

$$a = g^k \text{ mod } p$$

$$a = 7^3 \text{ mod } 257$$

$$a = 373 \text{ mod } 257 = 86$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^3 \text{ mod } P_3) \text{ mod } 257$$

$$= 117649 * 65 \text{ mod } 257$$

$$= 7647185 \text{ mod } 257$$

$$= 150$$

Nilai k untuk P4 = 5

$$a = g^k \text{ mod } p$$

$$a = 7^5 \text{ mod } 257$$

$$a = 16807 \text{ mod } 257 = 102$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^5 \text{ mod } P_4) \text{ mod } 257$$

$$= 282475249 * 82 \text{ mod } 257$$

$$= 23162970418 \text{ mod } 257$$

$$= 145$$

Nilai k untuk P5 = 2

$$a = g^k \text{ mod } p$$

$$a = 7^2 \text{ mod } 257$$

$$a = 49 \text{ mod } 257 = 49$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^2 \text{ mod } P_5) \text{ mod } 257$$

$$= 2401 * 77 \text{ mod } 257$$

$$= 184877 \text{ mod } 257$$

$$= 94$$

Nilai k untuk P6 = 4

$$a = g^k \text{ mod } p \quad a = 7^4 \text{ mod } 257$$

$$a = 2401 \text{ mod } 257 = 88$$

$$b = (y^k \text{ mod } P_i) \text{ mod } p$$

$$b = (49^4 \text{ mod } P_6) \text{ mod } 257$$

$$= 5764801 * 65 \text{ mod } 257$$

$$= 374712065 \text{ mod } 257$$

$$= 154$$

Tabel 1. Hasil Plainteks

Plainteks	Char	DEC	K	$a=(g^k)\text{mod } p$	$b=((y^k)*M)\text{ mod } p$	(a,b)
P1	D	68	4	88	256	(88,256)
P2	H	72	2	49	168	(49,168)
P3	A	65	3	86	150	(86,150)
P4	R	82	5	102	145	(102,145)
P5	M	77	2	49	94	(49,94)
P6	A	65	4	88	154	(88,154)

Hasil enkripsi dari Plaintek "DHARMA" adalah = (88,256), (49,168), (86,150), (102,145), (49,94), (88,154).

Dekripsi Metode Elgamal

Chiperteks:

(88,256), (49,168), (86,150), (102,145), (49,94), (88,154).

Kunci :  $x = 2$ ,  $p = 257$

Mencari Plainteks P1:

$$s = a^x \text{ mod } p \quad P1 = (b * S^{p-2}) \text{ mod } p$$

$$s = 88^2 \text{ mod } 257 \quad P1 = (256 * 34^{(257-2)}) \text{ mod } 257$$

$$s = 7744 \text{ mod } 257 \quad P1 = (256 * 34^{255}) \text{ mod } 257$$

$$s = 34 \quad P1 = 68 = D$$

Mencari Plainteks P2:

$$s = a^x \text{ mod } p \quad P2 = (b * S^{p-2}) \text{ mod } p$$

$$s = 49^2 \text{ mod } 257 \quad P2 = (168 * 88^{(257-2)}) \text{ mod } 257$$

$$s = 2401 \text{ mod } 257 \quad P2 = (168 * 88^{255}) \text{ mod } 257$$

$$s = 88 \quad P2 = 72 = H$$

Mencari Plainteks P3:

$$s = a^x \text{ mod } p \quad P3 = (b * S^{p-2}) \text{ mod } p$$

$$s = 86^2 \text{ mod } 257 \quad P3 = (150 * 200^{(257-2)}) \text{ mod } 257$$

$$s = 7396 \text{ mod } 257 \quad P3 = (150 * 200^{255}) \text{ mod } 257$$

$$s = 200 \quad P3 = 65 = A$$

Mencari Plainteks P4:

$$s = a^x \text{ mod } p \quad P4 = (b * S^{p-2}) \text{ mod } p$$

$$s = 102^2 \text{ mod } 257 \quad P4 = (145 * 124^{(257-2)}) \text{ mod } 257$$

$$s = 10404 \text{ mod } 257 \quad P4 = (145 * 124^{255}) \text{ mod } 257$$

$$s = 124 \quad P4 = 82 = R$$

Mencari Plainteks P5:

$$s = a^x \text{ mod } p \quad P5 = (b * S^{p-2}) \text{ mod } p$$

$$s = 49^2 \text{ mod } 257 \quad P5 = (94 * 88^{(257-2)}) \text{ mod } 257$$

$$s = 2401 \text{ mod } 257 \quad P5 = (94 * 88^{255}) \text{ mod } 257$$

$$s = 88 \quad P5 = 77 = M$$

Mencari Plainteks P6:

$$s = a^x \text{ mod } p \quad P6 = (b * S^{p-2}) \text{ mod } p$$

$$s = 88^2 \text{ mod } 257 \quad P6 = (154 * 34^{(257-2)}) \text{ mod } 257$$

$$s = 7744 \text{ mod } 257 \quad P6 = (154 * 34^{255}) \text{ mod } 257$$

$$s = 34 \quad P6 = 65 = A$$

Dalam proses pendekripsian algoritma Kunci Public Elgamal sama dengan langkah-langkah proses enkripsi, karna algoritma Kunci Public Elgamal merupakan kriptografi system kunci simetris dalam artian kunci enkripsi dan kunci

dekripsi. Seperti contoh diatas cipherteks yang didapat akan diproses kembali menjadi teks aslinya. Yaitu: **68, 72, 65, 82, 77, 65** menjadi **DHARMA**

#### **4. KESIMPULAN**

Dari hasil pembahasan tentang perancangan aplikasi penyandian pada agenda pribadi menggunakan algoritma ElGamal berbasis android, maka diambil beberapa kesimpulan 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. Ciphertext yang dihasilkan dari plaintext dengan menggunakan algoritma ElGamal dapat berbeda beda karena adanya penggunaan bilangan acak pada pengenkripsian plaintexts. Akan tetapi, ketika didekripsikan, plaintexts yang dihasilkan sama. Penggunaan blok-blok ciphertexts pada algoritma ElGamal menyebabkan panjang ciphertexts menjadi dua kali panjang dari plaintexts. Implementasi algoritma ElGamal berbasis android menjadi sebuah model kriptosistem. Dengan adanya aplikasi ini dapat membantu dalam proses enkripsi dan dekripsi agenda pribadi. Sehingga menjamin kerahasiaan dalam komunikasi pesan penting.

#### **REFERENCES**

- [1] Safaat, Nazruddin, Pemrograman Aplikasi Mobile Smartphone Dan Table PC Berbasis Android, Informatika, Bandung 2012.
- [2] M.Taufiq Tamam, 2010. Penerapan Algoritma Kriptografi ElGamal Untuk Pengamanan File Citra, Jurnal EECCIS Vol.4 No.1 : Yogyakarta
- [3] Wina Novianti Fatimah, ST. Pengenalan Eclipse, p.15. February 2011
- [4] Mulyadi, ST. 2010. Membuat Aplikasi Untuk Android. Multimedia Center Publishing, Yogyakarta.
- [5] Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, ANDI : Yogyakarta.
- [6] B. Haryanto. 2011. Esensi-esensi Bahasa Pemrograman Java. ANDI : Yogyakarta
- [7] S. Hermawan. 2011. Mudah Membuat Aplikasi Android. ANDI : Yogyakarta
- [8] Adi Nugroho, 2010, Rekayasa Perangkat Lunak Menggunakan UML dan Java. Penerbit ANDI : Yogyakarta
- [9] Shalahuddin, M. Belajar Pemrograman Dengan Bahasa C++ dan Java, Informatika, Bandung 2005.
- [10] Umni Nur Fadhillah. Aplikasi Agenda Pribadi Enot Berbasis Android, STMIK AMIKOM, Yogyakarta : 2013