**Penyandian SMS Pada Telephone Seluler Menggunakan Algoritma Elgamal**

**Siti Nur Aini(1116101364)**

*Teknik Informatika, Sekolah Tinggi Ilmu Komputer PGRI, Banyuwangi, Jawa Timur, Indonesia*

*E-mail:* [sitinuraini.hb@gmail.com](mailto:sitinuraini.hb@gmail.com)

***Abstrak*** — Perkembangan teknologi dan informasi sangat berkembang pesat terutama dalam bidang informasi, salah satunya adalah smart phone yaitu pertukaran informasi berupa pesan teks melalui SMS. Informasi terebut dapat berupa data penting yang bersifat privasi yang beberapa orang tidak boleh mengetahuinya, namun tingkat keamanan data informasi pada SMS masih sangat mengancam. Sistem keamanan pesan yang berbentuk teks salah satunya dengan teknik kriptografi. Kriptografi adalah ilmu keamanan pesan yang bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung

jawab. Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa dengan teknik enkripsi sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum dapat penyandian dikenal dengan istilah plaintext, dan setelah disamarkan dengan suatu cara penyandian dikenal dengan istilah plaintext dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini berubah menjadi ciphertext. Terdapat banyak algoritma yang di gunakan teknik kriptografi, salah satunya algoritma yang digunakan adalah code hill.

*Kata kunci* : teknologi, informasi, SMS, Kriptografi, plaintext,enkripsi, chipertext.

1. **Pendahuluan**

Perkembangan teknologi dan informasi saat ini sangat pesat terutama di bidang informasi komunikasi khususnya di dunia mobile seperti telepon seluler yang sudah menjadi gaya hidup masyarakat sebagai alat komunikasi. Seiring berkembangnya jaman komunikasi tidak harus bertatap muka langsung melainkan dengan cara hanya mengirimkan informasi yang berbentuk pesan teks singkat yang biasa di sebut dengan SMS(*Short Message Service*), pesan teks tersebut bisa berupa pesan penting yang sifatnya privasi yang beberapa orang tidak bisa melihat atau menerimanya.

Namun keamanan pesan teks ini adalah masih sangat mengancam karena banyak orang bisa menerima data atau pesan penting tersebut dengan cara menyadap pesan teks sehingga dapat menerima data penting yang bersifat private.

Untuk mengurangi resiko terancam bocornya pesan teks tersebut membutuhkan sistem penyandian pesan teks yang mampu menjaga kerahasiaan isi pesan.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integerasi, seperti autentikasi data, yang bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui

oleh pihak yang tidak bertanggung jawab,kriptografi mengubah tulisan yang semula bermakna menjadi tidak bermakna menggunakan berbagai macam algoritma kriptografi dengan cara enkripsi adalah proses dimana data yang dikirim berupa data jelas(plaintext) yang akan diubah menjadi data yang hampir tidak dapat dikenali(chipertext), sedangkan deskripsi mengubah kembali data yang tersamarkan menjadi data awal yang dapat dikenali.

Algoritma Elgamal adalah suatu *public key* yang dibuat pada tahun 1985. Keamanan dari algoritma ElGamal terletak pada susahnya perhitungan logaritma pada GF(p) ketika p merupakan bilangan prima yang besar. Logaritma ini disebut logaritma diskret karena nilainya berhingga dan bergantung pada bilangan prima yang digunakan. Karena bilangan prima yang digunakan adalah bilangan prima besar, maka sangat sulit bahkan tidak mungkin menurunkan kunci rahasia dari kunci publik yang diketahui walaupun serangan dilakukan dengan menggunakan sumber daya komputer yang sangat besar (1).

Berdasarkan latar belakang tersebut di perlukan adanya pokok – pokok permasalahan. Adapun permasalahannya :

1. Bagaimana cara menyandikan pesan teks *Short Message Service* (SMS) ?

2. Bagaimana cara enkripsi dan deskripsi pesan teks *Short Message Service* (SMS) dengan menggunakan algoritma ElGamal ?

Batasan masalah agar tidak melebarnya rumusan pembahasan permasalahan inputan berupa pesan teks, algoritma Elgamal menyandikan input berupa huruf, angka dan simbol.

Tujuan penelitian ini adalah mengutahui cara menyandikan pesan teks pada *Short Message Sor*t(SMS), dan mengetahui cara enkripsi dan deskripsi pesan teks *Short Message Sor*t(SMS) dengan menggunakan algoritma Elgamal.

1. **LANDASAN TEORI**

**2.1 Pengertian Kriptografi**

Kriptografi (*cryptography*) berasal dari dua kata dalam Bahasa Yunani, yaitu “*cryptos*” yang berarti rahasia, dan “*graphein*” yang berarti tulisan. Kriptografi adalah ilmu mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Secara umum, kriptografi terdiri dua proses utama, yaitu enkripsi dan dekripsi. Proses enkripsi akan mengubah pesan asli(plainteks) menjadi pesan terenkripsi dengan menggunakan algoritma dan kunci tertentu yang tidak dapat dibaca secara langsung(chiperteks). Proses dekripsi merupakan kebalikan dari proses enkripsi, yaitu proses untuk memperoleh kembali plainteks dari chiperteks menggunakan kunci dan algoritma tertentu (2).

**2.1.1 Kriptografi Modern**

Kriptografi modern mempunyai kerumitan yang sangat kompleks karena dioperasikan menggunakan komputer. Algoritma kriptografi modern tidak lagi mengandalkan kemanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *chipertext* yang berbeda pula. Algoritma kriptografi dapat bersifat umun dan boleh diketahui oleh siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat terpecahkan. Berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptografi dapat dibedakan menjadi dua jenis, yaitu :

1. Algoritma block chiper

Informasi yang hendak dikirim dalam bentuk blok-blok besar (misalnya 64 bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama pula.

2. Algoritma stream chiper

Informasi yang hendak dioperasikan dalam bentuk yang lebih kecil (byte atau bit), biasanya satu karakter persatuan waktu proses menggunakan transformasi enkripsi yang berubah setiap waktu.

**2.2 Algoritma**

**2.2.1 Algoritma Elgamal**

ElGamal adalah suatu *public key cryptosystem* asimetris yang dibuat pada tahun 1985 oleh Taher ElGamal. ElGamal digunakan untuk melakukan enkripsi dan tanda tangan digital. ElGamal menggunakan analisis matematis dalam enkripsinya yang didasarkan pada masalah logaritma diskrit. ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk sistem kriptografi ElGamal, dibutuhkan bilangan prima p dan elemen primitif α.

Dalam ElGamal menggunakan bilangan bulat dalam proses perhitungannya, maka pesan harus dikonversi ke dalam suatu bilangan bulat. Untuk mengubah pesan menjadi bilangan bulat digunakan kode ASCII (*American Standard for Information Interchange*). Kode ASCII merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Oleh karena itu, berdasarkan sistem kriptografi ElGamal di atas maka harus digunakan bilangan prima yang lebih besar dari 255 (Nasional, Mada, Matematika, Ilmu, & Alam, 2007). (3)

* Pembentukan Kunci

Pada proses pembentukan kunci ElGamal terdiri dari kunci rahasia dan kunci publik yang termasuk dalam golongan algoritma asimetris. Proses pembentukan kunci ini merupakan proses penentuan suatu bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan dekripsi pesan.

Pada proses ini dibutuhkan bilangan prima *p*, elemen primitif acak dan bilangan sembarang ɑ Kunci publik untuk enkripsi berupa pasangan 3 bilangan yang dibangkitkan dari nilai (p, ), dengan

*β = αɑ mod p*

Sedangkan kunci rahasia untuk dekripsi terdiri dari nilai ɑ, p. Masing-masing nilai mempunyai persyaratan yang harus dipenuhi. Langkah-langkah dalam pembuatan kunci adalah sebagai berikut :

1. Pilih sembarang bilangan prima p, dengan syarat p > 255.

2. Pilih elemen primitif acak dengan syarat < p.

3. Pilih bilangan acak ɑ dengan syarat 1 ≤ ɑ ≤ p – 2.

4. Hitung *β = αɑ mod p*

5. Publikasikan nilai *p*, *α dan β,* serta rahasiakan nilai *ɑ*.



Gambar 1. Flowchart Proses Pembentukan Kunci

Pihak yang membuat kunci publik dan kunci rahasia adalah penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi keuntungan menggunakan algoritma kriptografi kunci publik adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamnan jalur yang digunakan (Massandy, 2009).

Enkripsi

Proses enkripsi merupakan proses mengubah pesan asli (plainteks) menjadi pesan rahasia (chiperteks). Pada proses ini digunakan kunci publik (*p*,). Langkah-langkah dalam mengenkripsi pesan adalah sebagai berikut :

1. Potong plainteks menjadi blok-blok m1, m2, m3, …, mn nilai setiap blok di dalam selang [0, p – 1].

2. Ubah nilai blok pesan ke dalam nilai ASCII.

3. Pilih bilangan acak k, dengan syarat 1 ≤ k ≤ p – 1 sebanyak m.

4. Setiap blok m dienkripsi dengan rumus sebagai berikut :

γ = αki mod *p*

δ = βki m mod *p*

Susun chiperteks dengan urutan γ1, δ1, γ2, δ2, …, γn, δn. Pasangan γ dan δ adalah chiperteks untuk blok pesan m.

Dekripsi

Proses dekripsi merupakan proses mengubah pesan rahasia (chiperteks) menjadi pesan asli (plainteks). Pada proses ini digunakan kunci pribadi (ɑ, *p*). Langkah-langkah dalam mendekripsi pesan adalah sebagai berikut :

1. Hitung plaintext m dengan persamaan sebagai berikut

mi = δi.γ i(p-1-ɑ) mod *p*

2. Nilai mi yang di dapat dalam bentuk ASCII kemudian diubah menjadi plainteks .

3. Susun plainteks dengan urutan m1, m2, m3, ., mn.

Hasil yang didapat dari proses dekripsi berupa pesan asli (plainteks).

1. **Hasil Penelitian dan Analisa**

Salah satu cara untuk mengamankan pesan salah satunya dengan melakukan penyandian teks menggunakan algoritma kriptografi tertentu. Penyandian dilakukan dengan cara mengubah teks sebelum dikirim sehingga pesan awal berubah menjadi huruf atau angka acak yang tidak memiliki arti proses ini disebut enkripsi. Setelah pesan sampai kepada penerima maka penerima juga harus mengubah pesan acak tersebut menjadi pesan asli yang mengandung arti menggunakan algoritma yang sama seperti saat pengubahan pesan asli ke pesan acak yang disebut dengan deskripsi.

3.1 analisa Penerapan Algoritma

1. Algoritma Elgamal

Di berikan contoh kasus Bob mengirimkan pesan kepada rina, akan tetapi pesan harus dirahasiakan. Pesan yang akan di kirim “SEMANGAT”.

1. Pembentukan kunci

Pada metode ElGamal penerimalah yang harus membuat kunci publik yaitu Rina, misalkan dipilih bilangan prima *p* = 253 dan elemen primitif α = 5. Selanjutnya dipilih ɑ = 11. Maka dapat dihitung dengan rumus berikut:

*β =* αɑ *mod p*

*β = 511 mod 253*

*β = 137*

Sehingga diperoleh kunci publik (*p,α,β*) = (253, 5, 137) dan kunci rahasia ɑ = 11 p= 253. Kemudian Bob memberitahukan kunci publik ini kepada Rina. Dan kunci rahasia tetap dirahasiakan oleh Bob.

1. Proes Enkripsi

Sebelum melakukan enkripsi plainteks di konversi ke dalam kode ASCII.

|  |  |  |  |
| --- | --- | --- | --- |
| i | Karakter | mi | ASCII |
| 1 | S | M1 | 83 |
| 2 | E | M2 | 69 |
| 3 | M | M3 | 77 |
| 4 | A | M4 | 65 |
| 5 | N | M5 | 78 |
| 6 | G | M6 | 71 |
| 7 | A | M7 | 81 |
| 8 | T | M8 | 71 |

Berdasarkan Tabel di atas tersebut, diperoleh bahwa banyaknya karakter pada pesan tersebut adalah n = 8. Proses selanjutnya adalah menentukan bilangan acak rahasia dengan ketentuan berikut *k € {0,1, ..., p - 2}* sehigga berdasarkan p ditentukan *ki € {0,1, ..., 251}*, dengan nilai i = 1, 2, ..., 8. Selanjutnya berdasarkan rumus *γ = αk mod p* dan *δ = βk .m mod p*, dapat dihitung nilai γi = 2ki mod 253 dan δi = 137ki .mi mod 253 seperti pada Tabel dibawah.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I | Mi | Ki | γi = 2ki mod 253 | δi = 137ki .mi mod 23 |
| 1 | M1 | 41 | 91 | 56 |
| 2 | M2 | 11 | 137 | 150 |
| 3 | M3 | 13 | 89 | 239 |
| 4 | M4 | 31 | 113 | 205 |
| 5 | M5 | 33 | 198 | 224 |
| 6 | M6 | 9 | 218 | 214 |
| 7 | M7 | 51 | 84 | 137 |
| 8 | M8 | 15 | 97 | 79 |

Berdasarkan Tabel , diperoleh ciphertext (γi,δi), i = 1, 2, ..., 8 sebagai berikut.

(91, 56) (137, 150) (89, 239) (113, 205)

(198, 224) (218, 214) (84,137) (97, 79)

1. **Kesimpulan**

Daftar Pustaka

1. *Perancangan Aplikasi Penyandian Pesan Teks Menggunakan Vigenere Chiper Dan Algoritma Elgamal.* **Basyiah dan Syahputra, Fahmy.** medan : MEANS (Media Informasi Analisa dan Sistem), 2, Desember 2017, Vol. 2. 1-2.

2. *PENYANDIAN SHORT MESSAGE SERVICE (SMS) PADA TELEPON SELULAR DENGAN MENGGUNAKAN ALGORITMA GRONSFELD.* **Azanuddin.** Medan : s.n., Agustus 2013, Vol. IV.

3. *RANCANGAN KRIPTOGRAFI HYBRID KOMBINASI METODE VIGENERE CIPHER DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA.* **Ariska, Bella, Suroso dan Endri, Jon.** Malang : s.n., 3 Pebruari 2018.