SISTEM INFORMASI PEMBELAJARAN KRIPTOGRAFI MENGGUNAKAN METODA GOST

Sufajar Butsianto

Program Studi Teknik Informatika Sekolah Tinggi Teknologi Pelita Bangsa
sufajar.butsianto@pelitabangsa.ac.id

Disetujui, 15 Februari 2018

Abstraksi

Berbagai cara dilakukan orang untuk mendapatkan data dan informasi, meskipun dengan cara mencuri dan lalu mengubah isi dari informasi tersebut. Pada penelitian ini dibuat suatu aplikasi menggunakan teknik kriptografi yang dapat digunakan untuk mengamankan informasi yang dikirim melalui e-mail. Algoritma yang digunakan adalah algoritma GOST (Gosudarstvennyi Standard). Algoritma GOST merupakan algoritma simetris blok cipher 64 bit yang dikenal cukup aman karena memiliki 32 putaran dalam proses enkripsi dan dekripsi. Bahasa pemrograman yang digunakan adalah PHP. Pada aplikasi ini kunci enkripsi dan dekripsi diatur oleh sistem, hal ini dilakukan agar informasi kunci tidak dapat diketahui dengan mudah oleh pihak yang tidak berkepentingan. Berdasarkan implementasi dan pengujian program, dapat disimpulkan bahwa aplikasi ini mudah digunakan, pesan yang dikirim dan diterima melalui aplikasi ini aman karena sudah melalui proses enkripsi terlebih dahulu.

Kata kunci - Kriptografi, E-mail, Algoritma GOST.

Abstract

There are various ways people do to get data and information, although by stealing and then changing the content of the information. In this research, an application is made using cryptographic techniques that can be used to secure information sent via e-mail. The algorithm used is the GOST algorithm (Gosudarstvennyi Standard). The GOST algorithm is a 64-bit symmetric block cipher algorithm which is known to be quite safe because it has 32 rounds in the encryption and decryption process. The programming language used is PHP. In this application the encryption and decryption keys are set by the system, this is done so that key information cannot be easily identified by unauthorized parties. Based on the implementation and testing of the program, it can be concluded that this application is easy to use, messages sent and received through this application are safe because they have gone through the encryption process first.

Keywords - Cryptography, E-mail, GOST Algorithm.

1. Pendahuluan

Sekarang ini, sering ditemukan berbagai macam perangkat lunak pembelajaran. Perangkat lunak yang penulis ingin rancang adalah mengenai kriptografi. Kriptografi merupakan ilmu yang mempelajari tentang pengamanan data atau informasi, dalam kriptografi banyak ditemukan

metoda-metoda kriptografi. Salah satunya adalah metoda GOST, GOST ini merupakan singkatan dari "*Gosudarstvennyi Standard*" atau "*Government Standard*". Algoritmanya merupakan algoritma enkripsi sederhana yang memiliki jumlah proses sebanyak 32 *round* dan menggunakan 64 bit *block cipher* dengan 256 bit *key*. Metoda GOST juga menggunakan 8 buah *S-Box* yang permanen dan operasi *XOR* serta *Rotate Left Shift*.

Metoda GOST merupakan suatu algoritma *block cipher* yang dikembangkan oleh seorang berkebangsaan Uni Soviet. Metoda ini dikembangkan oleh pemerintah Uni Soviet pada masa perang dingin untuk menyembunyikan data atau informasi yang bersifat rahasia pada saat komunikasi. Algoritma ini merupakan suatu algoritma enkripsi sederhana yang memiliki jumlah proses sebanyak 32 *round* (putaran) dan menggunakan 64 bit *block cipher* dengan 256 bit *key*. Metoda GOST juga menggunakan 8 buah *S-Box* yang berbeda-beda dan operasi *XOR* serta *Left Circular Shift*.

Kriptografi adalah ilmu yang mempelajari bagaimana suatu pesan atau dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Dalam perkembangannya, kriptografi juga digunakan untuk identifikasi pengirim pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*fingerprint*). Kriptografi mempunyai sejarah yang sangat panjang. Sejak jaman Romawi, Julius Caesar telah menggunakan teknik kriptografi yang sekarang dianggap kuno dan sangat mudah dibobol untuk keperluan komunikasi militernya. Namun sekutu dapat menembus Enigma, kriptografi produk Jerman dan Purple, kriptografi produk Jepang, sekutu akhirnya dapat memenangkan perang dunia kedua karena dapat mengetahui beberapa langkah dan strategi militer lawan.

Penulis memilih topik perangkat lunak pembelajaran karena penulis ingin membuat bagaimana cara *user* (pengguna) lebih memahami serta menambah minat user terhadap pembelajaran tersebut, dengan menampilkan teori-teori serta animasi yang mendukung. Jenis perangkat lunak pembelajaran yang penulis singgung tentunya adalah pembelajaran kriptografi metoda GOST. Perangkat lunak pembelajaran ini dirancang supaya metoda GOST dapat lebih mudah dipahami baik algoritma maupun operasi-operasi yang terkandung dalam metoda GOST ini.

2. Landasan Teori

2.1. Kriptografi

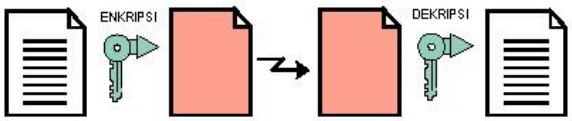
Kriptografi mulai digunakan dan disumbangkan pemikirannya pertama kali oleh empat kelompok, yakni militer, korps diplomatik, *diarist*, dan orang yang sedang jatuh cinta. Dari keempat kelompok orang tersebut, militer telah memainkan peranan yang paling penting dan telah mengembangkan bidang ini. Di dalam organisasi militer, pesan-pesan yang telah di-*encode* secara tradisional diberikan kepada pekerja kode berupah rendah untuk selanjutnya dienkrip dan ditransmisikan. Tugas ini diusahakan agar tidak dilakukan oleh spesialis yang elit. Kendala tambahan telah menjadi kesulitan dalam peralihan yang cepat dari satu algoritma kriptografi ke algoritma lainnya, karena hal ini memerlukan pelatihan orang dalam jumlah banyak.

Secara etimologi (ilmu asal usul kata), kata kriptografi berasal dari gabungan dua kata dalam bahasa Yunani yaitu "*kriptos*" dan "*graphia*". Kata *kriptos* digunakan untuk mendeskripsikan sesuatu yang disembunyikan, rahasia atau misterius. Sedangkan kata *graphia* berarti tulisan. Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau

orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.

Dalam arti lain, *cryptography* adalah seni dan ilmu dalam mengamankan pesan. Dalam dunia kriptografi, pesan disebut *plaintext* atau *cleartext*. Proses untuk menyamarkan pesan dengan cara sedemikian rupa untuk menyembunyikan isi aslinya disebut enkripsi. Pesan yang telah dienkripsi disebut *ciphertext*. Proses pengembalian sebuah *ciphertext* ke *plaintext* disebut dekripsi.



Gambar 2.1 Konsep Dasar dari Enkripsi dan Dekripsi

Cryptographer adalah orang yang mempraktekkan ilmu kriptografi, sedangkan *cryptoanalysts* adalah orang yang mempraktekkan kriptanalisis, seni dan ilmu dalam memecahkan *ciphertext*.

2.2. Algoritma Simetrik

Algoritma simetrik adalah suatu algoritma yang simetris dengan menggunakan sebuah kunci yang sama baik dalam melakukan enkripsi maupun dekripsi. Apabila kunci yang digunakan dalam melakukan enkripsi dan dekripsi berbeda, maka menyebabkan keluaran terakhir dari algoritma kacau, sehingga tidak berhasil mengembalikan bentuk *ciphertext* ke *plaintext* semula. Karena kunci ini memegang peranan yang sangat penting dalam melakukan enkripsi maupun dekripsi, maka algoritma simetrik ini disebut juga dengan algoritma kunci rahasia (*Secret key algorithm).* Algortima ini mengharuskan pengirim dan penerima pesan untuk menyetujui kunci yang akan digunakan dan keamanan dari algoritma ini tergantung dari kunci yang digunakan, sehingga kunci ini harus dirahasiakan. Jika kunci ini disebarkan berarti semua orang dapat melakukan enkripsi dan dekripsi pesan dalam sistem tersebut.

Dalam notasi matematika, proses algoritma kunci rahasia digambarkan sebagai berikut:

$E_k(P) = C$

$D_k(C) = P$

E_k dan D_k adalah fungsi enkripsi dan dekripsi yang menggunakan kunci sama.

2.3. Algoritma Asimetrik

Berbeda dengan algoritma kunci rahasia, algoritma kunci umum dirancang sedemikian rupa sehingga kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi, dan bahkan kunci yang digunakan untuk dekripsi tidak dapat dikalkulasikan atau diturunkan dari kunci enkripsi. Algoritma ini disebut algoritma kunci umum (*public key algorithm*) karena kunci enkripsi yang digunakan boleh disebarluaskan, berarti setiap orang dapat

melakukan enkripsi, namun hanya pihak yang memegang kunci dekripsi saja yang dapat melakukan dekripsi.

Beberapa istilah dalam algoritma kunci umum yaitu,

1. Kunci umum, yaitu kunci yang diberikan atau disebarkan kepada publik sehingga semua orang akan tahu.
2. Kunci privat, yaitu kunci yang tetap disimpan oleh pemilik kunci.

Dalam notasi matematika, proses algoritma kunci publik digambarkan sebagai berikut,

$$E_{k1}(P) = C$$
$$D_{k2}(C) = P$$

E_{k1} → fungsi enkripsi dengan kunci publik
D_{k2} → fungsi dekripsi dengan kunci privat

2.4. Digital Signature

Apabila kita menulis sebuah surat, biasanya kita menandatangani surat tersebut. Kita melakukan itu dengan tujuan untuk menunjukkan bahwa surat itu otentik, surat itu memang buatan kita. Tanda tangan digital juga bertujuan sama dengan tanda tangan biasa, bedanya proses penandatanganannya juga bersifat digital.

Tanda tangan digital menggunakan gabungan dua teknik kriptografi yaitu *hash* dan kriptografi asimetrik. Dokumen yang akan ditandatangani pertama-tama dibuatkan *digest*-nya, setelah itu *digest* tersebut dienkripsi dengan teknik kriptografi asimetrik menggunakan kunci privat, hasilnya adalah tanda tangan digital. Dokumen asli dan tanda tangan digital kemudian dikirim secara bersaman. Tujuan dari cara ini akan lebih jelas bila kita sudah melihat bagaimana cara melakukan verifikasinya.

Dokumen dan tanda tangan digital yang diterima kemudian diverifikasi. Tanda tangan digital yang diterima mula-mula didekripsi menggunakan kunci publik yang diasumsikan sebelumnya sudah dimiliki si penerima. Hasil dari dekripsi tersebut adalah *digest*, kita sebut saja D1 (*digest* yang diperoleh dari tanda-tangan digital). Langkah selanjutnya adalah membuat *digest* dari dokumen yang kita terima, hasilnya kita sebut saja D2 (*digest* yang diperoleh dari dokumen). Langkah terakhir kita bandingkan D1 dan D2, keduanya harus sama.

3. Pembahasan

3.1. Modul Teori Kriptografi Metoda GOST

Modul ini berisi teori-teori mengenai kriptografi metoda GOST. Modul ini dibagi menjadi 4 bagian, yaitu :

1. Teori Kriptografi Metoda GOST.
   Pada modul ini dijelaskan mengenai komponen dasar dan operasi-operasi yang digunakan pada metoda GOST.
2. Teori Proses Pembentukan Kunci.
   Pada modul ini dijelaskan mengenai proses pembentukan kunci pada metoda GOST.
3. Teori Proses Enkripsi.
   Pada modul ini dijelaskan mengenai proses kerja dari algoritma enkripsi, S-Box dan urutan kunci yang digunakan dalam proses enkripsi pada metoda GOST.
4. Teori Proses Dekripsi.

Pada modul ini dijelaskan mengenai proses kerja dari algoritma dekripsi dan urutan kunci yang digunakan dalam proses dekripsi pada metoda GOST.

3.2. Modul tentang Penjelasan Proses Pembentukan Kunci

Proses pembentukan kunci ini memerlukan *input data key* dengan panjang 256 bit atau 64 digit heksadesimal atau 32 buah karakter.

3.3. Modul tentang Penjelasan Proses Enkripsi

Proses enkripsi dari metoda GOST memproses input data *plaintext* 64 bit atau 16 digit heksadesimal atau 8 karakter dengan melalui 32 tahapan iterasi (putaran).

3.4. Modul tentang Penjelasan Proses Dekripsi

Proses dekripsi merupakan kebalikan dari proses enkripsi. Proses dekripsi dari metoda GOST menggunakan algoritma yang sama dengan proses enkripsi.

4. Pembahasan

4.1. Algoritma

Algoritma perancangan perangkat lunak pembelajaran kriptografi metoda GOST dibagi menjadi 4 bagian yaitu,

1. Algoritma Proses Pembentukan Kunci.
2. Algoritma Proses Enkripsi.
3. Algoritma Proses Dekripsi.
4. Algoritma Tampilan Proses Pembentukan Kunci.
5. Algoritma Tampilan Proses Enkripsi dan Dekripsi.

4.1.1 Algoritma Proses Pembentukan Kunci

Algoritma ini digunakan dalam proses enkripsi dan dekripsi, maka penulis merancang algoritma ini di dalam fungsi proses enkripsi dan dekripsi.

4.2. Implementasi Sistem

Implementasi sistem program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*).

Perangkat lunak ini direkomendasikan untuk dijalankan dengan menggunakan perangkat keras (*hardware*) yang mempunyai spesifikasi berikut :

1. Prosesor *Intel Pentium* IV 2.0 Ghz ke atas.
2. *Memory* 64 MB.
3. VGA *card* 1 MB.
4. Monitor dengan resolusi 800 × 600 *pixel*.
5. *Keyboard* dan *Mouse*

5. Kesimpulan

Setelah selesai menyusun tugas akhir ini, penulis menarik kesimpulan sebagai berikut:

1. Pembuatan modul pembelajaran kriptografi metoda GOST memerlukan dua komponen penting yaitu *MSFlexGrid* (*Microsoft FlexGrid*) yang digunakan sebagai tabel dan *Common Dialog Control* yang digunakan untuk membuka kotak dialog *Open* atau *Save*.
2. Perangkat lunak ini dapat membantu pemahaman cara kerja atau algoritma kriptografi khususnya metoda GOST.
3. Proses pembentukan kunci pada metoda GOST sangat sederhana sedangkan proses enkripsi dan dekripsi cukup panjang dan rumit.

Daftar Pustaka

A. Menezes, P. van, Oorschot, and S. Vanstone. 1997. Handbook of Applied Cryptography. USA: CRC Press, Inc.

Ariyus, Dony. 2006. Komputer Security. Yogyakarta: ANDI.

Bishop, Matt. 2005. Introduction to Computer Security. Boston: Pearson Eduction, Inc.

Cox, Ingemar J. 2008. Digital Watermarking and Steganography. USA: Morgan Kaufmann Publications.

Kurniawan, Yusuf. 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Cetakan Pertama. Bandung: Informatika Bandung.

Marcus, Teddy & CS. 2005. _Pemrograman Delphi dengan ADO Express. Bandung: Informatika.

Munir, Rinaldi. 2006. Kriptografy. Bandung: Informatika.

Rhee, Man Young. 1994. Crytography and Secure Communications. Korea: McGraw-Hill Book Co.

Richard M. Low, Mark Stamp. 2007. Applied Cryptanalysis Breaking Ciphers in the Real World. USA: John Wiley & Sons, Inc.