TIN: Terapan Informatika Nusantara
Vol 1, No 9, Februari 2021, Hal 445-450
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Penerapan Metode Gost Untuk Mendeteksi Keaslian File Dokumen

Lia Anggriani

Program Studi Teknik Informatika, Universitas BUDI DARMA, Medan, Indonesia
Email:liaanggriani803@gmail.com

Abstark−Manusia memiliki kemampuan untuk dapat mendeteksi keaslian *file* dokumen. Kemampuan ini akan sangat berguna bila diterapkan dalam pada mesin seperti komputer. Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma GOST(*Gosudarstennyi Standart* atau sering disebut *Goverment Standard*. Metode gost merupakan suatu algoritma blok *cipher* yang dikembangkan oleh seoarang berkebangsaan *Uni Soviet*. Kriptografi GOST merupakan blok *cipher* 64 bit dengan panjang kunci 256 bit, Algoritma ini mengiterasi algoritma enkripsi sederhana sebanyak 32 putaran (*round*), untuk menginkripsi pertama-tama *plaintext* 64 bit dipecah menjadi 32 bit bagian kiri, L dan 32 bit bagian kanan R. Subkunci (i) untuk putaran i adalah K pada satu putaran ke-i operasinya adalah sebagai berikut. Perancangan adalah suatu proses yang bertujuan untuk menganalisis, menilai, memperbaiki, dan menyusun suatu sistem, baik sistem fisik maupun non fisik yang optimum untuk waktu yang akan datang dengan memanfaatkan informasi yang ada. Perancangan adalah proses pengembangan spesifikasi sistem baru yang berdasarkan rekomendasi analisis sistem. Aplikasi merupakan program yang berisikan perintah-perintah untuk melakukan pengolahan data. Aplikasi secara umum yaitu suatu proses dari manual yang di informasikan ke komputer dengan membuat sistem atau program agar lebih berdaya guna secara optimal.

Kata Kunci: Metode Gost; Perancangan; Aplikasi.

Abstract−Humans have the ability to be able to detect the authenticity of document files. This capability will be very useful when applied to machines such as computers. The purpose of this research is to implement the GOST algorithm (Gosudarstennyi Standard or often called the Government Standard. The gost method is a block cipher algorithm developed by a national of the USSR. GOST cryptography is a 64-bit block cipher with a key length of 256 bits. This algorithm iterates over the algorithm. simple encryption of 32 rounds (round), to encrypt the 64-bit plaintext first broken down into 32 bits on the left, L and 32 bits on the right R. Design is a process that aims to analyze, assess, improve, and compile a system, both physical and non-physical systems that are optimal for the future by utilizing existing information Design is the process of developing a new system specification based on analysis recommendations system.Application is a noisy program n commands to perform data processing. Application in general is a manual process that is informed to the computer by creating a system or program to make it more optimally efficient.

Keywords: Gost Method; Design; Application

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi tidak hanya membawa dampak positif, tetapi juga membawa dampak negatif, salah satunya adalah tindakan plagiarisme. Plagiarisme dalam Kamus Besar Bahasa Indonesia (KBBI) adalah penjiplakan atau pengambilan karangan (pendapat dan sebagainya) orang lain dan menjadikannya seolah-olah karangan (pendapat dan sebagainya) sendiri.

Plagiarisme adalah suatu kejahatan akademik (*academic criminal*) dan aib yang sangat tidak mudah terhapuskan. Di kalangan mahasiswa dan kehidupan sehari-hari kegiatan plagiarisme sering ditemukan dalam makalah, bahkan skripsi, dan surat-surat penting seperti surat tanah, surat warisan dan lain-lain. Untuk mengatasi hal tersebut, maka perlu adanya suatu aplikasi komputer yang dapat mendeteksi keaslian *file* dokumen agar dapat mengurangi tindakan plagiarisme.

Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga keaslian data, Data penting dan vital yang tersimpan pada basis data seringkali menjadi target empuk bagi para penyerang, serangan yang terjadi dapat dilakukan oleh pihak luar (*hacker*) maupun pihak dalam (pegawai yang tidak puas).

File dokumen merupakan komponen yang sangat vital, sehingga memerlukan pengaman yang baik saat didistribusi ataupun saat disimpan atau untuk mendeteksi keaslian *file* dokumen. Kemudahan memperoleh informasi berdampak pada kemungkinan terjadinya praktik plagiat dalam dunia pendidikan. Pencegahan praktik plagiat merupakan suatu kebutuhan yang sangat penting dilakukan untuk menjamin kualitas intansi pendidikan.

Perancangan Aplikasi adalah konsep merancang merupakan aplikasi yang akan dibuat. Untuk dapat merancang konsep dalam bentuk membuat aplikasi dibutuhkan kreatifitas. Kreatifitas adalah kemampuan untuk menyajikan gagasan atau ide baru. Perancangan adalah penggambaran, perancangan dari pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh.

Metode *GOST (Gosudarstvenny Standard)* merupakan suatu algoritma *block cipher* yang dikembangkan oleh seorang berkebangsaan *Uni Soviet*. Metode ini dikembangkan oleh pemerintah *Uni Soviet* pada masa perang dingin untuk menyembunyikan data atau informasi yang bersifat rahasia pada saat komunikasi, sehingga dengan menerapkan metode *GOST* pada perancangan aplikasi mendeteksi keaslian *file* dokumen.

Oleh karena itu dibutuhkan suatu sistem yang terkomputerisasi sehingga dapat membantu pemeriksaan tingkat keaslian *file* dokumen dengan waktu yang lebih cepat. Melihat kendala tersebut, penulis berusaha untuk membuat suatu sistem untuk mendeteksi tingkat keaslian *file* dokumen. Untuk mengatasi persoalan mengetahui keaslian *file* dokumen yang pada intinya adalah cara mengantisipasi agar pihak-pihak yang tidak berhak, tidak mungkin dapat membaca atau bahkan merusak data yang bukan ditujukan padanya. Salah satu cara mendeteksi keaslian *file* dokumen tersebut adalah dengan merancang aplikasi menggunakan metode *GOST*.

TIN: Terapan Informatika Nusantara
Vol 1, No 9, Februari 2021, Hal 445-450
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

2. METODOLOGI PENELITIAN

2.1 Perancangan

Perancangan adalah suatu proses yang bertujuan untuk menganalisis, menilai, memperbaiki, dan menyusun suatu sistem, baik sistem fisik maupun non fisik yang optimum untuk waktu yang akan datang dengan memanfaatkan informasi yang ada. Perancangan adalah proses pengembangan spesifikasi sistem baru yang berdasarkan rekomendasi analisis sistem .

2.2 Aplikasi

Aplikasi merupakan program yang dikembangkan untuk memenuhi kebutuhan pengguna dalam menjalankan pekerjaan tertentu. Aplikasi merupakan sebuah program yang dibuat dalam sebuah perangkat lunak dengan komputer untuk memudahkan pekerjaan atau tugas-tugas seperti penerapan, penggunaan dan penambahan data yang dibutuhkan, contoh-contoh aplikasi adalah program pemroses kata dan *web browser.* Aplikasi akan menggunakan sistem operasi (OS) komputer dan aplikasi yang lainnya yang mendukung secara historis. Aplikasi merupakan program yang berisikan perintah-perintah untuk melakukan pengolahan data. Aplikasi secara umum yaitu suatu proses dari manual yang di informasikan ke komputer dengan membuat sistem atau program agar lebih berdaya guna secara optimal.

Berdasarkan defenisinya aplikasi dapat disimpulkan bahwa aplikasi adalah suatu perangkat lunak komputer yang memanfaatkan keamanan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna. Berdasarkan pembahasan diatas dapat disimpulkan bahwa aplikasi adalah suatu bentuk sistem yang membantu pekerjaan manusia, program siap pakai yang dapat digunakan untuk menjalankan perintah-perintah atau melakukan berbagai bentuk pekerjaan atau tugas-tugas tertentu seperti penerapan, penggunaan, dan pembahasan data.

2.3 Deteksi

Deteksi adalah suatu proses untuk memeriksa atau melakukan pemeriksaan terhadap sesuatu dengan menggunakan cara dan teknik tertentu. Deteksi dapat digunakan untuk berbagai masalah, misalnya dalam sistem pendeteksi suatu *file*, dimana sistem mengidentifikasi masalah-masalah yang berhubungan dengan *file* yang biasa disebut plagiat.

2.4 *File*

File adalah kumpulan dari kata dan juga informasi yang saling berhubungan dan juga tersimpan di dalam ruang penyimpan sekunder. Defenisi *file* dapat juga diartikan sebagai arsip atau data yang tersimpan di dalam komputer. Secara konsep *file* memiliki beberapa tipe, diantaranya adalah tipe data terdiri dari *character*, *numerik*, dan *binari.* Selain itu ada juga *file* yang bertipe program. Pada umumnya *file* pada komputer tersimpan di dalam folder tertentu, tergantung dimana si pemilik *file* ingin menyimpannya. Masing-masing *file* memiliki ektensi yang berbeda sesuai dengan jenis *file*nya. Pengertian ekstensi *file* adalah tanda yang membedakan antar satu jenis *file* dengan jenis *file* lainnya. Misalnya, *file* gambar akan memiliki ekstensi jpg, gif, png, dan lain-lain. Sedangkan untuk *file* video akan memiliki ekstensia mpeg, avi, mp4, wmv, dan lain-lain.Pengertian *file* adalah koleksi rekaman (*record*) yang saling berhubungan satu dengan yang lainnya, seperti satu *file* dari seluruh record yang berisi bidang kode-kode mata kuliah dan namanya Menurut. Pengertian *file* adalah urutan data yang digunakan untuk melakukan *encode* informasi digital yang berguna dalam hal pertukaran dan penyimpanan data.

2.5 Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu dari kata crypto dan graphia yang berarti ‘Penulisan rahasia’. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (*crytology*). Criptografi bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem infromasi seperti kerahasiaan, integritas data, autentikasi, dan ketiadaan penyangkaan. Keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi.

3. HASIL DAN PEMBAHASAN

Keaslian *file* dokumen yang bersifat rahasia rentan terhadap penyadapan dengan menyalurkan *file* asli ke internet. Menyalurkan keaslian *file* dokumen dengan bantuan media internet memiliki aspek penting yang harus diperhatikan oleh pengirim dan penerima *file* yaitu aspek keamanan *file* tersebut. Apabila *file* tersebut jatuh ke pihak yang tidak memiliki otoritas, maka dapat merugikan salah satu pihak pengirim. Masalah Keamanan *file* merupakan suatu hal yang sangat penting yang harus dijaga keasliannya. Ada beberapa cara dalam menjaga keaslian *file* dokumen agar tidak dicuri dan disalahgunakan oleh orang yang tidak bertanggung jawab, salah satunya adalah dengan teknik kriptografi.

Pengujian dalam mendeteksi keaslian *file* dokumen sangat diperlukan karena dengan adanya pengujian kita dapat mengetahui hasil dari perbedaan dari *file* dokumen yang akan diuji merupakan hasil dari pembentukan kode fungsi *Hash*

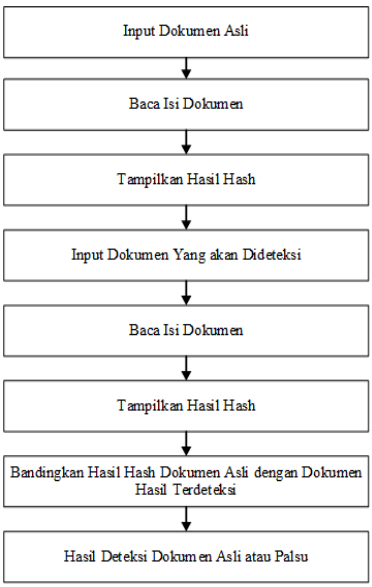
Pemalsuan merupakan suatu tindakan modifikasi dokumen, produk, gambar, atau video, di antara media lain. Dokumen yang sangat mudah di edit dan dipalsukan ini membuat banyak para oknum yang tidak bertanggung jawab

TIN: Terapan Informatika Nusantara
Vol 1, No 9, Februari 2021, Hal 445-450
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

merusak keaslian *doc*, dan menyebar *file* dokumen ke media sosial hingga informasi atau pesan pada *file* dokumen bisa berubah keasliannya. Dari latar belakang inilah peneliti mengambil penelitian ini yaitu mendeteksi keaslian *file* dokumen.

Contoh kasus proses hitungan manual dalam enkripsi menggunakan algoritma GOST. Proses pertama adalah menyiapkan *plaintex*t untuk enkripsi menggunakan algoritma GOST. Kemudian menyiapkan sebuah dokumen *doc* yang akan dideteksi keasliannya. Adapun proses pendeteksian keaslian *file* dokumen *doc* berdasarkan kriptografi disajikan pada gambar dibawah ini :

File dokumen yang akan di deteksi keasliannya yaitu *file* dokumen berformat *doc*. Berikut merupakan prosedur pendeteksian keaslian *file* dokumen *doc.*



Gambar 1. Diagram Proses Hashing

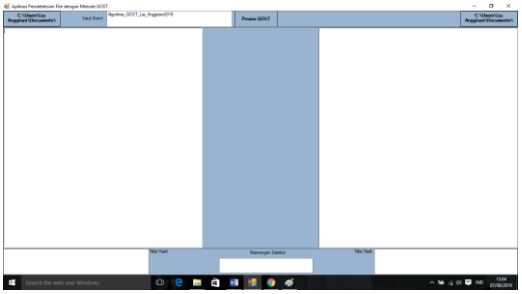
3.1 Pengujian Dokumen

Berikut merupakan contoh dokumen yang akan dilakukan pengujian dalam pemerosekan deteksi keaslian *file* dokumen.

Gambar 2. Dokumen Uji

3.2 Pengujian Sistem

Aplikasi pengujian metode *GOST* untuk mendeteksi keaslian *file* dokumen yang akan diuji merupakan hasil dari pembentukan kode fungsi *Hash* dengan menerapkan metode *GOST* yang digunakan. Berikut hasil dari implementasi metode *GOST* untuk mendeteksi keaslian *file* dokumen dengan menggunakan aplikasi *Microsoft Visual Studio 2008* seperti gambar 2:

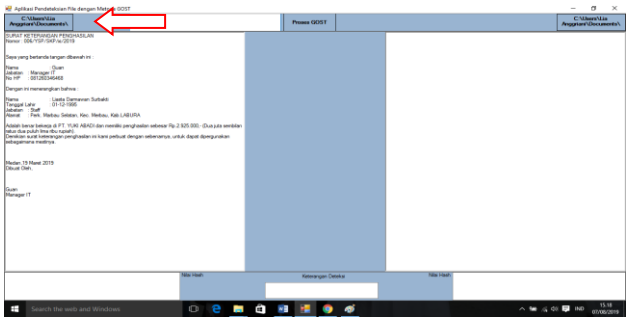


Gambar 3. Aplikasi *Microsoft Visual Studio 2008*

TIN: Terapan Informatika Nusantara
Vol 1, No 9, Februari 2021, Hal 445-450
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

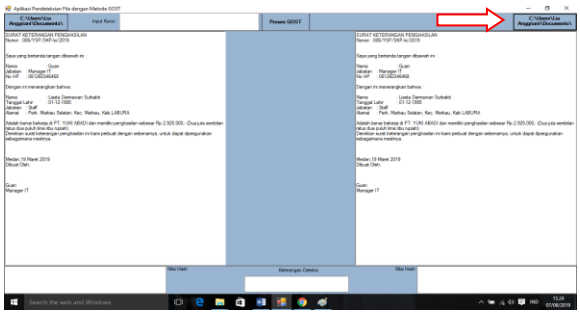
Pada Form aplikasi *Microsoft Visual Studio 2008* terdapat beberapa langkah-langkah yang dapat dilakukan oleh user untuk menjalankan pengujian implementasi metode *GOST* sebagai berikut :

1. Menginputkan *File* Dokumen Asli
   Menginputkan *file* dokumen adalah proses dimana memanggil file dokumen yang akan dicari nilai *Hash* seperti tampilan gambar 3 :



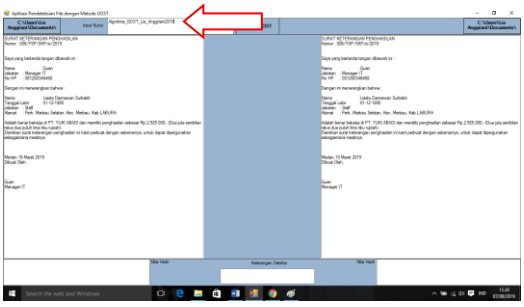
Gambar 4. Menginputkan Dokumen Asli

2. Menginputkan File Dokumen Uji
   Menginputkan *file* dokumen Uji adalah proses dimana memanggil file dokumen yang akan dicari nilai *Hash* seperti tampilan gambar 4 :



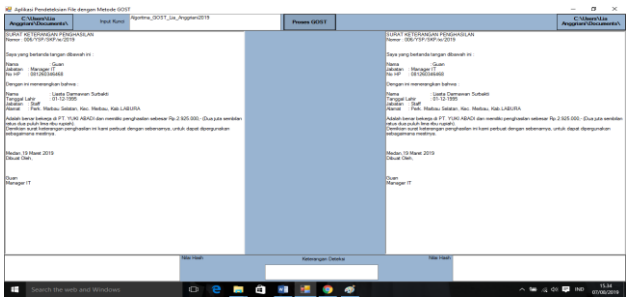
Gambar 5. *File* Dokumen Uji

3. Menginputkan Kunci
   Menginputkan kunci adalah proses dimana untuk mengetahui hasil *file* tersebut asli atau palsu seperti tampilan gambar 5 :



Gambar 6. Menginputkan Kunci

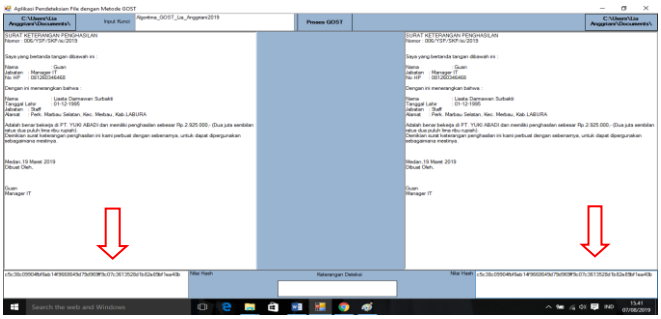
4. Memilih Tombol Proses *GOST*
   Memilih tombol proses *GOST* adalah proses dimana menentukan hasil *hash file* dokumen asli atau palsu seperti gambar 6 :



Gambar 7. Tombol Proses *GOS*

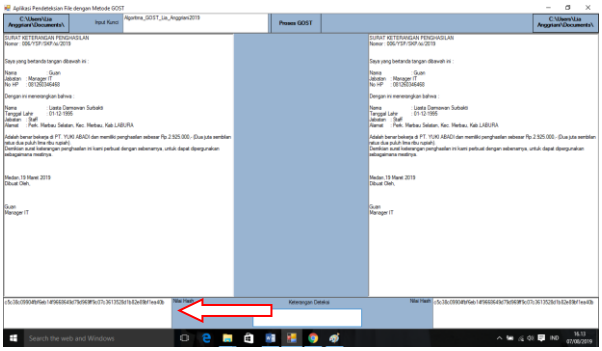
TIN: Terapan Informatika Nusantara
Vol 1, No 9, Februari 2021, Hal 445-450
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

5. Tampilan Nilai *Hash File* Dokumen
   Tampilan nilai *Hash file* dokumen adalah menampilkan nilai *Hash* jika nilai *Hash* sama maka dokumen yang di uji keasliannya Asli, dan Jika nilai *Hash* berbeda maka *file* Tesebut palsu seperti gambar 7 :



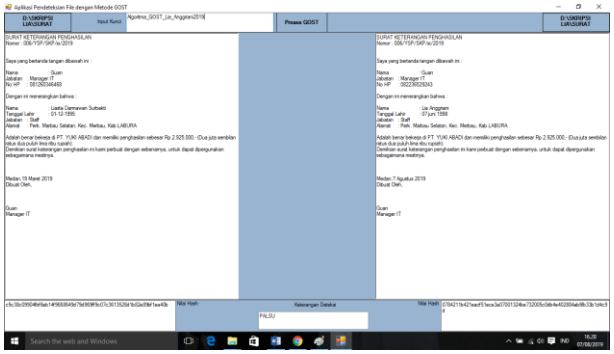
Gambar 8. Tampilan Nilai *Hash File* Dokumen

6. Tampilan Keterangan Deteksi
   Tampilan keterangan deteksi adalah tampilan akhir proses deteksi keaslian file dokumen seperti **gambar 8** :



Gambar 9. Tampilan Keterangan Deteksi

7. Tampilan *File* Dokumen Palsu
   Berikut tampilan *file* dokumen palsu yang telah di edit atau dimanipulasi, saat di inputkan kunci *GOST* dan diproses nilai *Hash* berbeda sehingga dapat dikatakan bahwa *file* tersebut palsu seperti gambar 9 :



Gambar 10. Tampilan *File* Dokumen Palsu

4. KESIMPULAN

Berdasarkan dari penelitian yang telah dilakukan dapat disimpulkan penerapan algoritma *GOST* telah membuktikan bahwa suatu *file* yang dapat dideteksi keasliannya dengan membandingkan hasil *Hash*. Aplikasi file dokumen dapat dirancang dan dibangun dengan menggunakan aplikasi *Microsoft Visual Studio 2008* dengan menerapkan Algoritma *GOST* sehingga memudahkan penulis melakukan pengujian mendeteksi keaslian *file* dokumen.

REFERENCES

[1] S. Emy Setyaningsih, Kriptografi & implementasinya menggunakan matlap, Yogyakarta: ANDI, 2015.
[2] Schneir, "Pengamanan basis data sistem penjualan dengan menggunakan teknik enkripsi kriptografi," *Jurnal Teknologi Informasi dan Komunikasi*, no. 6, pp. 2252-4517, 2018.
[3] Sarineen, "Pengamanan basis data sistem penjualan dengan menggunakan teknik enkripsi kriptografi gost," *Jurnal teknologi informasi dan komunikasi* , no. 6, pp. 2252-4517, 2018.

[4] Kahn, "Pengamanan Basis Data Sistem Penjualan dengan Menggunakan Teknik Enkripsi Kriptografi Gost," *Jurnal Teknologi Informasi dan Komunikasi*, no. 4, pp. 2252-4517, 2018.
[5] d. Bendict Marthin, "Pengamanan basis data sistem penjualan dengan menggunakan teknik enkripsi kriptografi gost," *Jurnal Teknologi Informasi dan Komunikasi*, no. 4, pp. 2252-4517, 2018.