Pemanfaatan Kriptografi AES dan SHA Untuk Pengamanan Surat Kedinasan Pada Kantor Pemerintahan Kabupaten / Kota Bandung

Utilization of AES and SHA Cryptography for Security of Letters of Service in Bandung Regency / Municipal Government Office

Muhammad Barja Sanjaya[1]
[1] Diploma 3 Manajemen Informatika
Fakultas Ilmu Terapan, Universitas Telkom
Bandung 40257, Jawa Barat, Indonesia
Email : mbarja@tass.telkomuniversity.ac.id

Abstrak – Surat kedinasan merupakan suatu wadah dan media untuk mempertukarkan data atau pesan yang dilakukan oleh pegawai di suatu kantor atau instansi pemerintahan. Seiring berkembangnya zaman, mekanisme pengiriman surat kedinasan juga melibatkan pemanfaatan teknologi internet sehingga proses pengiriman menjadi lebih cepat. Namun, belum adanya bentuk pengamanan terhadap isi dari pesan tersebut dapat memicu atau pun berdampak buruk terhadap internal instansi. Oleh karena itu, diusulkan adanya standardisasi mekanisme pengiriman surat yakni pengamanan pada *file* surat kedinasan yang akan dikirimkan tersebut berupa penyandian data dengan metode kriptografi *Advanced Encryption Standard* (AES). Adapun metode kriptografi biasa saat ini sudah diragukan lagi ketika ingin diterapkan meski jumlah *bit* kunci yang digunakan ditingkatkan. Diperlukan pembaharuan berupa kombinasi antara AES dengan fungsi hash *Secure Hash Algorithm* (SHA) sehingga *file* dokumen surat kedinasan yang akan dikirimkan tetap terlindungi dari akses ilegal.

Kata kunci *:* pengamanan, surat kedinasan, AES, SHA, akses ilegal.

Abstract *– Official letter is one of medium to exchange data or message between employees in government office. Today the mechanism of sending official letters have already involved internet technology so that it takes faster in sending the letter. However, there is still no protection to the letter that other party can access illegally. That's why it is proposed a new method as standardization in mechanism of sending official letter such as a secure to letter which will be sent by using cryptography Advanced Encryption Standard (AES). As for the ordinary AES has been already not considered as secured since more researches concern AES performances were conducted even though it has been already given additional bit in key length. It is so indeed necessary to modify AES by combining to Secure Hash Algorithm (SHA) that the official letter is in secured against illegal access*.

Keyword : *protection, official letter, AES, SHA, illegal access.*

I. PENDAHULUAN

Perkembangan internet dewasa ini sungguh kian pesat dan sudah merasuki ke segala bidang atau disiplin ilmu. Salah satunya yakni disiplin ilmu sosial atau pun kedinasan di suatu kantor pemerintahan dalam negeri. Dalam kesehariannya, banyak karyawan di kantor dinas pemerintahan dalam negeri tersebut berinteraksi dan beroperasi dengan teknologi internet yang dimuat dalam komputer. Beragam aktivitas terkait dengan teknologi internet dilakukan di semua kalangan di instansi tersebut. Dalam hal surat menyurat pun yang dilakukan oleh karyawan untuk domain internal atau pun untuk eksternal juga didukung dengan memanfaatkan teknologi internet dan komputer. Namun, hal tersebut dinilai masih belum optimal dalam memanfaatkan teknologi.

Hal ini bisa dilihat pada konten surat yang mestinya perlu dirahasiakan mengenai isi pesan ditujukan untuk siapa saja yang diperbolehkan atau pun diizinkan untuk mengakses surat tersebut [1][2]. Dan terlebih, dikhawatirkan adanya pengubahan isi pesan pada surat yang akan dikirimkan sehingga tingkat integritas dari data pesan yang ada pada surat tersebut sudah hilang atau berkurang. Hal tersebut bisa saja dan sangat memungkinkan terjadi di kalangan instansi pemerintahan dikarenakan belum adanya suatu standarisasi yang jelas dan dimengerti karyawan satu dengan lainnya sehingga dapat berakibat fatal jika isi surat bisa dibaca atau diakses oleh pihak yang tidak ada wewenang terkait. Sangatlah jelas jika hal ini dibiarkan dan tidak segera ditindak-lanjuti untuk segera membuat suatu standarisasi mengenai mekanisme pengiriman surat kedinasan tersebut dapat berakibat fatal pada instansi. Sehingga dengan adanya batasan hak akses tersebut diharapkan bisa meminimalisir adanya kesimpang-siuran atau ketidak-jelasan informasi bilamana terjadi hal-hal yang tidak diinginkan [3].

Oleh karena itu, pada penelitian ini diusulkan suatu standarisasi pada mekanisme pengiriman surat kedinasan pada instansi pemerintahan yakni dengan menerapkan atau mengimplementasikan kriptografi *Advanced Encryption Standard* (AES) yang dikombinasikan dengan *Secure Hash Algorithm* (SHA)

pada file surat kedinasan yang dimaksud. Adannya dukungan kombinasi ini dikarenakan AES sudah diragukan lagi untuk diimplementasikan meskipun panjang *bit* kunci ditingkatkan [7]. Sehingga integritas pesan pada surat tersebut dapat dipertahankan dan hanya bisa diakses oleh pihak yang berwenang. Dengan adanya pemanfaatan penerapan kriptografi AES dan SHA ini diharapkan level integritas data surat dan level keamanannya juga terlindungi dari pihak-pihak yang tidak berwenang atau terkait.

II. DASAR TEORI

Berikut dasar teori pendukung yang disertakan dalam penelitian ini, diantaranya: *Advanced Encryption Standard*, *Secure Hash Algorithm*, Blum Blum Shub, dan Surat Dinas Kelembagaan.

A. Kriptografi *Advanced Encryption Standard*

Advanced Encryption Standard (AES) merupakan salah satu metode kriptografi simetrik yakni menggunakan kunci yang sama dalam hal proses penyandian data yang dilakukan oleh pihak penerima atau pun pengirim. AES melibatkan empat proses utama di dalam memproses komputasi enkripsi maupun dekripsinya, yakni : *Key Scheduling* (*Add Round Key*), *Sub Byte Transformation*, *Shift Rows*, dan *Mix Column*.

Proses *Key Scheduling* merupakan proses yang memperbaharui kunci yang digunakan di tiap iterasi proses komputasi dan juga menjamin kunci yang dihasilkan berbeda antara satu dengan yang lainnya. Juga dengan adanya proses penjadwalan kunci ini menjamin tidak adanya pola yang bisa dievaluasi pada deretan kunci-kunci yang digunakan di proses enkripsi. Proses berikutnya yakni *Sub Byte* yakni mentransformasikan *byte* isi pesan atau informasi yang menjadi plainteks ke bentuk matriks berukuran 4x4. Pada proses ini dilakukan transfomasi namun mengacu pada tabel Sbox yang telah ditentukan. Isi pada tabel Sbox tersebut sudah dilakukan kalkulasi dan telah memenuhi kriteria saling relatif prima antara satu data dengan data lainnya. Sub proses ketiga yakni *Shift Rows* merupakan proses menggeser baris per baris di plainteks yang telah dikonversi ke dalam bentuk matriks berukuran 4x4. Sedangkan pada sub proses *Mix* Column, dilakukan penggeseran kolom demi kolom pada plainteks.

Menurut NIST [**7**] dijelaskan bahwa AES masih bisa diimplementasikan sebagai salah satu metode penyandian data untuk mengamankan serta memproteksi konten dengan catatan panjang kunci yang digunakan minimal 256 *bit*. AES juga masih menjadi kandidat pilihan utama di beberapa instansi dikarenakan karena proses komputasinya masih memakan konsumsi *memory* yang minimum dan proses komputasi yang relatif lebih cepat dibandingkan dengan kriptografi asimetrik [**5**].

B. Kriptografi *Secure Hash Algorithm*

Selain kriptografi simetrik juga fungsi satu arah yakni *Secure Hash Algorithm* (SHA) dilibatkan pada proses komputasi yang diusulkan. SHA menjamin salah satu indikator pada kriptografi yakni pada poin keutuhan atau integritas data. SHA hanya bersifat satu arah maksudnya hanya bisa menyandi saja tanpa bisa didekrip menjadi data asli (plainteks) kembali. SHA akan digunakan untuk menyandikan kunci yang dihasilkan dari proses *random number* dengan BBS sehingga keotentikan *bit-bit* yang digunakan pun terjamin [**6**]. *Bit-bit* yang dihasilkan tersebut akan dilakukan proses *hashing* menjadi *byte* kunci untuk digunakan di proses enkripsi dengan kriptografi AES.

C. *Random Number* Blum-Blum-Shub

Random number merupakan salah satu ciri khas yang sering dijumpai di ilmu sains terapan. *Random number* berguna untuk menghasilkan *bit-bit* arus yang akan dilibatkan di proses awal sebagai tahap inisialisasi yang bisa dihasilkan dari proses komputasi persamaan aritmatika atau aljabar. Salah satu *random number generator* yakni Blum Blum Shub (BBS) dengan persamaan khasnya yang menyertakan operasi modulo pada deret polinomial dengan derajat kuadrat. Adapun persamaan aljabar dari BBS adalah sebagai berikut:

$$X_{n+1} = X_n^2 \textbf{ mod } m \qquad (1)$$

Variabel X menyatakan nilai *byte random number* ke sekian sedangkan variabel m merupakan perkalian dua bilangan *integer* positif (misal bilangan p dan q) dan tak nol serta memenuhi kriteria kongruen terhadap nilai dari kalkulasi aritmatika 3 modulo 4 [4].

D. Surat Dinas Kelembagaan

Surat dinas merupakan salah satu media yang digunakan untuk kepentingan pekerjaan formal pada suatu instansi atau pun institusi. Surat dinas seringkali digunakan untuk memberikan instruksi, berisi undangan atau pun hal lain terkait di kelembagaan instansi. Berbagai macam kegunaan surat dinas diantaranya: sebagai dokumen bukti tertulis, alat pengingat, sebagai bukti sejarah atas perkembangan instansi, atau bisa juga sebagai pedoman kerja dalam bentuk surat perintah [**8**].

III. HASIL DAN PEMBAHASAN

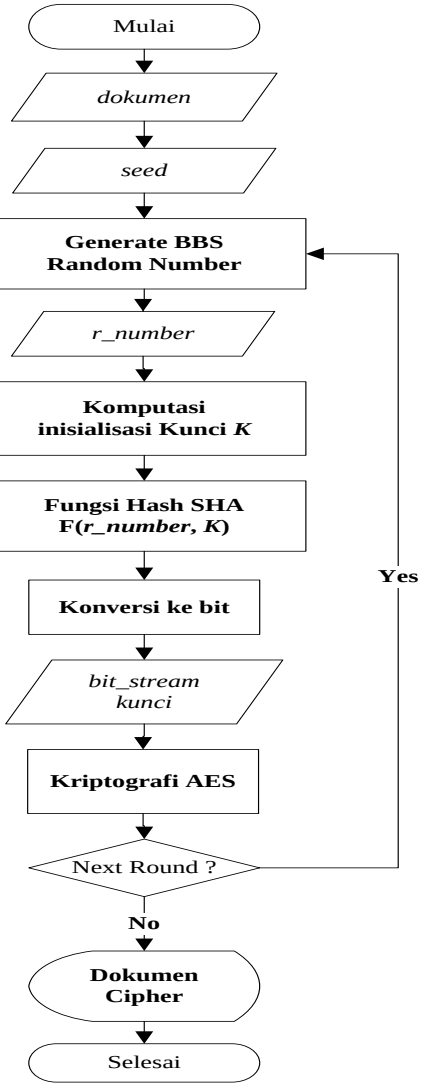
Berikut dijelaskan mengenai metode usulan dan hasil pengujian pada sistem.

1. **Metodologi usulan**

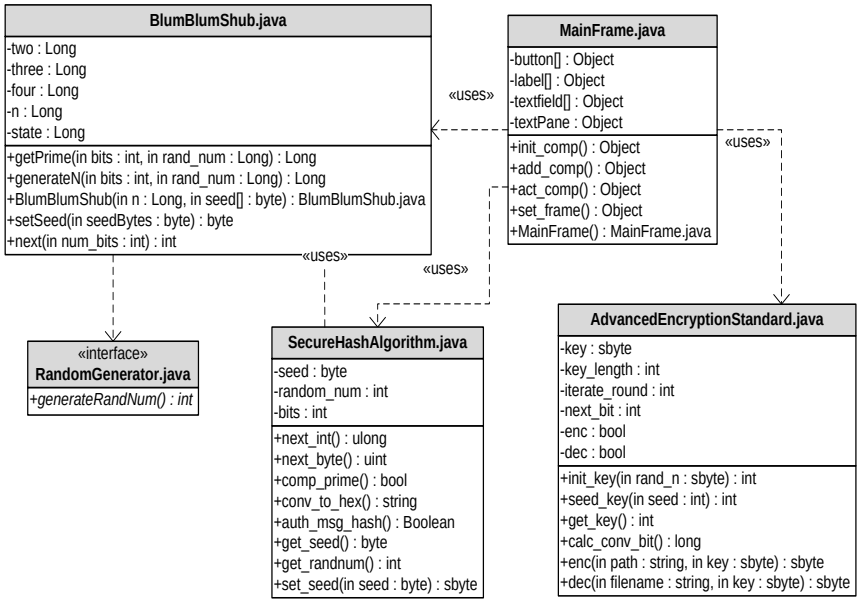
   Adapun perancangan sistem yang diusulkan dimodelkan pada diagram sebagai berikut:

   a. *Flowchart*

      Gambar 1 menunjukkan deskripsi *flowchart* sistem



Gambar 1. *Flowchart* sistem usulan



Gambar 2. Diagram class sistem

Keterangan flowchart:

1. Input dokumen
2. Input nilai awal kunci, berupa *seed*. Bilangan *seed* didefinisikan di domain *integer* positif dan tak nol.
3. Lakukan komputasi *random number generator* Blum-Blum-Shub (BBS) untuk menghasilkan bilangan *r_number*.
4. Lakukan proses inisialisasi kunci di tiap ronde yang akan digunakan untuk proses Hash.
5. Lakukan konversi dari hasil Hash ke dalam deretan *bit* yang bisa disebut arus *bit*.
6. Lakukan kriptografi AES untuk mengenkripsi dokumen
7. Lakukan di iterasi atau putaran berikutnya. Jika masih ada iterasi proses yang akan dilakukan, maka lakukan proses ke-3. Jika sudah selesai untuk semua iterasi proses, maka lakukan proses ke-8.
8. Tampilkan hasil dokumen yang sudah dienkrip. Adapun dokumen yang telah dilindungi dengan enkripsi AES disebut dengan dokumen *cipher*. Untuk proses dekripsi sama dengan proses enkripsi dan AES menggunakan kunci yang sama untuk melakukan proses enkripsi atau pun dekripsi serta urutan proses yang sama juga pada rancangan usulan di penelitian.

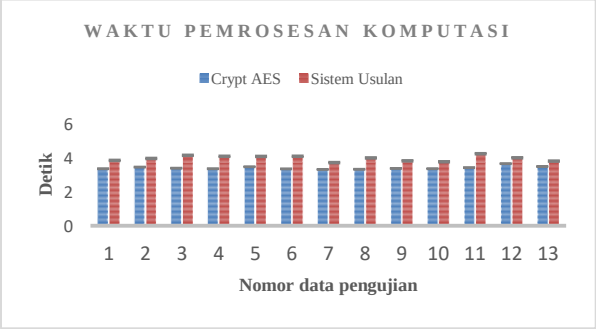
b. Diagram class
Untuk perancangan diagram *class*-nya, ditunjukkan pada **Gambar 2**.

Pada sistem yang diusulkan di penelitian ini, dibutuhkan *file class* dengan format ekstensi (*dot*) java antara lain: *class Advanced Encryption Standard* sebagai implementasi metode kriptografi simetrik dan *Secure Hash Algorithm* untuk kriptografi satu arah. Sedangkan *Blum Blum Shub* diperlukan untuk menghasilkan *bit-bit* secara acak. Serta, terdapat satu *file interface* yakni *Random Generator* yang memiliki satu *method* generateRandNum() untuk dilakukan polimorfisme *overriding* di *class* Blum Blum Shub.

2. **Hasil pengujian dan pembahasan**

Adapun hasil pengujian yang dilakukan difokuskan tidak hanya pada *cipher* yang telah dihasilkan, namun juga pada perfomansi yang dihasilkan dari komputasi yang telah dilangsungkan pada saat pengujian sistem. Performansi yang dimaksud antara lain waktu proses komputasi dan konsumsi daya *memory* yang diperlukan. Kedua hal ini menjadi penting dan utama untuk menjadi sorotan perhatian dikarenakan dampak implementasi teknologi tidak hanya bisa memfasilitasi kebutuhan instansi namun juga harus tetap memenuhi performansi yang layak pada instansi tersebut.

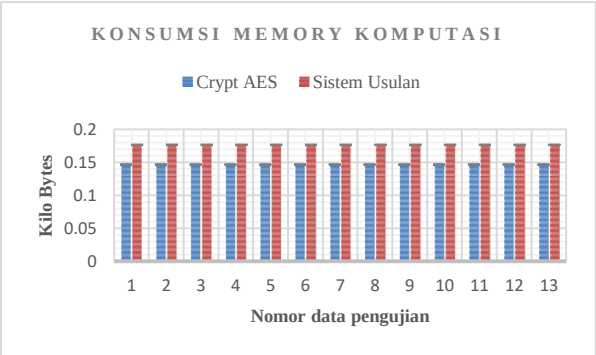
a. Waktu proses komputasi
Berikut data hasil pengujian yang telah dilakukan dan disajikan dalam bentuk grafik:



Gambar 3. Grafik perbedaan waktu proses

Pada **gambar 3** ditunjukkan bahwa waktu pemrosesan sistem usulan memang terlihat ada peningkatan atau tambahan waktu. Hal ini dikarenakan adanya proses pengecekan relatif prima atau tidak untuk kunci yang dihasilkan di tiap iterasi atau ronde pada AES. Namun rataan selisih penambahan waktu proses komputasi pada sistem usulan dengan AES yakni berkisar 0,5569485 detik dan dengan nilai standar deviasi yang minimum yakni sebesar 0,0274836 detik.

b. Konsumsi daya *memory*
Sedangkan perbandingan kebutuhan *memory* untuk memproses penyandian data selama pengujian dilakukan disajikan dalam bentuk grafik sebagai berikut:



Gambar 4. Konsumsi daya *memory*

Berdasarkan **gambar 4** mengenai kebutuhan *memory* untuk melangsungkan proses komputasi, terlihat bahwa sistem usulan membutuhkan *memory* tambahan di tiap pengujian yang telah dilakukan. Adanya peningkatan *memory* ini disebabkan pada sistem usulan menyertakan proses aritmatika untuk perhitungan kriteria relatif prima antar

kunci yang digunakan di komputasi kriptografi. Akan tetapi penambahan *memory* yang terjadi pada saat proses dilakukan masih dapat dikategorikan sangat minimum yakni sebesar 0,03 *Kilo Bytes* dan besar selisih *memory* tersebut juga memiliki nilai yang stabil di tiap pengujian yang dilakukan.

IV. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan maka dapat disimpulkan sebagai berikut:

1. Kriptografi usulan pada penelitian yang dilakukan bisa menjadi salah satu fasilitas untuk mengamankan data atau berkas dokumen di instansi atau lembaga. Terlebih, spesifikasi yang diperlukan untuk men-*deploy* tidak terlalu mahal dari segi kompleksitas waktu dan *memory* yang dibutuhkan. Berdasarkan dari data pengujian bahwa rata-rata waktu pemrosesan hanya berkisar 3,9738089 detik pada sistem usulan dan 3,4168604 detik jika menggunakan kriptografi AES.
2. Nilai standar deviasi minimum pada parameter waktu proses komputasi sebesar 0,0274836 detik juga mengindikasikan bahwa sistem usulan masih dapat diterapkan.
3. Parameter lain yang juga menjadi perhatian utama untuk menerapkan penyandian data untuk berkas yakni konsumsi daya *memory* yang dibutuhkan untuk melangsungkan proses komputasi. Berdasarkan data hasil pengujian, diperlukan waktu tambahan untuk memproses sistem usulan sebesar 0,03 *Kilo Bytes* dibandingkan jika menerapkan kriptografi AES murni. Juga adanya kestabilan pada nilai atau besarnya *memory* yang dibutuhkan di tiap pengujian yang telah dilakukan.

Pada penelitian berikutnya disarankan juga dapat menyandi data atau berkas dokumen yang telah dilakukan pemindaian. Hal ini kemungkinan besar akan membutuhkan daya *memory* tambahan dikarenakan data yang akan diproses berupa *file image* yang terdiri dari rangkaian tiga layer *Red*, *Green* dan *Blue* (RGB). Serta, parameter yang menjadi perhatian utama untuk penyandian data gambar adalah nilai *Avalenche Effect* dan Ketahanan terhadap serangan *Brute Force Attack*.

UCAPAN TERIMA KASIH

Terima kasih kepada seluruh rekan kerja di Universitas Telkom Bandung dan sahabat saya yang senantiasa telah menyemangati, khususnya kepada Adhiz Indrasari, Ibrahim Tjipta Kusuma S, dan Muhammad Aditya Pratama S. Moga kita semua tetap semangat dan menyemangati diri untuk senantiasa mendukung pendidikan di NKRI demi mencerdaskan kehidupan bangsa dan negara.

DAFTAR PUSTAKA

[1] Wardhani, Fadhila Cahya. "*Analisis Dan Perancangan Sistem Keamanan Pengiriman Dokumen: Enkripsi Dan Dekripsi Tanda Tangan Digital Menggunakan Digital Signature Algorithm* (*DSA*)". Program Studi S1 Sistem Komputer. Universitas Telkom. Bandung. 2015.

[2] Ardhiana, Riandini Rizki. "*Analisis Dan Perancangan Sistem Keamanan Pengiriman Dokumen: Enkripsi Dokumen Disisipi Tanda Tangan Digital Menggunakan International Data Encryption Algorithm (IDEA)*". Program Studi S1 Sistem Komputer. Universitas Telkom. Bandung. 2015.

[3] Siskawati, Dewi. "*Perancangan Dan Analisis Modifikasi Kunci Kriptografi Algoritma RC6 Pada Data Teks*". Program Studi S1 Sistem Komputer. Universitas Telkom. Bandung. 2015.

[4] Anggreni, Dwi N. "*Perancangan Dan Analisis Modifikasi Kunci Kriptografi Algoritma Twofish Pada Data Teks*". Program Studi S1 Sistem Komputer. Universitas Telkom. Bandung. 2015.

[5] Forouzan, Behrouz. A. 2008. "*Cryptography and Network Security*". International Edition. New York. MacGraw-Hill Companies, Inc.

[6] Menezes, A. and Van Oorschot, P. and Vanstone, S. 1997. "*Handbook of Applied Cryptography*". Florida: CRC Press Inc.

[7] J. Daemen and V. Rijmen. 2002. "*The Design of Rijndael: AES – The Advanced Encryption Standard*". Springer Verlag.

[8] Ulyani, Mara. *Buku Lengkap Aneka Surat Dinas (Buku Pilihan)*. Penerbit Flash Books. Juni 2012. ISBN: 9786027641235.

BIODATA PENULIS

Nama lengkap peneliti adalah Muhammad Barja Sanjaya, dan lebih akrab disapa dengan nama Barja. Lahir di Sumenep pada akhir tahun 1985. Memulai pendidikan Strata I di Sekolah Tinggi Teknologi Telkom, jurusan Teknik Informatika pada tahun 2004-2009, dan melanjutkan studi Strata II Teknik Informatika di Universitas Telkom pada tahun 2012-2014. Peneliti juga telah menyandang gelar OCA dari Oracle Academy pada bulan April 2017. Bidang yang menjadi konsentrasi utama peneliti yakni Algoritma, Matematika dan Keamanan Sistem dengan Teknik Kriptografi dan Steganografi. Peneliti juga mengajar mata kuliah yang berkaitan dengan disiplin ilmu pemrograman di Universitas Telkom sejak tahun 2010.