KRIPTOGRAFI VERNAM CIPHER UNTUK MENCEGAH PENCURIAN DATA PADA SEMUA EKSTENSI FILE

Eko Hari Rachmawanto[1], Christy Atika Sari[2], Yani Parti Astuti[3], Liya Umaroh[4]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Nakula I No. 5-11 Semarang
Telp. (024) 3517261
E-mail: eko.hari@dsn.dinus.ac.id[1], atika.sari@dsn.dinus.ac.id[2], yanipartiastuti@dsn.dinus.ac.id[3], liyaumaroh17@gmail.com[4]

ABSTRAK

Pertukaran informasi melalui media internet secara bebas membuat pemilik informasi perlu waspada. Bukan hanya informasi umum, namun informasi khusus yang bersifat rahasia. Perlu adanya kendali untuk mengatur keamanan dalam informasi tersebut. Dalam hal ini, peran teknik penyandian data yang dikenal dengan nama kriptografi sangat penting. Kriptografi merupakan teknik untuk menyandikan data melalui proses ekripsi dan dekripsi dengan kunci tertentu sehingga menghasilkan data tersandikan yang tidak diketahui oleh orang lain. Dalam makalah ini akan digunakan algoritma vernam cipher. Algoritma ini termasuk algoritma kunci simetrik yaitu adanya kesamaan kunci antara enkripsi dan dekripsi. Keunggulan vernam cipher dibanding cipher yang lain yaitu menggunakan pseudorando-key yang sama panjang dengan fungsi XOR. Kunci acak pada vernam cipher berfungsi untuk menyulitkan kriptanalis dalam menemukan plainteks asli. Vernam cipher telah diuji coba melalui aplikasi kriptografi dengan media semua ekstensi file dan membuktikan bahwa algoritma tersebut handal. Hal ini dibuktikan dengan proses dekripsi setiap file yang diproses dapat kembali seperti semula dan tidak mengalami kerusakan. Hasil percobaan menggunakan 4 buah file dengan ukuran sama yaitu 100 kb namun mempunyai format file yang berbeda. Hasil dari proses enkripsi untuk semua file diubah ke bentuk *pdf dan tidak terdapat kerusakan file serta lama waktu eksekusi untuk semua proses enkripsi dan dekripsi tidak lebih dari 0.25 detik.

Kata Kunci: kriptografi, vernam cipher, fungsi XOR, pseudorandom-key

1. PENDAHULUAN

Penggunaan komputer dalam berbagai bidang kehidupan membawa perkembangan yang sangat pesat pada perangkat keras maupun perangkat lunak komputer. Sebelum adanya kemajuan di bidang telekomunikasi dan komputer, manusia menggunakan uang secara nyata untuk bertransakasi secara tatap muka. Pada dua dekade ini, kemajuan telekomunikasi dan komputer memungkinkan manusia untuk menyimpan data secara digital. Aktivitas penyimpanan data secata digital tentu saja mempunyai banyak resiko. Hal ini jelas terlihat apabila dalam aktivitas tersebut terdapat informasi yang penting dapat diakses oleh orang lain yang tidak berkepentingan (*unauthorized* person), misalnya informasi mengenai password atau PIN. Saat ini masalah keamanan pada komputer menjadi isu penting pada era teknologi informasi.

Perlindungan terhadap informasi yang berharga dapat dilakukan dengan menggunakan metode/algoritma tertentu, diantaranya yang popular adalah kriptografi. Metode ini mempunyai keunggulan dalam mengamankan data dan telah digunakan dalam semua bidang kehidupan. Kriptografi yang berasal dari kata yunani "*cryptos*" yang artinya rahasia dan "*graphein*" yang artinya tulisan, sehingga kriptografi adalah ilmu untuk menjaga kerahasiaan pesan dengan cara menyandikan ke bentuk yang tidak dimengerti (Ariyus, 2008). Keungulan dari kriptografi adalah

kemampuan penyandian pesan sehingga pesan terlihat seperti diacak. Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data, adalah suatu bidang ilmu dan seni *(art and science)* yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data dari pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. Sekarang bidang ilmu ini menjadi salah satu isu suatu topik riset yang tidak habis-habisnya diteliti dengan melibatkan banyak peneliti.

Kriptografi tidak sekedar berupa kerahasiaan data (*privacy*) saja, tapi juga bertujuan untuk menjaga integritas data (*data integrity*), keaslian data (*authentication*) dan anti penyangkalan *(non-repudiation)*. Di dalam kriptografi terdapat 5 hal utama yaitu enkripsi, dekripsi, dan kunci (*key*), pengirim, dan penerima. Enkripsi merupakan proses penyandian plainteks (pesan awal) menjadi cipherteks (pesan yang tersandikan), sedangkan dekripsi merupakan kebalikan dari proses enkripsi (Elminaam, et al., 2010). Baik proses enkripsi dan dekripsi, keduanya menggunakan kunci untuk menjaga kerahasiaan data. Penggunaan kriptografi mulai dari penggunaan kartu ATM, penggunaan password untuk file-file dokumen kantor, transaksi dengan kartu kredit, transaksi di bank, percakapan dengan handphone, dan akses internet telah membuktikan pentingnya kriptografi dalam pengamanan informasi.

Salah satu algoritma dalam kriptografi modern berbasis bit yang sering digunakan yaitu *vernam cipher* (*cipher aliran*). *Vernam cipher* dinilai lebih baik dalam hal performa dibanding dengan *block cipher* (Munir R., 2006). Algoritma ini beroperasi pada plainteks/cipherteks dalam bentuk *bit* tunggal sehingga pesan dienkripsikan/didekripsikan bit per bit, dengan demikian algoritma ini lebih *valid* untuk digunakan mengamankan data.

Dewasa ini bidang ilmu kriptografi memiliki kemungkinan aplikasi yang sangat luas, mulai dari bidang militer, telekomunikasi, jaringan komputer, keuangan dan perbankan, pendidikan dan singkatnya dimana suatu kerahasiaan data sangat diperlukan disitulah kriptografi memegang peranan penting. Produk-produk yamg menggunakan kriptografi sebagai dasarnyapun cukup beragam, mulai dari kartu ATM, *E-Commerce, secure e-mail* dan lain-lain. Kriptografi adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *cryptographer.* Sedang, *cryptanalysis* adalah suatu ilmu dan seni membuka *(breaking) ciphertext* dan orang yang melakukannya disebut *cryptanalyst*. *Cryptographic system* atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pen*cipher*an tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan.

2. VERNAM CIPHER

Vernam cipher adalah jenis algoritma enkripsi simetri. *Vernam cipher* dapat dibuat sangat cepat sekali, jauh lebih cepat dibandingkan dengan algoritma *block cipher* yang manapun. Algoritma block cipher secara umum digunakan untuk unit plaintext yang besar sedangkan stream cipher digunakan untuk blok data yang lebih kecil, biasanya ukuran bit (Stinson, 1995). Proses enkripsi terhadap plaintext tertentu dengan algoritma block cipher akan menghasilkan *ciphertext* yang sama jika kunci yang sama digunakan. Dengan *stream cipher*, transformasi dari unit plaintext yang lebih kecil ini berbeda antara satu dengan lainnya, tergantung pada kapan unit tersebut ditemukan selama proses enkripsi.

Satu *vernam cipher* menghasilkan apa yang disebut suatu *keystream* (suatu barisan bit yang digunakan sebagai kunci). Proses enkripsi dicapai dengan menggabungkan keystream dengan *plaintext* biasanya dengan operasi *bitwise XOR* (Kromodimoeljo, 2009). Pembentukan *keystream* dapat dibuat independen terhadap *plaintext* dan *ciphertext*, menghasilkan *synchronous stream cipher*, atau dapat dibuat tergantung pada data dan enkripsinya, dalam hal mana stream cipher disebut sebagai *self-synchronizing*. Kebanyakan bentuk *stream cipher* adalah *synchronous stream cipher*.

Konsentrasi dalam *stream ciphers* pada umumnya berkaitan dengan sifat sifat teoritis yang menarik dari one-time pad. Suatu one-time pad, kadang-kadang disebut *Vernam cipher*, menggunakan sebuah string dari bit yang dihasilkan murni secara *random* (Kromodimoeljo, 2009). *Keystream* memiliki panjang sama dengan pesan *plaintext*; string random digabungkan dengan menggunakan *bitwise* XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Karena *keystream* seluruhnya adalah random, walaupun dengan sumber daya komputasi tak terbatas seseorang hanya dapat menduga *plaintext* jika melihat *ciphertext*. Metode *cipher* seperti ini disebut memberikan kerahasiaan yang sempurna (*perfect secrecy*). Metode vernam *cipher* yang umum digunakan adalah RC4. Satu hal yang menarik bahwa mode operasi tertentu dari suatu *block cipher* dapat mentransformasikan secara efektif hasil operasi tersebut ke dalam satu *keystream* generator dan dalam hal ini, *block cipher* apa saja dapat digunakan sebagai suatu *stream cipher*; seperti dalam DES, CFB atau OFB. Akan tetapi, *vernam ciphers* dengan desain khusus biasanya jauh lebih cepat.

Cipherteks diperoleh dengan melakukan penjumlahan *modulo* 2 satu bit plainteks dengan satu bit kunci:

$$C_i = (P_i + K_i) \bmod 26 \quad (1)$$

ISBN: 978-979—3649-96-2 Unisbank Semarang, 28 Juli 2016

Dimana, P_i adalah bit plainteks, K_i adalah bit kunci, dan C_i adalah bit cipherteks. Plainteks diperoleh dengan melakukan penjumlahan *modulo* 2 satu bit cipherteks dengan satu bit kunci:

$$C_i = (P_i - K_i) \ mod \ 26 \quad (2)$$

Aliran-bit-kunci dibangkitkan dari sebuah pembangkit yang dinamakan pembangkit aliran-bit-kunci (*keystream generator*). Aliran-bit-kunci (sering dinamakan *running key*) di-XOR-kan dengan aliran bit-bit plainteks, p_1, p_2, …, p_i, untuk menghasilkan aliran bit-bit cipherteks:

$$C_i = P_i \oplus K_i \quad (3)$$

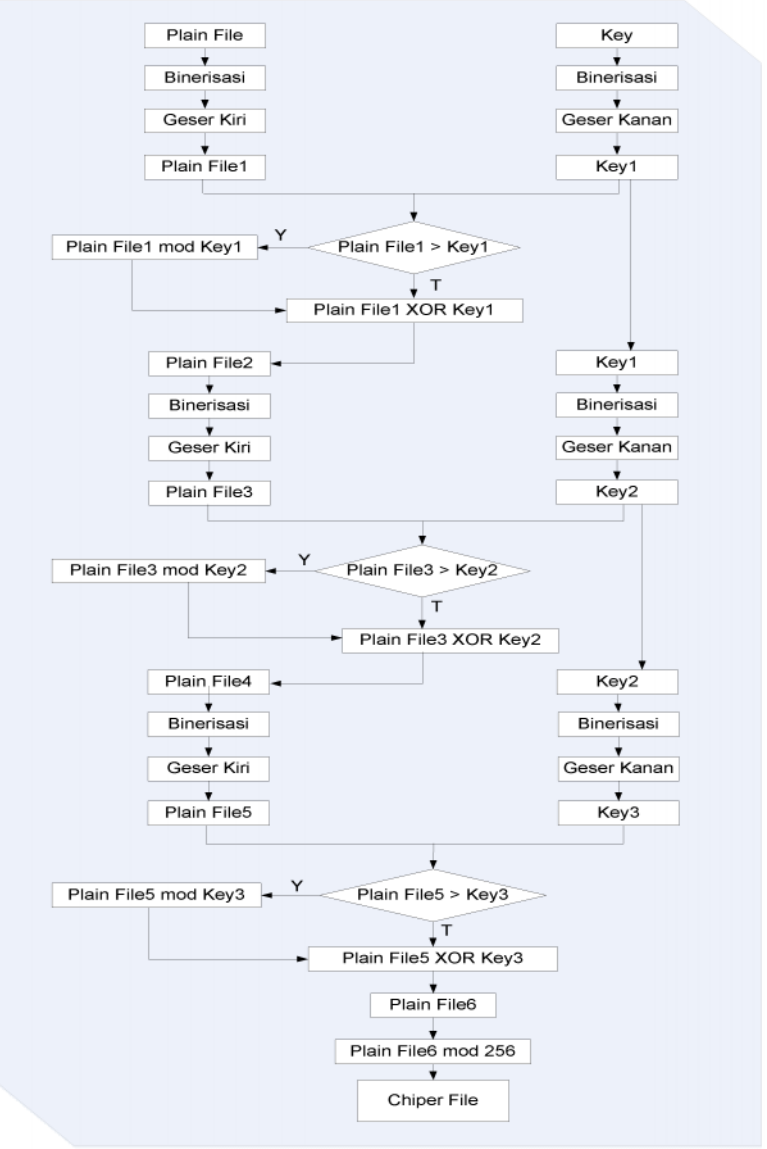
Di sisi penerima, bit-bit cipherteks di-XOR-kan dengan aliran-bit-kunci yang sama untuk menghasilkan bit-bit plainteks:

$$P_i = C_i \oplus K_i \quad (4)$$

Merancang pembangkit bit-aliran-kunci yang bagus cukup sulit karena membutuhkan pengujian statistik untuk menjamin bahwa keluaran dari pembangkit tersebut sangat mendekati barisan acak yang sebenarnya.

3. HASIL DAN PEMBAHASAN

Proses enkripsi menggunakan Kriptografi *Vernam Cipher* dapat dideskripsikan seperti pada Gambar 1 berikut ini.



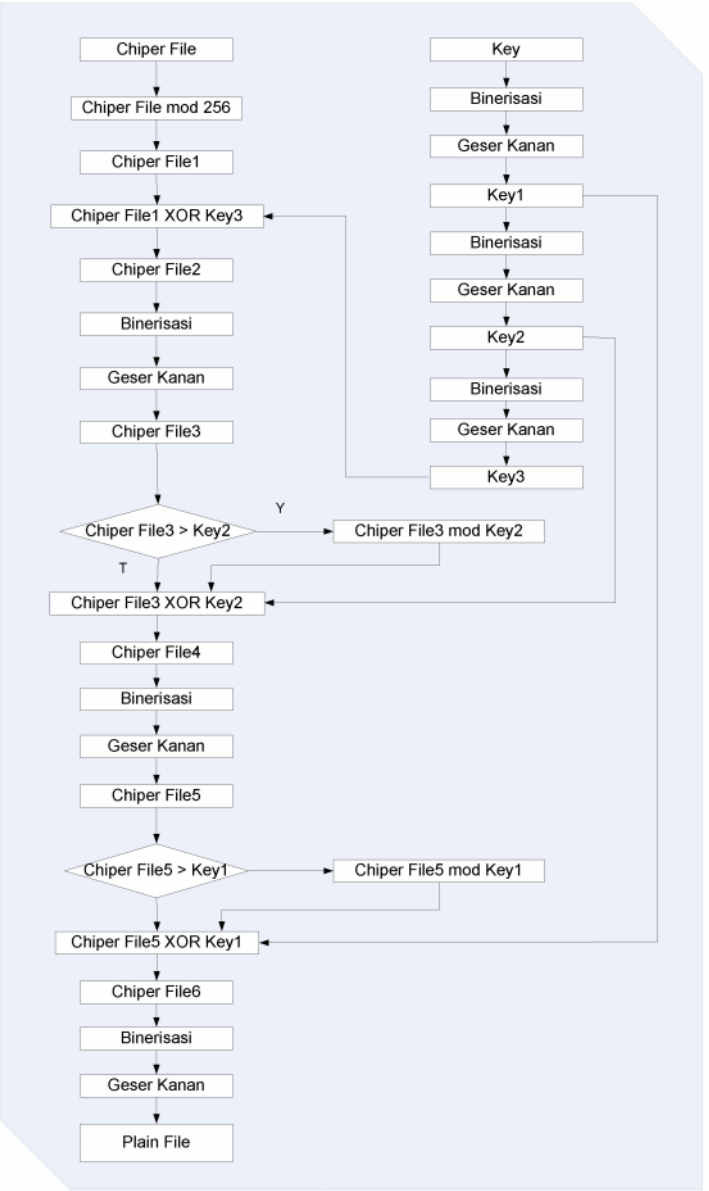
Gambar 1 Enkripsi Menggunakan Vernam Cipher

Berdasarkan Gambar 4, proses enkripsi *file* dapat dijabarkan sebagai berikut:

ISBN: 978-979—3649-96-2 Unisbank Semarang, 28 Juli 2016

1. Menyiapkan *file* dan kunci yang akan digunakan. *Plainfile* kemudian dibinerkan dan digeser ke kiri satu kali, misal C maka akan menjadi B, yang kemudian disebut *Plainfile*1. Sedangkan pada kunci juga dilakukan proses binerisasi tetapi kunci digesser ke kanan satu kali dan hasil pergeseran tersebut menghasilkan Key1. Apabila *Plainfile* 1 lebih besar dari pada Key1, maka akan dilakukan proses mod pada Plain File 1 terhadap Key1 dan kemudian *Plainfile*1 XOR Key1. Apabila Plain File1 lebih kecil atau sama dengan Key1 maka proses yang akan dilakukan adalah XOR pada *Plainfile*1 terhadap Key1.
2. Hasil dari XOR *Plainfile*1 disebut *Plainfile*2. *Plainfile*2 kemudian dibinerkan dan digeser ke kiri, dan hasil pergeseran ini disebut *Plainfile*3. Sedangkan Key1 dibinerkan dan digeser ke kanan, hasil proses pergeeran ini disebuut Key2. Selanjutnya, *Plainfile* 3 dan Key2 digunakan untuk proses pemilihan, apakah *Plainfile*3 lebih besar dari Key2, apabila benar maka akan dilakukan proses *Plainfile*3 mod Key2 kemudian *Plainfile*3 XOR Key2. Apabila *Plainfile*3 lebih kecil atau sama dengan Key2 maka akan dilakukan proses Plain File3 XOR Key2.
3. Hasil dari XOR *Plainfile*3 disebut *Plainfile*4. *Plainfile*4 kemudian dibinerkan dan digeser ke kiri, dan hasil pergeseran ini disebut Plain File5. Sedangkan Key2 dibinerkan dan digeser ke kanan, hasil proses pergeeran ini disebuut Key3. Selanjutnya, *Plainfile*5 dan Key3 digunakan untuk proses pemilihan, apakah *Plainfile*5 lebih besar dari Key3, apabila benar maka akan dilakukan proses *Plainfile*5 mod Key3 kemudian Plain File5 XOR Key3. Apabila *Plainfile*5 lebih kecil atau sama dengan Key3 maka akan dilakukan proses *Plainfile*5 XOR Key3. Hasil dari XOR *Plainfile*5 disebut *Plainfile*6, kemudian *Plainfile*6 di mod 256 sehingga dihasilkan *Chiper File*.

Setelah mnegetahui langkah-langkah enkripsi file, maka akan dilakukan proses dekripsi file seperti ditunjukkan pada Gambar 5



ISBN: 978-979—3649-96-2 Unisbank Semarang, 28 Juli 2016

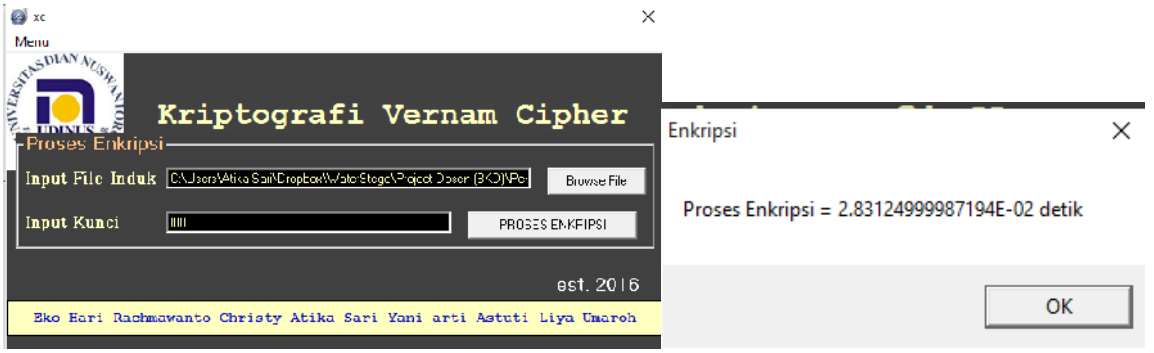
Gambar 2 Dekripsi Menggunakan Vernam Cipher

Berdasarkan Gambar 2, proses dekripsi *file* dapat dijabarkan sebagai berikut:

1. Menyiapkan *Chiper File* dan *Key* hasil proses enkripsi.*Chiper File* di mod 256, hasil proses ini disebut *Chiper File*1. Kemudian *Key* dibinerkan dan digeser ke kanan 1 sehingga menghasilkan *Key*1, *Key*1 dibinerkan dan digeser ke kanan 1 sehingga menghasilkan *Key*2, dan *Key*2 dibinerkan dan digeser ke kanan 1 sehingga menghasilkan *Key*3.
2. *Key* 3 kemudian digunakan untuk melakukan proses XOR pada *Chiper File*1, yaitu *Chiper File*1 XOR *Key*3, sehingga dihasilkan *Chiper File*2. Setelah itu, *Chiper File*2 kemudian dibinerkan dan digeser 1 kali ke kanan sehingga menghasilkan *Chiper File*3.
3. Apabila *Chiper File*3 lebih besar dari *Key*2 maka *Chiper File*3 mod *Key*2 dan kemudian di XOR kan yaitu *Chiper File*3 XOR *Key*2 sehingga dihasilkan *Chiper File*4. Apabila *Chiper File*3 tidak lebih besar dari *Key*2 maka hanya akan dilakukan proses XOR saja. Selanjutnya *Chiper File*4 dibinerkan dan digeser ke kanan 1 kali sehingga dihasilakn *Chiper File*5.
4. Apabila *Chiper File*5 lebih besar dari *Key*1 maka *Chiper File*5 mod *Key*1 dan kemudian di XOR kan yaitu *Chiper File*5 XOR *Key*1 sehingga dihasilkan *Chiper File*6. Apabila *Chiper File*5 tidak lebih besar dari *Key*1 maka hanya akan dilakukan proses XOR saja. Selanjutnya *Chiper File*6 dibinerkan dan digeser ke kanan 1 kali sehingga dihasilkan *Plain File*.

Berikut ini merupakan tampilan aplikasi dalam mengolah file kriptografi menggunakan algoritma *Vernam Cipher*.

Gambar 3 Tampilan Awal Aplikasi



(a) (b)

Gambar 4 (a) Proses Enkripsi, (b) Lama Waktu Proses Enkripsi

(a) (b)

Gambar 5 (a) Proses Dekripsi File dari doc ke pdf, (b) Lama Proses Dekripsi

ISBN: 978-979—3649-96-2 Unisbank Semarang, 28 Juli 2016

Dalam percobaan ini digunakan file berformat *.doc dengan ukuran 23 kb. Dari hasil pengamatan untuk file berukuran 23 kb dibutuhkan waktu enkripsi 2,8 detik sedangkan waktu dekripsi 0,03 detik. Dalam aplikasi ini file induk dan file hasil dapat dimodifikasi dengan cara mengubah format file. Hal ini bertujuan untuk mengaburkan/mengecoh pihak yang tidak berwenang.

4. KESIMPULAN

Dari hasil percobaan menggunakan kriptografi *Vernam Cipher* membuktikan bahwa aplikasi dapat mengacak file dengan aman dan tidak menimbulkan kecurigaan pada pihak lain. Pada file hasil, tidak menimbulkan efek yang dapat merusak ataupun mengganggu kinerja file sebelumnya.

Tabel 1 Lama Eksekusi Proses Enkripsi Dekripsi berukuran 100 kb

Nama File	Lama Enkripsi (dalam detik)	Lama Dekripsi (dalam detik)
AESERVIC.dll	0.13	0.14
f3400632.txt	0.21	0.13
Photothumb.db	0.24	0.14
websiteta	0.14	0.20

Tabel 1 merupakan percobaan lain yang dilakukan untuk mengtahui performa Vernam Cipher digunakan 4 buah file dengan ukuran sama yaitu 100 kb namun mempunyai format file yang berbeda. Hasil dari proses enkripsi untuk semua file diubah ke bentuk *pdf sehingga dihasilkan lama eksekusi untuk proses enkripsi dan dekripsi. Hasl ini membuktikan bahwa algoritma Vernam cipher handal dalam mengamankan data.

PUSTAKA

Abd Elminaam, D., Abdual Kader, H., & Hadhoud, M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *International Journal of Network Security, Vol.10, No.*, 216-222.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi : Teori, Analisis dan Impelementasi.* Yogyakarta: Penerbit Andi.

Kromodimoeljo, S. (2009). *Teori dan Aplikasi Kriptografi.* SPK IT Consulting.

Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

Stinson, D. (1995). *Cryptography Theory and Practice.* Florida: CRC Press.