Enkripsi PDF dengan Menggunakan Kriptografi Visual dan *Two-Man Rule*

Saskia Imani 13517142[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517142@std.stei.itb.ac.id

***Abstrak*—*Portable Document Format* (PDF) adalah salah satu format yang paling umum digunakan untuk menjamin tampilan teks dan gambar pada dokumen yang konsisten pada berbagai perangkat lunak, perangkat keras, dan sistem operasi yang berbeda. Terdapat berbagai program manajemen dan pembaca PDF yang juga menawarkan layanan enkripsi untuk menjamin keamanan dokumen. Namun, terdapat kelemahan pada sistem enkripsi yang ditawarkan, sehingga menyebabkan dokumen menjadi lemah terhadap serangan eksfiltrasi, yaitu penyisipan data yang tidak seharusnya ke dalam dokumen oleh pihak ketiga. Dalam makalah ini, diuraikan sebuah skema enkripsi baru dengan menggunakan kriptografi visual dan prinsip *two-man rule* untuk meningkatkan keamanan enkripsi PDF.**

***Kata kunci*—Dekripsi, eksfiltrasi, enkripsi, kriptografi visual, PDF, *two-man rule*.**

I. PENDAHULUAN

Di tengah kemajuan teknologi yang pesat, dan munculnya berbagai pertukaran informasi yang harus dilakukan melalui internet, terjadi pula peningkatan kebutuhan keamanan informasi. Kriptografi menjadi solusi untuk kebutuhan keamanan informasi, dan menyediakan berbagai manipulasi bagi pengirim untuk mengubah informasi menjadi suatu bentuk yang tidak dapat diketahui atau dimodifikasi oleh pihak ketiga, dan mengubahnya kembali menjadi informasi semula agar dapat dibaca oleh pihak penerima.

Dalam konteks pembagian dokumen dalam bentuk Portable Document Format (PDF), kriptografi digunakan untuk menyediakan layanan enkripsi yang dapat menyamarkan isi dari dokumen dan membubuhkan sebuah kata sandi yang harus dimasukkan untuk dapat membaca isi asli dari dokumen tersebut. Enkripsi pada PDF tergolong aman dari segi kerahasiaan pesan dan kepastian identitas pengirim pesan, dan teknik tambahan seperti *digital watermarking* membantu menjamin pengakuan dari pengirim terhadap pesan.

Namun, dari segi keaslian pesan, enkripsi pada PDF memiliki kelemahan yang menyebabkan mudahnya suatu pihak ketiga untuk menyisipkan informasi tambahan yang tidak diinginkan ke dalam PDF tersebut. Informasi tambahan ini sangat berbahaya, karena dapat melakukan berbagai hal seperti memberikan informasi yang salah ataupun menjalankan kode secara otomatis, sehingga keamanan dari penerima menjadi terkompromi. Oleh banyak penyedia jasa enkripsi PDF, kelemahan ini dianggap sebagai suatu hal yang lumrah dan tidak dapat diperbaiki. Keamanan PDF lebih lanjut harus diserahkan kepada teknologi lain yang lebih kompleks seperti perangkat lunak *digital rights management* (DRM) dan keamanan yang disediakan dari pihak penyedia saluran yang digunakan untuk pengiriman PDF.

Kriptografi merupakan sebuah ilmu yang terus menerus berkembang seiring waktu. Salah satu keunikan dari kriptografi adalah pemanfaatan konsep-konsep yang sudah ada terdahulu, seperti pergeseran huruf dan teori bilangan, dan menerapkannya ke dalam berbagai teknik yang lebih bersifat modern seperti *block cipher*, kriptografi kunci-publik, dan kriptografi visual. Banyak jenis kriptografi maupun kriptoanalisis menjadikan konsep yang sederhana menjadi inspirasi untuk memecahkan berbagai permasalahan yang lebih kompleks.

Adapun terdapat *two-man rule*, sebuah konsep yang dipakai oleh berbagai pihak dan organisasi yang bertanggung jawab terhadap informasi yang sifatnya sangat rahasia atau kegiatan yang bersifat kritis. Prinsip *two-man rule* menyatakan bahwa untuk setiap akses kepada fasilitas yang berupa informasi atau aksi, diperlukan dua buah pihak yang berbeda secara bersamaan untuk mengakses fasilitas tersebut. Prinsip ini digunakan dalam bidang profesi militer, seperti dalam peluncuran nuklir, dan bidang keamanan dan komunikasi yang berskala besar. Prinsip *two-man rule* yang sederhana, namun telah teruji dan terjamin keamanannya, berpotensi menjadi solusi untuk permasalahan keamanan yang masih terdapat pada kriptografi seputar enkripsi dan autentikasi pada dokumen dalam format PDF.

II. LANDASAN TEORI

A. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-tenik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1]. Aspek keamanan secara rincinya dapat dibagi menjadi 4 (empat), antara lain:

1. Kerahasiaan pesan (*confidentiality*), yaitu wujud asli dari pesan hanya dapat diketahui oleh pihak pengirim dan penerima pesan
2. Keaslian pesan (*data integrity*), yaitu pesan dari pengirim adalah pesan yang sama yang didapatkan oleh penerima tanpa adanya perubahan
3. Keaslian pengirim pesan (*authentication*), yaitu

jaminan bahwa identitas pengirim pesan adalah asli dan bukan samaran dari pihak ketiga; dan

4. Tidak dapat melakukan penyangkalan (*non-repudiation*), yaitu pihak pengirim pesan yang beridentitas tidak dapat menyangkal bahwa telah mengirim pesan

Dalam kriptografi, terdapat beberapa istilah untuk aspek-aspek yang terlibat di dalamnya. Pihak pengirim disebut juga *sender*, dan pihak penerima disebut juga *receiver*, sedangkan pihak ketiga seringkali disebut sebagai penyadap (*eavesdropper*). Sujud asli dari sebuah pesan disebut plainteks (*plaintext*), dan wujud sebuah pesan yang telah disamarkan disebut ciperteks (*ciphertext*). Terdapat dua proses utama dalam kriptografi, antara lain proses enkripsi (*encryption*) yang mengubah pesan dari bentuk plainteks menjadi ciperteks, dan proses dekripsi (*decryption*) yang mengubah bentuk pesan dari bentuk ciperteks menjadi plainteks.

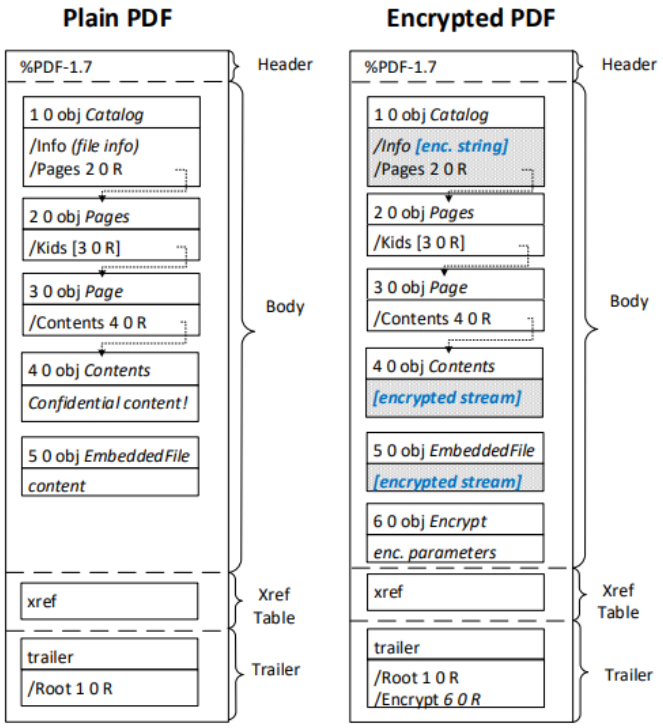
Terdapat berbagai alogritma yang telah dicetuskan untuk melakukan enkripsi dan dekripsi, yang diberi istilah *cipher*. Masing-masing *cipher* memiliki langkah-langkah yang berbeda, dan melibatkan beberapa informasi yang berbeda pula untuk melakukan enkripsi dan dekripsi. Informasi yang terlibat dalam *cipher* dan bukan plainteks atau ciperteks diberi istilah kunci (*key*)[2].

B. Portable Document Format (PDF)

Portable Document Format (PDF) adalah sebuah format berkas yang dikembangkan oleh Adobe pada tahun 1993 untuk menampilkan dokumen secara digital secara konsisten terlepas dari aplikasi perangkat lunak, perangkat keras, ataupun sistem operasi yang digunakan untuk menampilkan dokumen tersebut. Sebuah berkas PDF didasarkan pada bahasa PostScript, dan mengandung deskripsi lengkap penataan posisi untuk tampilan teks, grafik vektor dua dimensi, citra, dan berbagai informasi lainnya [3]. Pada tahun 2008, PDF telah menjadi sebuah standar dari International Organization for Standardization (ISO) dengan kode 32000-1:2008. PDF juga menyediakan enkripsi dan tanda tangan digital, lampiran, serta metadata.

PDF mendukung enkripsi menggunakan algoritma AES dengan mode Ciper Block Chaining (CBC) [4]. Secara teori, diharapkan bahwa sebuah berkas PDF yang telah dienkripsi tidak dapat dibuka oleh pihak yang tidak memiliki kata sandi untuk membuka berkas tersebut, sehingga berkas PDF dapat secara aman dibagikan melalui saluran yang tidak aman sekalipun. Perbandingan struktur internal sebuah berkas PDF yang tidak dienkripsi dan berkas PDF yang dienkripsi ditunjukkan secara sederhana pada Gambar 1.

Serangan terhadap enkripsi PDF diklasifikasikan menjadi dua jenis, yaitu serangan tanpa interaksi pengguna dan serangan dengan interaksi pengguna. Pada serangan tanpa interaksi pengguna, korban serangan, yaitu pihak yang menerima dan membuka berkas PDF dengan kata sandi yang sesuai, hanya perlu membuka PDF untuk terjadinya kebocoran sebagian atau seluruh plainteks pada berkas PDF tersebut. Sedangkan pada serangan dengan interaksi pengguna, korban serangan harus berinteraksi dengan berkas terlebih dahulu, misalnya harus mengklik sebuah halaman tertentu dalam dokumen atau mengklik ‘OK’ pada sebuah dialog konfirmasi yang muncul



Gambar 1. Perbandingan struktur internal yang disederhananakan dari berkas PDF tanpa enkripsi (kiri) dan dengan enkripsi (kanan)

ketika membuka berkas PDF.

Pada dokumen PDF, hanya isi dari dokumen tersebut terenkripsi, sedangkan objek-objek yang menentukan struktur dari dokkumen tidak terenkripsi dan dapat dengan mudah dimanipulasi. Seorang penyadap dapat menduplikasi atau menghapus halaman-halaman, atau mengubah urutan dokumen. Selain itu, sejak PDF versi 1.5, ditambahkan dukungan terhadap *crypt filter*, yang memampukan enkripsi secara parsial hanya kepada sebagian dari PDF. Dengan adanya *crypt filter*, penyadap dapat menambahkan berbagai halaman dengan konten yang tidak seharusnya atau memodifikasi halaman yang terenkripsi dengan menambahkan *overlay*, sehingga mengubah keseluruhan tampilan dari halaman tersebut.

Selain serangan yang dikarenakan enkripsi parsial, terdapat juga serangan yang memanfaatkan kelemahan algoritma CBC dengan menggunakan apa yang disebut *CBC gadget*. Dengan menggunakan *CBC gadget*, penyadap yang mengetahui sebagian dari plainteks dapat memodifikasi sebagian konten dari sebuah dokumen PDF ataupun menambahkan konten baru ke dalam bagian yang diketahui plainteksnya. Konten baru yang ditambahkan umumnya berupa sebuah metode untuk mengambil data dalam PDF tersebut dan menyalurkannya kepada sebuah *server* yang dikontrol oleh penyadap, dengan memanfaatkan bentuk-bentuk konten interaktif yang didukung oleh format PDF seperti formulir PDF, *hyperlink*, dan kode JavaScript.

Sebuah pengujian terhadap serangan dilakukan terhadap 27 aplikasi perangkat lunak yang mendukung format PDF, dengan hasil seperti yang ditunjukkan pada Gambar 2. Sejumlah besar aplikasi yang diuji lemah terhadap serangan langsung yang memanfaatkan enkripsi parsial, sedangkan semua aplikasi yang

Application	Version		Attack A	Attack B
Acrobat Reader DC	(2019.008.20081)	Windows	●	◐
Foxit Reader	(9.2.0.9297)	Windows	◐	◐
PDF-XChange Viewer	(2.5.322.9)	Windows	●	◐
Perfect PDF Reader	(8.0.3.5)	Windows	●	●
PDF Studio Viewer	(2018.1.0)	Windows	●	●
Nitro Reader	(5.5.9.2)	Windows	●	●
Acrobat Pro DC	(2017.011.30127)	Windows	●	◐
Foxit PhantomPDF	(9.5.0.20723)	Windows	◐	◐
PDF-XChange Editor	(7.0.326.1)	Windows	●	◐
Perfect PDF Premium	(10.0.0.1)	Windows	●	●
PDF Studio Pro	(12.0.7)	Windows	●	●
Nitro Pro	(12.2.0.228)	Windows	●	●
Nuance Power PDF	(3.0.0.17)	Windows	●	◐
iSkysoft PDF Editor	(6.4.2.3521)	Windows	◐	◐
Master PDF Editor	(5.1.36)	Windows	●	●
Soda PDF Desktop	(11.0.16.2797)	Windows	◐	◐
PDF Architect	(7.0.23.3193)	Windows	◐	◐
PDFelement	(6.8.0.3523)	Windows	◐	◐
Preview	(10.0.944.4)	Mac	○	◐
Skim	(1.4.37)	Mac	○	◐
Evince	(3.32.0)	Linux	◐	◐
Okular	(1.7.3)	Linux	◐	◐
MuPDF	(1.14.0)	Linux	◐	◐
Chrome	(70.0.3538.67)	Web	●	●
Firefox	(66.0.2)	Web	○	◐
Safari	(11.0.3)	Web	○	◐
Opera	(57.0.3098.106)	Web	●	●

● Exfiltration (no user interaction)
◐ Exfiltration (with user interaction)
○ No exfiltration / not vulnerable

Gambar 2. Hasil pengujian 27 aplikasi perangkat lunak yang mendukung PDF terhadap serangan langsung dan serangan menggunakan *CBC gadget*

diuji dapat diserang dengan menggunakan sebuah *CBC gadget*. Salah satu solusi yang telah ditawarkan untuk meningkatkan keamanan pada PDF adalah dengan meniadakan kemampuan untuk melakukan enkripsi parsial. Solusi lain adalah dengan mewajibkan enkripsi dengan algoritma yang mendukung penjagaan integritas pada PDF [5].

C. Kriptografi Visual

Kriptografi visual atau *visual cryptography* adalah sebuah teknik kriptografi yang mengenkripsi informasi visual berupa citra digital dengan suatu cara sehingga dekripsi cukup dilakukan dengan mempersepsi informasi menggunakan indra penglihatan (mata). Proses enkripsi dilakukan dengan membagi gambar menjadi sejumlah bagian yang disebut *share*, sedangkan untuk proses dekripsi dilakukan penumpukkan sejumlah *share* sehingga dibentuk sebuah gambar gabungan yang dapat langsung diamati oleh pihak penerima.

Setiap citra digital terdiri dari sejumlah *pixel*, yang masing-masing memiliki panjang *n*-bit tergantung jenis warna yang terdapat pada citra digital. Citra *true color* mengandung campuran warna merah, hijau, dan biru, dan memiliki panjang 24 *bit* pada setiap *pixel*, sedangkan citra *grayscale* mengandung campuran warna hitam dan putih dan memiliki panjang 8 *bit* pada setiap *pixel*. Citra biner hanya terdiri dari warna hitam dan warna putih, sehingga hanya terdiri dari 1 *bit* pada setiap *pixel*.

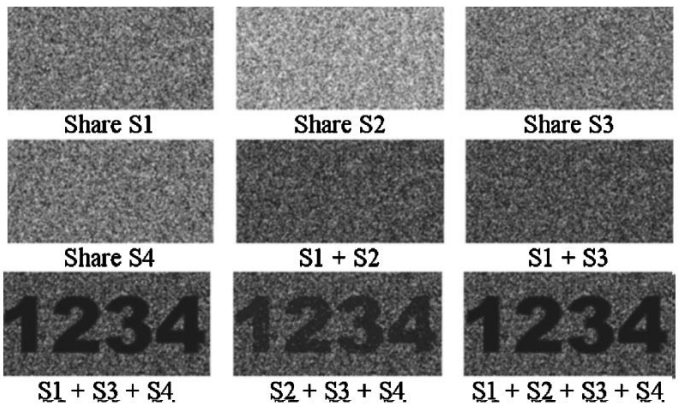
Pada kriptografi visual pada citra biner, setiap *pixel* dibagi menjadi sejumlah *sub-pixel*. Pada setiap *share*, muncul perwakilan *pixel* yang tidak memiliki nilai yang sama dengan citra asli yaitu hitam atau putih, namun merupakan *sub-pixel* dengan kombinasi warna hitam dan putih. Penumpukkan setiap *share* akan menyebabkan kombinasi dari berbagai jenis *sub-pixel* dan membentuk sebuah *pixel* yang dapat dipersepsi menjadi warna "putih" atau "hitam"[7]. Suatu skema tertentu diberikan notasi Skema(*k*,*n*), dengan *k* adalah jumlah *share* yang dibutuhkan untuk mendekripsi pesan dan *n* adalah jumlah *share* total.

Digunakan beberapa matriks dalam proses kriptografi visual, antara lain:

- *B* = matriks *n* x 1 yang bernilai 1 seluruhnya
- *I* = matriks identitas *n* x *n* (diagonal utama = 1)
- *BI* = matriks hasil penggabungan B dan I
- *c(BI)* = matriks komplemen dari *BI*

Sehingga akan dihasilkan jenis-jenis representasi pixel hitam (C_0), yaitu seluruh matriks hasil permutasi kolom dari *BI* dan pixel putih (C_1), yaitu seluruh matriks hasil permutasi kolom dari *c(BI)*. Contoh enkripsi dan dekripsi untuk kriptografi visual citra biner dengan menggunakan Skema(3,4) diilustrasikan pada Gambar 4 [7].

Untuk menghasilkan solusi kriptografi visual yang valid untuk suatu Skema(*k*,*n*), terdapat 3 (tiga) buah syarat yang harus dipenuhi oleh skema tersebut.

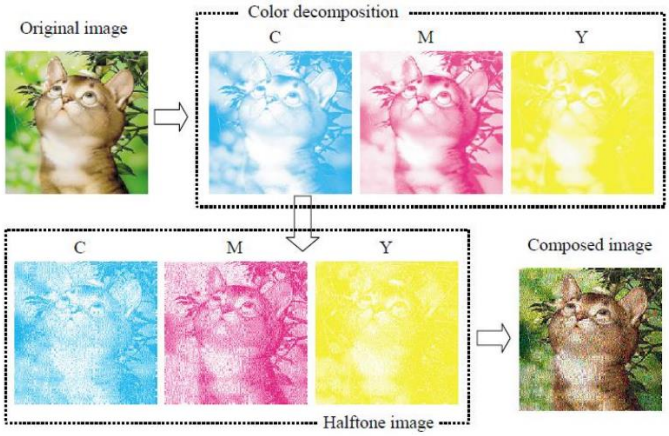


Gambar 4. Contoh kriptografi visual citra biner dengan menggunakan Skema(3,4)

1. Untuk sembarang matriks *S* pada C_0, bobot Hamming untuk sejumlah *k* dari *n* baris memenuhi $H(V) \leq d - \alpha m$.
2. Untuk sembarang matriks *S* pada C_1, bobot Hamming untuk sejumlah *k* dari *n* baris memenuhi $H(V) \geq d$.
3. Untuk sembarang subset $\{i_1, i_2, ..., i_q\}$ dari {1, 2, ..., n}, $q < k$, dua buah kumpulan matriks berukuran $q \times m$, yakni D_0 dan D_1, yang diperoleh dari hasil

restricting masing-masing matriks berukuran $n \times m$ dari C_0 dan C_1 pada baris-baris $i_1, i_2, ..., i_q$ tidak dapat dibedakan satu sama lainnya karena memiliki matriks yang sama dengan frekuensi yang sama.

Sedangkan pada kriptografi visual pada citra *grayscale* dilakukan dengan mengubah citra tersebut ke dalam bentuk *halftone* terlebih dahulu, yang pada dasarnya terdiri dari *pixel-pixel* biner, dan kemudian menerapkan skema kriptografi visual citra biner. Pada citra *true color* yang berbasis RGB atau CMY, citra lebih dulu didekomposisi menjadi R, G, dan B, atau C, M, dan Y, dan kemudian diubah menjadi bentuk *halftone*. Kemudian masing-masing komposisi citra dienkripsi dengan skema kriptografi visual citra biner dengan kombinasi warna putih dan *x*, dengan *x* adalah salah satu warna R, G, B, C, M, atau Y[8].



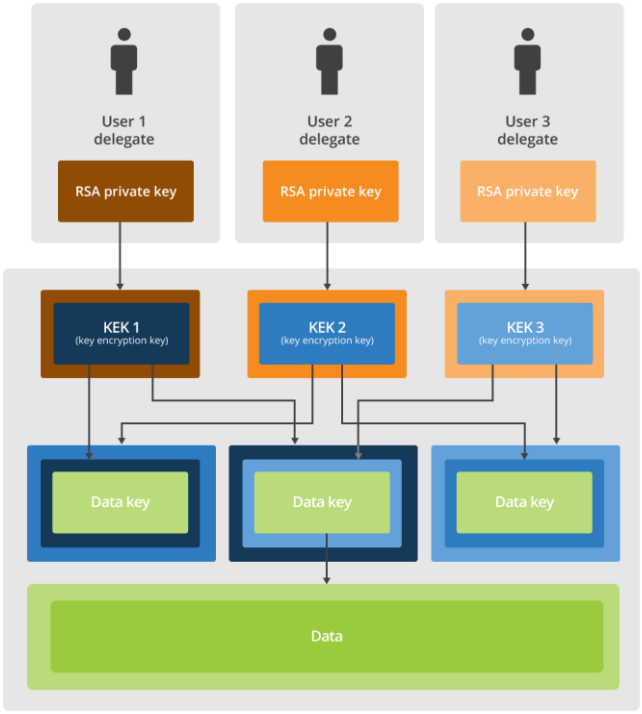
Gambar 5. Contoh kriptografi visual pada citra *true color*

D. Two-Man Rule

Aturan dua orang, atau lebih dikenal dalam bahasa Inggris sebagai *two-man rule* adalah sebuah mekanisme pengamanan yang didesain untuk mencapai tingkat keamanan tinggu untuk materi ataupun operasi yang bersifat kritis. Aturan ini menyatakan bahwa untuk mengakses maupun melakukan aksi yang berada pada naungan aturan ini, harus terdapat kehadiran dua pihak yang memiliki hak untuk mengakses atau melakukan aksi tersebut. Mekanisme ini paling dikenal digunakan untuk mengendalikan kode peluncuran nuklir oleh angkatan udara Amerika Serikat.

Aturan ini telah dijadikan inspirasi dalam kriptografi, contohnya oleh perusahaan Microsoft dalam fitur Double Key Encryption (DKE) yang ditawarkan untuk layanan Microsoft 365. Untuk setiap berkas atau informasi yang disimpan oleh pengguna pada *storage* yang disediakan oleh Microsoft 365, diberlakukan enkripsi oleh dua kunci yang berbeda. Pihak Microsoft hanya menyimpan salah satu dari kedua kunci tersebut, sehingga tidak dapat mengakses data yang dimiliki pengguna secara sepihak tanpa kunci yang nantinya hanya mampu diberikan oleh pengguna.

Salah satu contoh penerapan lainnya dari aturan ini adalah pada kriptografi yang dilakukan oleh CloudFlare, sebuah perusahaan infrastruktur dan keamanan situs web. Dalam layanannya yang diberi nama Red October, diterapkan *two-man rule* kepada suatu kunci dekripsi data. Setiap kunci dekripsi yang disimpan merupakan hasil enkripsi kunci asli dengan dua buah kata sandi yang dimiliki oleh pihak-pihak pengakses data, sehingga dibutuhkan sekurangnya dua pihak untuk dapat melakukan dekripsi. Untuk lebih jauh meningkatkan keamanan, kata sandi yang dimiliki masing-masing pihak juga dienkripsi Kembali dengan menggunakan algoritma kriptografi asimetri, yaitu RSA. Skema layanan Red October diilustrasikan pada Gambar 6 [9].



Gambar 6. Skema kriptografi oleh layanan Red October

III. RANCANGAN IMPLEMENTASI

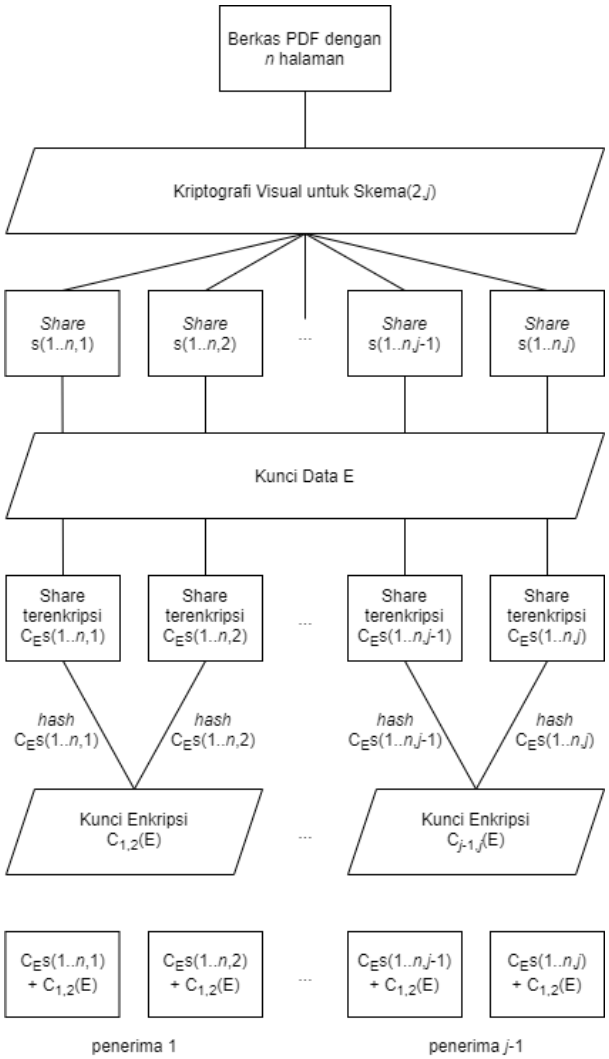
Berdasarkan kriptografi visual dan prinsip *two-man rule* yang telah ada, dan dengan mempertimbangkan sifat dari PDF yang spesifikasinya adalah dapat menampilkan setiap komponen setiap halaman dengan tata letak yang sama pada berbagai aplikasi perangkat lunak yang berbeda, dapat dirancang sebuah skema enkripsi dan dekripsi baru untuk meningkatkan keamanan berkas PDF terhadap serangan berupa eksfiltrasi dan penyisipan pesan oleh pihak penyadap ke dalam berkas. Dengan skema ini, pengirim pesan dapat memilih beberapa kombinasi pasangan *share* berbeda yang diinginkan. Jumlah share dinotasikan dengan *j*.

Skema enkripsi dan dekripsi secara umum terdiri dari 3 (tiga) komponen, antara lain:

- *Modul kriptografi visual*. Modul ini digunakan untuk mendekomposisi dan mengenkripsi setiap halaman pada PDF menjadi *j*-buah *share*, serta membalikkan proses tersebut untuk proses dekripsi. Satu buah share diberi notasi S(*i*,*j*) dengan *i* adalah indeks nomor halaman dan *j* adalah indeks *share*.
- *Modul kriptografi AES-CBC*. Modul ini digunakan untuk mengenkripsi dan dekripsi setiap *share* dengan kunci data E, serta mengenkripsi dan dekripsi kunci data tersebut terhadap setiap dua

pasang *share* berdasarkan hasil fungsi *hash* dari *share* tersebut. Hasil fungsi hash untuk pasangan share dinotasikan sebagai *K1* dan *K2*, sehingga hasil enkripsi kunci data dinotasikan sebagai $C_{K1,K2}(E)$.

Sedangkan tahap-tahap operasi terhadap berkas PDF yang dilakukan oleh skema diilustrasikan pada Gambar 7.



Gambar 7. Skema implementasi kriptografi visual dengan *two-man rule* pada PDF

Rincian tahap-tahap untuk melakukan enkripsi berkas PDF diuraikan sebagai berikut.

1. Pengirim memasukkan jumlah *share* berbeda yang diinginkan (*j*).
2. Dengan menggunakan modul kriptografi visual dengan Skema(2,*j*), berkas PDF didekomposisi dan dienkripsi setiap halamannya. Dihasilkan *j*-buah berkas hasil enkripsi yang masing-masing mengandung sebuah *share* berbeda untuk setiap halaman.
3. Setiap *share* dienkripsi dengan modul kriptografi AES-CBC menggunakan sebuah kunci *E* yang dipilih oleh pengirim.
4. Dihitung nilai fungsi hash untuk setiap *share*.
5. Dengan menggunakan modul kritpgrafi AES-CBC, kunci data *E* dienkripsi menggunakan sepasang nilai *hash* dari sepasang *share* yang berbeda. Kunci enkripsi yang dihasilkan, $C_{K1,K2}(E)$, dipasangkan dengan masing-masing *share* yang menghasilkan *K1* dan *K2*.
6. Dihasilkan *j*-buah pasangan *share* yang telah dienkripsi dan kunci enkripsi.

Agar seorang penerima dapat melakukan dekripsi, penerima harus memiliki sepasang *share* dan kunci yang sesuai untuk pasangan *share* tersebut. Dilakukan tahap-tahal sebagai berikut.

1. Dihitung nilai fungsi *hash* untuk pasangan *share* sehingga menghasilkan *K1* dan *K2*.
2. Dengan modul kriptografi AES-CBC, *K1* dan *K2* digunakan untuk mendekripsi kunci enkripsi menjadi kunci data *E*.
3. Dengan menggunakan modul kriptografi AES-CBC, kunci data *E* digunakan untuk mendekripsi pasangan *share*.
4. Dengan menggunakan modul kriptografi visual, pasangan *share* kemudian ditumpukkan sehingga membentuk dokumen yang utuh.

Masing-masing *share* yang membentuk sepasang serta kunci untuk pasangan *share* dikirim secara secara terpisah.

IV. KELEBIHAN DAN KEKURANGAN

Kelebihan utama dari impementasi kriptografi visual dengan menggunakan *two-man rule* yang telah dirincikan adalah pengirim dapat tetap menjamin aspek-aspek keamanan yang telah dipenuhi metode enkripsi terdahulu, sekaligus menghindari serangan-serangan yang dilakukan terhadap berkas PDF. Hal ini dikarenakan jika penyadap hanya dapat mengakses salah satu *share*, ataupun sepasang *share* tanpa kunci, penyisipan akan mengakibatkan tidak munculnya konten yang bermakna setelah dilakukan dekripsi pada modul kriptografi visual. Dengan skema implementasi, dokumen PDF hanya dapat mengandung konten berbentuk citra untuk setiap halamannya, sehingga pengirim juga dapat menghindari serangan dengan menggunakan *CBC gadget*, yang memiliki syarat harus mengetahui sebagian dari plainteks.

Salah satu kelebihan lainnya adalah kecepatan proses enkripsi dan dekripsi yang dilakukan, jika dibandingkan hanya mengganti modul enkripsi terdahulu menjadi menggunakan modul enkripsi yang lebih aman seperti RSA, yang akan meningkatkan lamanya proses enkripsi dan dekripsi. Kriptografi visual, walaupun memiliki proses enkripsi yang tidak terlalu sederhana, memiliki proses dekripsi yang sangat sederhana, sehingga akan jauh lebih cepat. Namun jika kebutuhan lebih mengutamakan keamanan dan kerahasiaan, selain dengan kedua modul yang telah dispesifikasikan pada skema, dapat juga digunakan modul kriptografi RSA untuk menggantikan modul AES-CBC pada operasi enkripsi share dengan kunci data E, agar dienkripsi dengan menggunakan kunci publik penerima.

Namun masih terdapat juga beberapa kelemahan dari skema implementasi, salah satunya adalah pengirim harus mengendalikan paling kurang 3 (tiga) buah berkas yang berbeda, yaitu pasangan *share* dan kunci enkripsi yang bersesuaian, untuk setiap berkas PDF yang dienkripsi.

Kelemahan lain dari skema implementasi yang diusulkan

adalah keterbatasan fitur PDF yang dapat dimanfaatkan dengan menggunakan implementasi kriptografi visual. Untuk dapat melakukan proses enkripsi dan dekripsi, konten hanya dapat berbentuk gambar untuk setiap halaman, sehingga teks harus pula diubah ke dalam bentuk citra. Telah ada berbagai layanan yang menyediakan *optical character recognition* (OCR) berbasis citra digital, yaitu proses konversi berkas citra digital yang mengandung teks menjadi bentuk berkas teks[10], dokumen PDF yang mengandung konten teks dapat kembali diproses dengan OCR setelah melakukan dekripsi kriptografi visual. Sedangkan fitur-fitur PDF yang lebih kompleks seperti *formatting* untuk teks, serta bentuk formulir dan *hyperlink*, tidak dapat didukung dengan menggunakan kriptografi visual.

V. KESIMPULAN

Dengan memanfaatkan kriptografi visual dan prinsip two-man rule, dapat dibentuk sebuah skema implementasi enkripsi dan dekripsi pada berkas PDF yang dapat terhindar dari sejumlah serangan umum yang dilakukan terhadap berkas PDF yang dienkripsi dengan hanya menggunakan algoritma AES-CBC tanpa menambah waktu proses enkripsi dan dekripsi yang dibutuhkan secara signifikan. Dengan membagi sebuah dokumen menjadi sejumlah *share*, dengan minimal sepasang *share* dengan kunci yang bersesuaian dibutuhkan untuk melakukan proses dekripsi, penerima dapat melakukan validasi konten sebuah PDF dengan menggabungkan pasangan share, dan mendapatkan bukti yang langsung secara visual jika terdapat modifikasi terhadap salah satu ataupun kedua *share* tersebut.

Namun, masih terdapat beberapa kelemahan dari skema yang diusulkan, salah satunya adalah banyaknya jumlah berkas yang harus dikelola oleh pengirim, yaitu 3 (tiga) buah berkas untuk setiap berkas PDF yang dienkripsi. Kelemahan lain dari skema implementasi adalah jenis konten dalam PDF yang didukung terbatas kepada hanya konten dalam bentuk citra. Agar skema dapat mendukung enkripsi dan dekirpsi untuk teks, halaman PDF dapat terlebih dahulu dikonversi menjadi citra sebelum proses enkripsi. Dan setelah melakukan proses dekripsi dapat dimanfaatkan layanan OCR untuk melakukan ekstraksi teks dari citra.

VII. UCAPAN TERIMA KASIH

Segala puji dan syukur penulis panjatkan kehadirat Tuhan YME, karena berkat anugerah hikmat dan karunia-Nya maka penulis dapat menyelesaikan makalah ini. Tidak lupa penulis juga berterima kasih kepada Bapak Ir. Rinaldi Munir sebagai dosen mata kuliah IF4020 Kriptografi, yang membekali penulis dengan berbagai wawasan yang dibutuhkan untuk menulis makalah ini. Penulis juga berterima kasih kepada keluarga penulis, yang mendukung penulis dalam pengerjaan makalah di rumah selama masa pandemi, serta kepada mahasiswa rekan-rekan penulis yang saling memberikan semangat dalam mengerjakan makalah masing-masing.

REFERENSI

[1] Menezes, A. J. (1997). *Handbook of Applied Cryptography*. CRC Press.

[2] Munir, R. (2020). *Pengantar Kriptografi* [PowerPoint slides]. Diakses tanggal 20 Desember 2020 dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pengantar-Kriptografi-(2020).pdf

[3] Adobe Systems Incorporated. (2006). *PDF Reference (Sixth edition, version 1.23)* [PDF document]. Diakses tanggal 20 Desember 2020 dari https://www.adobe.com/content/dam/acom/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf

[4] ISO. (2008). *Document management—Portable document format—Part 1: PDF 1.7* (Standard No. 32000-1:2008) [PDF document]. Diakses tanggal 20 Desember 2020 dari http://wwwimages.adobe.com/www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf

[5] Müller, J., Ising, F., Mladenov, V., Mainka, C., Schinzel, S., & Schwenk, J. (2019, November 6). Practical Decryption exFiltration. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security.

[6] Munir, R. (2020). *Review Beberapa Block Cipher dan Stream Cipher (Bagian 4: Advanced Encryption Standard (AES))* [PowerPoint slides]. Diakses tanggal 20 Desember 2020 dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Review-beberapa-block-cipher-dan-stream-cipher-2020-bagian4.pdf

[7] Munir, R. (2020). *Kriptografi Visual, Teori dan Aplikasinya (Bagian 1)* [PowerPoint slides]. Diakses tanggal 20 Desember 2020 dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian1.pdf

[8] Munir, R. (2020). *Kriptografi Visual, Teori dan Aplikasinya (Bagian 2)* [PowerPoint slides]. Diakses tanggal 20 Desember 2020 dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-z2021/Kriptografi-Visual-Bagian2.pdf

[9] Sullivan, Nick. "Red October: CloudFlare's Open Source Implementation of the Two-Man Rule." *The Cloudflare Blog*, 27 Aug. 2018. Diakses tanggal 21 Desember 2020 dari blog.cloudflare.com/red-october-cloudflares-open-source-implementation-of-the-two-man-rule/

[10] Nicomsoft. "Optical Character Recognition (OCR) – How It Works." *Nicomsoft*. Diakses tanggal 21 Desember 2020 dari www.nicomsoft.com/optical-character-recognition-ocr-how-it-works/.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2020

Saskia Imani 13517142