PENERAPAN METODE KRIPTOGRAFI RSA PADA PENGIRIMAN DOKUMEN *MERCHANT* BANK XYZ

Saputra Prakarsa
Program Studi Teknik Informatika Universitas Darma Persada
Jl. Raden Inten II, Pondok Kelapa, Jakarta Timur
Email: prakarsa1031@gmail.com

ABSTRAK

Sistem pengiriman dokumen merupakan salah satu pilihan yang tepat bagi sebuah perusahaan untuk mengirimkan dan meyimpan banyak data secara rapih dan baik. Permasalahan pada saat ini, Perusahaan Bank XYZ belum menggunakan teknologi sistem pengiriman dan penyimpanan file berbasis website, sehingga merasakan dampak kesulitan dalam mencari file yang pernah di kirimkan melalui banyak media yang lain. Dalam mewujudkan hal tersebut, maka Bank XYZ membuat sebuah sistem pengiriman dokumen. Sistem pengiriman dokumen berbasis website ini bekerja dengan menggunakan perangkat komputer perusahaan secara Online. Sistem pengiriman dokumen ini juga ditujukan untuk menyimpan dokumen secara aman dengan metode enkripsi RSA. Tujuan sistem pengiriman dokumen ini untuk memberikan kemudahan dalam mengirimkan dan menyimpan dokumen *Merchant* perusahaan.

ABSTRACT

The document delivery system is one of the right choices for a company to send and store a lot of data neatly and properly. The problem at this time, XYZ Bank Company has not used the technology of website-based file storage and storage systems, so that it feels the impact of the difficulty in finding files that have been sent through many other media. In realizing this, Bank XYZ created a document delivery system. This website-based document delivery system works by using a company computer online. The document delivery system is also intended to store documents securely with the RSA encryption method. The purpose of this document delivery system is to provide convenience in sending and storing company Merchant documents.

Keywords : *upload file*, PHP, *Online*, RSA, Encryption, Description.

1. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi yang semakin pesat membuat manusia ingin melakukan semuanya dengan serba cepat dan tepat dalam melakukan sesuatu. Saat ini, website merupakan salah satu pilihan yang memegang peranan penting dalam kegiatan bisnis. Website dapat digunakan untuk mengolah data – data dan menampilkannya menjadi informasi yang berguna bagi pemakainya. Penggunaan website semakin mengalami kemajuan dari waktu ke waktu, baik dari segi jumlah pemakai dan manfaat yang didapatkan.

Bank adalah adalah sebuah lembaga intermediasi keuangan, umumnya didirikan dengan kewenangan untuk menerima simpanan uang, meminjamkan uang, dan menerbitkan promes atau yang dikenal sebagai banknote. Kata bank berasal dari bahasa Italia *banca* berarti tempat penukaran uang . Sedangkan menurut undang-undang perbankan, bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak.

Dalam menjalankan kegiatan perbankan, ada beberapa proses yang harus dilakukan. Dalam hal ini, Bank XYZ juga memiliki suatu proses dan syarat bagi suatu badan usaha yang ingin bekerja sama dengan Bank XYZ. Salah satunya adalah unit *Transaction Banking Retail Sales* (TBRS) dengan bagian *Transaction Banking Electronic* (TBE) yang menekuni bidang *E-Commerce.* Dalam Hal ini, pihak *Merchant* (Sebutan untuk Badan Usaha yang akan bekerja sama dengan Bank XYZ) wajib menyertakan beberapa dokumen untuk menyelesaikan proses kerja sama, seperti Akta dan Kemenhum, KTP Direktur, SK Domisili, Foto Lokasi, NPWP, dll. Dokumen – dokumen tersebut akan di berikan pada masing – masing *Region* (Sebutan cabang Bank XYZ, di mana ada 12

lokasi yang mengurus hal ini), dan melalui *Region* tersebut, maka akan dikirimkan ke cabang pusat.

Pada saat ini, proses pengiriman file dokumen *merchant* dari pihak *region* ke cabang pusat masih menggunakan via *email*. Kendala yang di alami dalam unit ini adalah ketika pihak *region* mengirimkan dokumen tersebut kepada salah seorang pihak pusat yang lebih dikenal oleh *region* tesebut, maka pihak yang lain tidak bisa melihat dokumen tesebut, kecuali pihak *region* mengenal dan mengirimkan dokumen tesebut ke seseorang dari pihak pusat lainnya. Namun permasalahan yang lebih besar adalah ketika pihak pusat yang sudah lebih lama bekerja dan lebih dikenal oleh *region* – *region* memutuskan untuk *resign* (sebutan keluar dari pekerjaan). Hal ini membuat dokumen – dokumen *merchant* tersebut tidak terarsipkan dengan baik.

Untuk itu, pihak unit *Transaction Banking Electronic* (TBE) berkeinginan membuat sistem website, dimana ada akun user untuk seluruh *region* dalam mengupload dokumen – dokumen pihak *merchant*, serta dokumen – dokumen tersebut dapat diterima oleh akun pihak pusat. Melalui website ini, maka pihak pusat tidak perlu lagi kerepotan dengan masalah - masalah yang sudah disebutkan sebelumnya.

2. TINJAUAN PUSTAKA

2.1 PHP

PHP singkatan dari PHP: *Hypertext Preprosessor*. Ia merupakan bahasa berbentuk skrip yang ditempatkan dalam *server* dan diproses di *server*. Secara khusus PHP dirancang untuk membentuk *web* dinamis. Artinya ia dapat berbentuk suatu tampilan berdasarkan permintaan terkini. Misalnya, menampilkan isi *database* ke halaman *web*. PHP bersifat bebas dipakai. Anda tidak perlu membayar apapun untuk menggunakan perangkat lunak ini. Kode php di awali dengan <?php dan di akhiri dengan ?> . Pasangan kedua kode inilah yang berfungsi sebagai *tag* kode PHP.

Salah satu kelebihan dari PHP adalah mampu berkomunikasi dengan berbagai *database* yang terkenal. Dengan demikian menampilkan data yang bersifat dinamis yang diambil dari *database* merupakan hal yang mudah untuk diimplementasikan. Pada saat ini PHP sudah dapat berkomunikasi dengan berbagai *database* meskipun memiliki kelengkapan yang berbeda-beda.(Artanto. 2013).

2.2 Basis Data

Basis data dan teknologi basis data memiliki dampak yang besar terhadap meningkatnya pengguna komputer. Adil untuk mengatakan bahwa basis data memainkan peranan penting di hampir semua area, di mana computer tersebut digunakan termasuk dunia usaha, perdagangan elektronik, teknik, kedokteran, genetika, hukum, pendidikan, dan ilmu perpustakaan. Kata basis data sangat umum digunakan, maka harus dimulai dengan mendefinisikan apa arti dari basis data itu sendiri. Menurut Ramez Elmasri, Shamkant B. Navanthe dalam Fundamentals of Basis data Systems 6th edition (2011 , 4) Basis data adalah kumpulan data yang terkait. Dengan data, fakta yang diketahui, direkam dan memiliki makna yang implisit.

2.2.1 SQL

Bahasa SQL dapat dianggap sebagai salah satu alasan utama keberhasilan komersial dari basis data relasional. Karena itu menjadi standar untuk database relasional, pengguna kurang peduli tentang migrasi aplikasi database mereka dari jenis sistem basis data lainnya misalnya jaringan atau sistem hirarki ke basis data relasional. Hal ini karena jika pengguna menjadi tidak puas dengan produk DBMS relasional tertentu yang digunakan, makan pengguna mengkonversi ke produk DBMS relasional yang lain tidak diharapkan terlalu mahal dan memakan waktu karena kedua sistem mengikuti standar bahasa yang sama. Keuntungan lain dari memiliki standarisasi adalah bahwa pengguna dapat menulis pernyataan dalam program aplikasi database yang dapat mengakses data yang disimpan dalam dua atau lebih DBMS relasional tanpa harus mengubah sub-bahasa basis data (SQL) jika kedua DBMS relasional mendukung standar SQL.

2.3 Kriptografi

Kriptografi merupakan merupakan studi metode untuk mengirim pesan secara rahasia (yaitu, dienkripsi atau disamarkan) sehingga hanya penerima yang dimaksud dapat menghapus penyamaran dan membaca pesan (atau menguraikannya). Kata krriptografi memiliki *etimologi*, yaitu kripto dari Bahasa Yunani, artinya tersembunyi, dan graphein, artinya menulis. Pesan asli disebut plaintext, dan pesan tersamar disebut ciphertext. Pesan yang telah dienkapsulasi dan dikirim, disebut *cryptogram*.

2.3.1 RSA

Menurut (Sentot Kromodimoeljo dalam Teori dan Aplikasi Kriptograf Teori dan Aplikasi Kriptograf (2009), Tahun 1978, Len Adleman, Ron Rivest dan Adi Shamir mempublikasikan

sistem RSA. Semula sistem ini dipatenkan di Amerika Serikat dan seharusnya masa paten habis tahun 2003, akan tetapi RSA Security melepaskan hak paten setelah 20 September 2000. Sebetulnya sistem serupa telah dilaporkan oleh Clifford Cocks tahun 1973 meskipun informasi mengenai ini baru dipublikasi tahun 1997 karena merupakan hasil riset yang diklasifikasikan sangat rahasia oleh pemerintah Britania Raya (Clifford Cocks bekerja untuk GCHQ, suatu badan di Britania Raya yang fungsinya serupa dengan fungsi NSA di Amerika Serikat), jadi validitas paten patut dipertanyakan karena adanya prior art.

2.17 UML

1. Definisi *Unified Modelling Language* (UML)

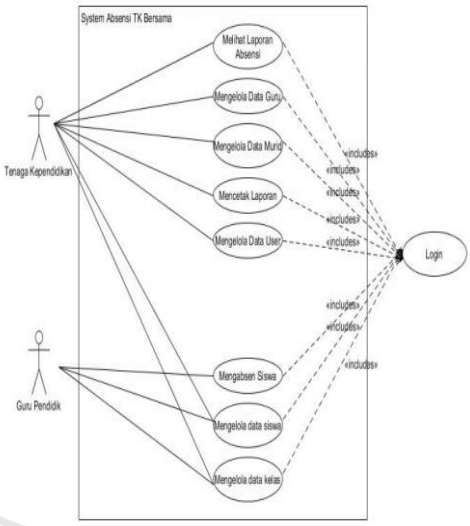
UML adalah Bahasa standar untuk membuat rancangan *software*. UML biasanya digunakan untuk menggambarkan dan membangun, dokumen artifak dari *software – intensive system*. UML awalnya termotivasi oleh keinginan untuk membakukan sistem notasi yang berbeda dan pendekatan untuk desain perangkat lunak yang dikembangkan oleh Grady Booch , Ivar Jacobson dan James Rumbaugh di *Rational Software* di 1994-1995, dengan pengembangan lebih lanjut yang dipimpin oleh mereka melalui tahun 1996. Pada tahun 1997 UML diadopsi sebagai standar oleh *Object Management Group* (OMG), dan telah dikelola oleh organisasi ini sejak. Pada tahun 2005 UML juga diterbitkan oleh *International Organization for Standardization* (ISO) sebagai standar ISO disetujui. Sejak itu telah periodik direvisi untuk menutupi revisi terbaru dari UML. (Booch. 2005:7)

2. Diagram-Diagram UML

Ada beberapa diagram yang disediakan UML antara lain :

a. Diagram *Use Case*

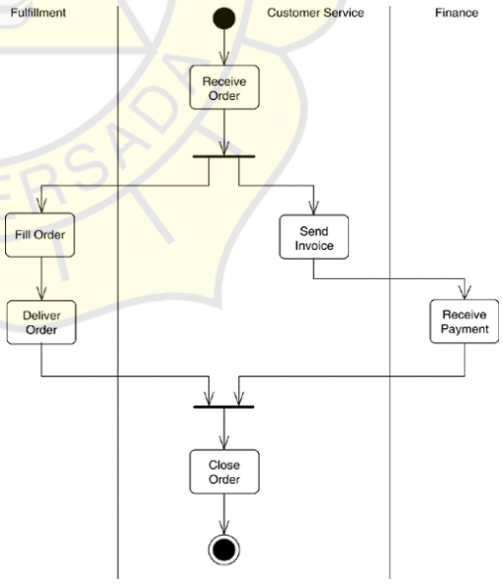
Diagram untuk menunjukkan peran dari berbagai pengguna dan bagaimana peran-peran menggunakan sistem. Diagram *use case* digunakan untuk memodelkan bisnis proses berdasarkan perspektif pengguna sistem. Diagram use case terdiri atas diagram untuk *use case* dan *actor*. *Actor* merepresentasikan orang yang akan mengoperasikan atau orang yang berinteraksi dengan sistem aplikasi. *Use case* merepresentasikan operasi-operasi yang dilakukan oleh *actor*. *Use case* digambarkan berbentuk *elips* dengan nama operasi dituliskan didalamnya. *Actor* yang melakukan operasi dihubungkan dengan garis lurus ke *use case*. (Satzinger et al. 2009:242).



Gambar 1 Contoh Diagram *Use Case* (Pratama. 2019)

b. Diagram Aktivitas

Diagram aktivitas adalah teknik untuk menggambarkan logika prosedural, proses bisnis, dan jalur kerja. Dalam beberapa hal, diagram aktivitas memainkan peran mirip dengan diagram alir, tetapi perbedaan prinsip antara notasi diagram alir adalah diagram aktivitas mendukung *behavior paralel. Node* pada sebuah diagram aktivitas disebut sebagai *action*, sehingga diagram tersebut menampilkan sebuah diagram aktivitas yang tersusun dari *action*. (Fowler. 2005:163)



Gambar 2 Contoh Diagram Aktivitas (Pratama. 2019)

c. Diagram Sekuensial

Diagram Sekuensial merupakan grafik dua dimensi dimana obyek ditunjukkan dalam dimensi horizontal, sedangkan *lifeline*

ditunjukkan dalam dimensi vertikal. Banyaknya diagram sekuensial yang harus digambar adalah minimal banyak pendefinisian *use case* yang memiliki proses sendiri atau yang penting semua *use case* yang telah didefinisikan interaksi jalannya pesan sudah dicakup pada diagram sekuensial sehingga semakin banyak *use case* yang didefinisikan maka diagram sekuensial

dalam arsitektur dan teknologi yang digunakan saat ini. Umpan balik ini diberikan oleh sistem yang sedang berjalan, tetapi hanya akan bekerja dengan orang yang terlatih dan memiliki komitmen serta tanggung jawab atas berbagai proses yang digambarkan dalam SPDLC tersebut. (Goldman et al. 2004)

3. METODOLOGI

Metodologi yang digunakan dalam penelitian ini adalah *waterfall*. Berikut penjelasan tahap-tahap yang dilakukan dalam penelitian ini:

1. Requirements analysis and definition

Layanan sistem, kendala, dan tujuan ditetapkan oleh hasil konsultasi dengan pengguna yang kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.

2. *System and software design*

Tahapan perancangan sistem mengalokasikan kebutuhan-kebutuhan sistem baik perangkat keras maupun perangkat lunak dengan membentuk arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan penggambaran abstraksi sistem dasar perangkat lunak dan hubungannya.

3. Implementation and unit testing

Pada tahap ini, perancangan perangkat lunak direalisasikan sebagai serangkaian program atau unit program. Pengujian melibatkan verifikasi bahwa setiap unit memenuhi spesifikasinya.

4. Integration and system testing

Unit-unit individu program atau program digabung dan diuji sebagai sebuah sistem lengkap untuk memastikan apakah sesuai dengan kebutuhan perangkat lunak atau tidak. Setelah pengujian, perangkat lunak dapat dikirimkan ke customer.

5. Operation and maintenance

tahapan ini merupakan tahapan yang paling panjang. Sistem dipasang dan digunakan secara nyata. Maintenance.

4. PEMBAHASAN

4.1 Analisis Sistem Bank XYZ

Bank XYZ pada saat ini, proses pengiriman file dokumen merchant dari pihak region ke yang harus dibuat juga semakin banyak. (Munawar. 2005 : 28)

2.18 Security Policy Development Life Cycle (SPDLC)

SPDLC digambarkan sebagai suatu siklus yang dimulai dari tahap evaluasi yang memvalidasi efektivitas dari tahap analisa awal. Umpan balik dari hasil evaluasi ini bisa berdampak pada perubahan

cabang pusat masih menggunakan via email. Kendala yang di alami dalam unit ini adalah ketika pihak region mengirimkan dokumen tersebut kepada salah seorang pihak pusat yang lebih dikenal oleh region tesebut, maka pihak yang lain tidak bisa melihat dokumen tesebut, kecuali pihak region mengenal dan mengirimkan dokumen tesebut ke seseorang dari pihak pusat lainnya. Namun permasalahan yang lebih besar adalah ketika pihak pusat yang sudah lebih lama bekerja dan lebih dikenal oleh region – region memutuskan untuk resign (sebutan keluar dari pekerjaan). Hal ini membuat dokumen – dokumen merchant tersebut tidak terarsipkan dengan baik.

Untuk itu, pihak unit Transaction Banking Electronic (TBE) berkeinginan membuat sistem website, dimana ada akun user untuk seluruh region dalam mengupload dokumen – dokumen pihak merchant, serta dokumen – dokumen tersebut dapat diterima oleh akun pihak pusat. Melalui website ini, maka pihak pusat tidak perlu lagi kerepotan dengan masalah - masalah yang sudah disebutkan sebelumnya.

4.2 Analisis Sistem Baru

Solusi dari permasalahan diatas adalah dengan membangun sebuah sistem Website untuk melakukan Pengiriman Dokumen *Merchant* dengan metode RSA. Dengan sistem ini *Administrator* bisa melakukan pengiriman dan unduh dokumen secara aman, serta pengarsipan dokumen yang baik.

4.3 Kebutuhan Perangkat Keras

Pada penelitian yang dilakukan, dibutuhkan perangkat keras (*hardware*) untuk menunjang implementasi pada sistem yang dibuat adalah sebagai berikut :

4.3.1 Komputer

Komputer merupakan alat yang digunakan untuk membuka website pengiriman dokumen *merchant* secara *online*. Komputer yang dijalankan dengan spesifikasi sebagai berikut :

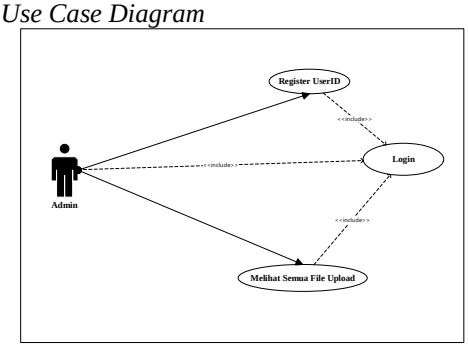
1. CPU 4 *core*, ruang penyimpanan 500 GB, memory 8 GB RAM
2. *Operating System* Windows 10.
3. *Browser Google Chrome*

4.5 Perancangan Sistem

Pada bagian ini akan dijelaskan mengenai

perancangan *Use Case Diagram, Sequence Diagram, Activity Diagram* dan *Deployment Diagram.*

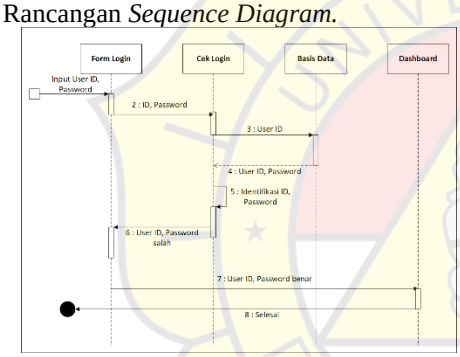
4.5.1 Use Case Diagram



Gambar 3.1 *Rancangan Use Case Diagram*

Pada gambar 3.1 diketahui bahwa admin dapat melakukan registrasi id user, & melihat hasil unggahan berkas dari semua user. Proses – proses yang telah disebutkan di atas dapat dilakukan oleh admin dengan melakukan login terlebih dahulu.

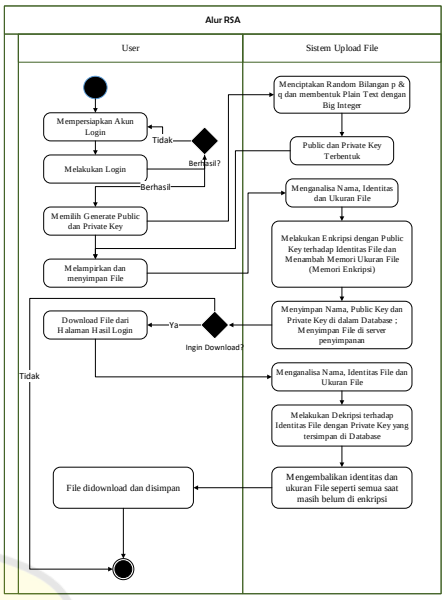
4.5.2 Rancangan *Sequence Diagram.*



Gambar 3.2 Rancangan *Sequence Diagram.*

Dalam gambar 3.2 menjelaskan proses seorang admin atau user melakukan login di website pengiriman berkas *Merchant*. Login admin atau user dilakukan dengan menginputkan id dan password, lalu id tersebut akan di cek oleh basis data. Jika id terdaftar dalam basis data, maka basis data akan mencocokkan password id yang terdaftar dalam Basis Data dengan password yang telah diinputkan oleh admin atau user. Jika Password tersebut cocok, maka tampilan halaman akan mengarah ke dashboard dan proses login admin atau user telah selesai.

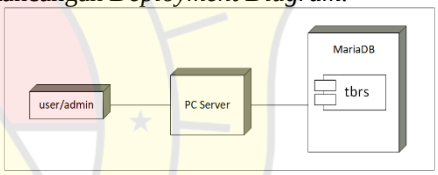
4.5.3 Rancangan *Activity Diagram.*



Gambar 3.3 Rancangan *Activity Diagram.*

Dari activity diagram gambar 3.7 , activity diagram diatas dapat diketahui bagaimana alur proses kerja metode RSA dalam melakukan enkripsi saat melakukan upload file dan dekripsi saat melakukan download file.

4.5.3 Rancangan *Deployment Diagram.*



Gambar 3.4 Rancangan *Deployment Diagram.*

Pada gambar 3.4 Deployment Diagram di atas memperlihatkan hubungan keseluruhan antara perangkat-perangkat keras/aplikasi user/admin dan server yang terdapat database dari sistem aplikasi tersebut. PC Server menjadi jalur informasi antara user/admin dengan database. Admin dapat mengakses database melalui PC Server. Demikian sebaliknya, database akan mengirimkan data kepada user/admin melalui PC Server.

4.6 Perancangan Database

Database berisi tabel “tb_user” dan Tabel “tb_document.

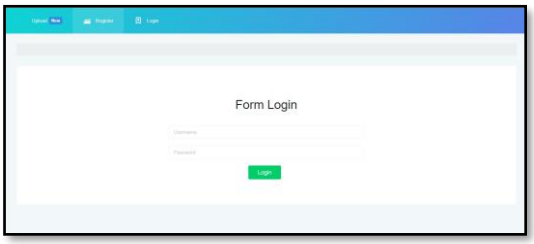
4.7 Hasil Implementasi

Hasil implementasi ini merupakan hasil dari perancangan penerapan metode kriptografi RSA pada pengiriman dokumen *Merchant* Bank XYZ. Ini adalah beberapa tampilan hasil implementasi sebagai berikut :

4.7.1 Tampilan Halaman Login

Halaman utama login di gunakan untuk melakukan verifikasi pengguna, apakah pengguna yang akan menggunakan adalah admin

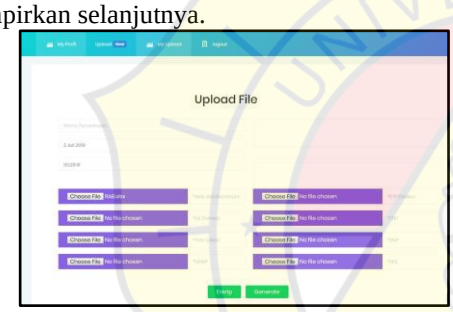
atau user. Pada halaman berikut ini adalah gambar tampilan login yang berisi kolom username dan password yang wajib di isi untuk dapat ke halaman selanjutnya.



Gambar 4.7 Tampilan halaman login

4.3.1 Tampilan Halaman Upload

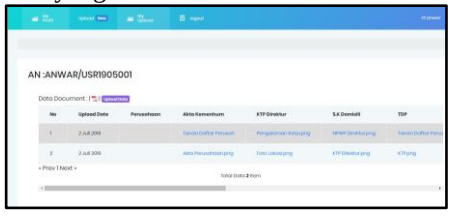
Pada halaman ini, pengguna dapat melakukan proses pengiriman bekas dengan melakukan input nama perusahaan dan melampirkan delapan berkas di masing – masing kolom yang tersedia. Sebelum melakukan pelampiran file, pengguna wajib memilih tombol "generate" guna menerapkan pengamanan data dengan metode RSA pada berkas yang akan dilampirkan selanjutnya.



Gambar 4.8 Tampilan halaman *upload*

4.3.2 Tampilan Halaman Hasil *Upload*

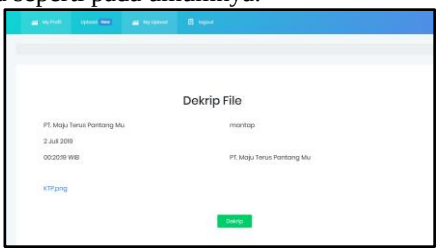
Halaman hasil upload berisi daftar berkas – berkas yang telah dikirimkan user melalui halaman upload sebelumnya. Pada halaman ini, Admin dapat melihat, menyimpan dan menghapus semua hasil upload berkas dari setiap user, sedangkan user hanya dapat melihat, menyimpan dan menghapus hasil upload akun sendiri dan tidak dapat melihat hasil upload yang dilakukan oleh user lain. Pada halaman ini juga berisi rincian tanggal upload berkas dan nama perusahaan yang memiliki berkas tersebut.



Gambar 4.9 Tampilan halaman Hasil *Upload*

4.3.3 Tampilan Halaman *Download*

Halaman download ini berisikan rincian berkas (nama perusahaan, waktu upload, keterangan, dan lain sebagainya) yang akan di lihat/disimpan oleh admin ataupun user yang melakukan upload berkas. Dalam proses mendownload, berkas tersebut akan disimpan dengan melakukan dekripsi terlebih dahulu. Kunci untuk melakukan dekripsi berkas tersebut adalah disebut "public key". Apabila tidak melakukan dekripsi terlebih dahulu, maka berkas tersebut akan tersimpan namun tidak dapat terbuka seperti pada umumnya.



Gambar 4.10 Tampilan *Download*

5. HASIL PENGUJIAN

Hasil Pengujian

Berikut ini adalah hasil pengujian beberapa file dengan format Txt, Docx, Pdf, Jpg, Png, Xlsx dan Pptx untuk mengukur tingkat perbedaan enkripsi dari masing – masing file. Pada proses enkripsi ini, yang pertama dilakukan adalah menekan tombol "*generate*" pada aplikasi untuk melakukan pembentukan *public key* dan *private key* sebagai kunci enkripsi dan dekripsi. Dalam melakukan "*generate key"*, setiap kali pembentukannya akan menghasilkan kunci yang berbeda. Ini merupakan ciri khas dari kunci RSA pada sistem ini, karena dibuat secara random setiap dilakukan pembentukan kunci. Dimana kunci ini akan merubah *Plaintext* yang sedari awal sudah bebentuk ASCII dan menjadi identitas sebuah file grafik (seperti doc, txt, jpg, ppt, pdf, dll).

Pada proses pembuatan kunci untuk melakukan pengujian ini, sistem membuat 2 bilangan prima dengan karakter yang sangat besar dan secara acak dengan menggunakan proses Big Integer (Perlu dilakukan agar tidak menyebabkan *overflow*, mengingat ukuran *chipertext* yang akan dibuat besar). Kedua bilangan ini dikenal dengan istilah "P" dan "Q". Adapun kedua bilangan prima yang tercipta saat proses pengujian ini berlangsung adalah :

Bilangan P :

'G?\6g W n TP-~dH6 1C>

Dan Bilangan Q :

S 3" Jm5- 6 2p D w) yT /

P dan Q yang terbentuk diatas merupakan bilangan ASCII yang umumnya memiliki DEC antara 00 sampai 32 dan 128 seterusnya. Dimana bilangan ini tdak dapat dibaca karena merupakan karakter yang tidak biasa pada umumnya. Namun apabila kedua bilangan prima ASCII tersebut di terjemahkan ke desimal, maka akan menjadi seperti berikut :
Bilangan P :

65533 32 39 65533 65533 19 71 65533 65533 63 65533 65533 92 54 65533 65533 65533 4 1969 65533 87 65533 65533 51211 110 65533 65533 65533 65533 65533 65533 65533 84 80 45 32 65533 126 5 100 72 54 65533 17 65533 19 11 65533 32 65533 65533 65533 65533 49 17 26 17 67 15 62 65533

Dan Bilangan Q :
65533 65533 21 65533 9 65533 83 65533 20 65533 65533 65533 31 65533 1765 65533 26 32 65533 34 51 4 65533 65533 74 109 53 65533 31 65533 21 23 65533 65533 54 65533 50 112 65533 65533 65533 68 65533 8 65533 12 65533 119 65533 65533 41 65533 16 65533 5 65533 121 84 65533 32 27 47

Dari P dan Q yang telah terbentuk di atas, kita dapat menentukan *Public Key* dengan rumus gcd (Φ(p.q), e) =1 , Maka hasilnya adalah sebagai berikut :

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCx5+T/5u0oPmLq5mHTu8r8olks81V9L5eDyhNuH+Ap74fOMcWtEB+8Eov5GRjkxHkuwFD+nV2QzbBuhQyq+n+JG4jUOdjONZmmFU4y5B1GmscYRJd2+VoRhhaUi4CU1Ow0rKeqjHyrrNzgwMVWWzPKC6/+qHu31vAaXD0AvCvp5wIDAQAB

Yang apabila bilangan ASCII *Public Key* tersebut diterjemahkan ke dalam desimal akan mejadi seperti berikut :

77 73 71 102 77 65 48 71 67 83 113 71 83 73 98 51 68 81 69 66 65 81 85 65 65 52 71 78 65 68 67 66 105 81 75 66 103 81 67 120 53 43 84 47 53 117 48 111 80 109 76 113 53 109 72 84 117 56 114 56 111 108 107 115 32 56 49 86 57 76 53 101 68 121 104 78 117 72 43 65 112 55 52 102 79 77 99 87 116 69 66 43 56 69 111 118 53 71 82 106 107 120 72 107 117 119 70 68 43 110 86 50 81 122 98 66 117 104 81 121 113 43 110 43 74 71 52 106 85 32 79 100 106 79 78 90 109 109 70 85 52 121 53 66 49 71 109 115 99 89 82 74 100 50 43 86 111 82 104 104 97 85 105 52 67 85 49 79 119 48 114 75 101 113 106 72 121 114 114 78 122 103 119 77 86 87 87 122 80 75 67 54 47 43 32 113 72 117 51 49 118 65 97 88 68 48 65 118 67 118 112 53 119 73 68 65 81 65 66

Dan *Private Key* dapat terbentuk dengan menggunakan rumus e-1 (mod Φ(n)) , adapun *Private Key* yang terbentuk saat data hasil pengujian ini dibuat adalah :

MIICXAIBAAKBgQCx5+T/5u0oPmLq5mHTu8r8olks81V9L5eDyhNuH+Ap74fOMcWtEB+8Eov5GRjkxHkuwFD+nV2QzbBuhQyq+n+JG4jUOdjONZmmFU4y5B1GmscYRJd2+VoRhhaUi4CU1Ow0rKeqjHyrrNzgwMVWWzPKC6/+qHu31vAaXD0AvCvp5wIDAQABAoGADjKBVeKp3mJMJo7IE8uSwWJ7V1j744eewceokUs96lrRLaVPLyZwQeQBA5n7IJaFTTPPwuHwC5Q+ljNL9YEUGEy+QDjTWPlqwFcgmka3eS0jTStvtATPCnWQsHUFuHo2za7Vfe3Y4LAdeS3hZci+UP6MUoKv8kyH/M/eaXnIb3ECQQDBbgBGWzjRR206YBjRMcdmjgs+Tu7WWfW9SlM7Vdc00IfPNo6RkfVAIXe+MoNNhFp94Hh0/Abrvhn9XF3fdHprAkEA63RbMRa0MSJ12c6buPcNz0SWb3rHjHszWQqdQJe5a0dwrR8I0yGbQjyrHzqiyJC1gf+jOiImw1ZacVHvT1uldQJAOs4KX1lUSKuCVYDpio+ro04DtQmiKqBmyQlTjHJoXrIW17QqW68X9Es4cCZDLMnUCPi5JjeIkxrUI+Z0035ByQJBAMNwZs19Wf666vXrMIk80MKt3O0WDhNGpF2RmOvnxOoOd7HL4+hUqeo2L5iRdFNlArSwfE2h0WktAY+0gh7uJI0CQGtsw8UyhgqoUHYHl/NuU0iKEblhb1lFK89yPbvaDTlDvd+4m24Je/pHhPBzA8MdNXwWJnE9zXNHVd8kPHT8/mU=

Yang apabila bilangan ASCII *Private Key* diatas diterjemahkan ke dalam desimal akan mejadi seperti berikut :

89 97 110 103 32 97 112 97 98 105 108 97 32 98 105 108 97 110 103 97 110 32 65 83 67 73 73 32 116 101 114 115 101 98 117 116 32 100 105 116 101 114 106 101 109 97 104 107 97 110 32 107 101 32 100 97 108 97 109 32 100 101 115 105 109 97 108 32 97 107 97 110 32 109 101 106 97 100 105 32 115 101 112 101 114 116 105 32 98 101 114 105 107 117 116 32 58

Public Key dan *Private Key* yang terbentuk di atas memiliki jumlah karakter yang jauh lebih banyak dibandingkan RSA yang di terapkan pada teks. Alasan mengapa RSA yang diterapkan pada file memiliki karakter yang lebih panjang adalah karena *Plaintext* yang dimiliki sebuah file umunya jauh lebih banyak dari pada sekedar teks biasa. Sebagai contoh, apabila sekedar mengenkripsi kata “halo” maka akan membentuk *Public Key* dan *Private Key* yang lebih panjang dibandingkan kata “halo” yang tertulis di file (doc, pdf, dll). Lalu *Public Key* dan *Private* Key yang terbentuk di atas akan

tersimpan dalam sistem, sehingga pengirim file hanya perlu melakukan upload seperti biasa.

Masing – masing file yang akan di upload memiliki beberapa karakter *Plaintext* sebagai identitas file tersebut, yang apabila di rubah akan membuat file tersebut tidak dapat terbaca dengan baik. Kunci *Public Key* akan berfungsi sebagai pengunci file dan mengubah *Plaintext* file tersebut menjadi *Chipertext*. Sehingga file akan berubah menjadi tidak terbaca. Berdasarkan hasil pengujian yang dilakukan, dapat di simpulkan bahwa proses enkripsi dengan menggunakan *Publick Key* menyebabkan karakter *Plaintext* yang dirubah ke *Chipertext* menjadi lebih banyak dan menyebabkan size file bertambah.

Tabel 4.5 Data Uji Coba Aplikasi

No	Panjang Karakter			Jenis File	Size File Enkripsi		Durasi
	Isi Teks	Plaintext	Chipertext		Sebelum	Sesudah	
1	4	4	110	Txt	1 KB	1 KB	3.6 Detik
2	15	15	115	Txt	1 KB	1 KB	3.7 Detik
3	4	9.337	12.825	Docx	12 KB	17 KB	12.9 Detik
4	15	9.362	12.871	Docx	12 KB	17 KB	15.7 Detik
5	4	136.276	202.357	Pdf	178 KB	264 KB	2 Menit 25 Detik
6	15	138.482	205.604	Pdf	180 KB	268 KB	2 Menit 37 Detik
7		97.85	138.66	Jpg	121 KB	180 KB	1 Menit 36 Detik
8	15	6.711	9.076	Xlsx	8 KB	12 KB	10.8 Detik
9		57.258	84.243	Png	73.6 KB	109 KB	1 Menit 2 Detik
10		46.162	66.01	Pptx	57.5 KB	86 KB	48 Detik
11		18.866	28.014	Gif	25 KB	37 KB	20 Detik

6. KESIMPULAN

Berdasarkan hasil perancangan, implementasi dan hasil pengujian Penerapan Sistem Kriptografi RSA pada Pengiriman Dokumen *Merchant* Bank XYZ, maka dapat diambil beberapa kesimpulan sebagai berikut:

a. Dengan adanya aplikasi ini, maka berkas yang telah dikirimkan akan lebih mudah di arsipkan sesuai dengan urutan tanggal dan dapat dengan mudah diambil kembali sewaktu – waktu di waktu yang akan datang.
b. Aplikasi ini adalah aplikasi berbasis web yang dikembangkan dengan menggunakan bahasa pemrograman PHP dan Database MySQL. Metode yang digunakan adalah Enkripsi dan Dekripsi RSA (Rivest-Shamir-Adleman).
c. Aplikasi ini memberikan rasa aman dalam mengirimkan berkas yang bersifat rahasia dan hanya di tujukan untuk dilihat oleh admin atau beberapa orang yang diberikan hak akses.
d. Pemeliharaan sistem dapat dilakukan secara berkala dengan terus memperhatikan tingkat keberhasilan dan kekurangan pengguna dalam memakai aplikasi ini dalam jangka waktu 1 tahun kedepan.

REFERENSI

[1] Alan Beaulieu, “Learning SQL Second Edition”, O’Reilly, 2009.

[2] Ian Sommerville, “*SOFTWARE ENGINEERING, 9TH EDITION”,* McGraw-Hill, 2011.

[3] James Rumbaugh, Ivar Jacobson, Grady Booch, “The Unified Modeling Language Reference Manual Second Edition”, Addison-Wesley, 2005.

[4] Jeffrey L. Whitten, Lonnie D. Bentley, Kevin C. Dittman, “Systems Analysis and Design Method Seventh Edition”, McGraw-Hill/Irwin, 2007.

[5] Kenneth E.Kendall, Julie E.Kendall “ System Analysis and Design Eight Edition”, Pearson Education, Inc.,Prentice Hall, 2011.

[6] Kevin Tatroe, Peter Macintyre, Rasmus Lerdorf, “Programming PHP Third Edition”, O’Reilly Media, Inc, 2013.

[7] Ramez Elmasri, Shamkant B. Navathe, “ Fundametals Of Database Systems Sixth Edition”, Pearson Education, Inc,Addison-Wesley,2011.

[8] Sentot Kromodimoeljo, “TEORI&APLIKASI KRIPTOGRAFI”, SPK IT Consulting, 2009.

Sugiyono. 2013. Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.