Jurnal Pendidikan Teknologi dan Kejuruan
Vol. 17, No. 2, Juli 2020
P-ISSN : 0216-3241 E-ISSN : 2541-0652

KRIPTOGRAFI SIMETRIS RC4 PADA TRANSAKSI ONLINE BOOKING ENGINE SYSTEM

Ketut Agus Seputra[1)], Gede Arna Jude Saskara [2)]

[1,2] Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha
Email: agus.seputra@undiksha.ac.id[1], judesaskara@gmail.com[2]

ABSTRAK

Perkembangan industri pariwisata di Bali membawa dampak pada makin meningkatnya persaingan bisnis pariwisata di Bali. Persaingan dapat terlihat dari munculnya agent-agent wisata baru di Bali. Untuk dapat bertahan dalam persaingan industri pariwisata, pelaku pariwisata tersebut harus mampu memanfaatkan peluang dalam meraih keuntungan dengan cara mengoptimalkan efektivitas pemasaran dan dan keuntungan. Salah satu cara yang dapat ditempuh adalah dengan penjualan/transaksi paket wisata secara online melalui internet booking engine system (BES). Terdapat isu utama dalam aktivitas transaksi secara online, yaitu masalah keamanan informasi. Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Penerapan keamanan informasi khususnya dalam transaksi paket wisata online dapat berupa penggunaan metode kriptografi menggunakan algoritma RC4. Keefektifan dan kemudahan pemrosesan, membuat algoritma RC4 mudah dan ringan untuk diimplementasikan. Algoritma RC4 diimplementasikan guna melakukan enkripsi data pelanggan yang disimpan dalam basis data. Informasi yang sudah disimpan tersebut akan ditampilkan kembali ke plaintext melalui proses dekripsi menjadi informasi yang sebenarnya. Modul kritptografi disisipkan pada aplikasi, yaitu pada akhir proses transaksi sebelum data tersimpan. BES yang dibuat menggunakan framework codeigniter sangat mendukung untuk implementasi kriptografi dengan efisien. Pengujian algoritma dilakukan terhadap 922 baris data dengan melihat waktu dan memori yang digunakan dalam melakukan enkripsi hingga dekripsi. Hasil pengujian performa menunjukkan bahwa panjang kunci mempengaruhi waktu pemrosesan data. Pengujian berikutnya dilakukan terhadap modul kriptografi pada BES menggunakan black box testing yang menyatakan bahwa modul kriptografi dapat berjalan dengan baik, data pelanggan yang terenkripsi dapat didekripsi pada semua proses, serta tidak menganggu proses transaksi pada BES.

Kata kunci: kriptografi, RC4, booking engine system

ABSTRACT

The development of the tourism industry in Bali had an impact on the increasing competition in Bali's tourism business. Competition can be seen from the emergence of new travel agents in Bali. In order to survive in the competitive tourism industry, the tourism players should be able to take advantage of opportunities in gaining profits by optimizing and marketing effectiveness and profits. One way that can be achieved is by sales / transaction travel packages online via the internet booking engine. There is a major issue explicitly in online transaction activity, mainly the problem of information security. Information security protects information from a widethreats to ensure business continuity, minimize loss of the company and maximize return on investment and business opportunities. Implementation of information security, especially in the online travel package deals can be the use of cryptographic methods using the RC4 algorithm. Where the purchase transaction information (plaintext) made by consumers will be transformed into the password data (ciphertext) which can not be identified, and then stored into the database. The information stored will be displayed back into plaintext is called descriptions into actual information.

Keywords : *Internet Booking Engine, RC4 Algorithm*

1. PENDAHULUAN

Bali sebagai salah satu tujuan wisata dunia menjadi lokomotif utama dalam rangka meningkatkan kunjungan wisatawan ke Indonesia. Keragaman budaya, alam yang indah, serta masyarakat yang santun masih menjadi atribut utama yang diandalkan Bali. Tentunya peluang tersebut harus mampu di manfaatkan oleh semua pemangku kepentingan pariwisata dalam meraih keuntungan dan mengembangkan bisnis. Salah satu pihak yang terlibat langsung dalam industri pariwisata adalah agent wisata. Bisnis berkembang secara dinamis, persaingan dalam dunia bisnis juga semakin dinamis dengan munculnya agen-agen wisata yang baru. Pelaku wisata ini harus mampu memikirkan cara-cara untuk terus bertahan dan bahkan mampu mengembangkan bisnis mereka. Salah satu inti usaha yang harus dioptimalkan adalah peningkatan efektifitas pemasaran melalui teknik-teknik pemasaran yang lebih efektif dengan biaya minimal dengan memanfaatkan teknologi informasi dan komunikasi saat ini.

Revolusi Industri 4.0 telah membawa perubahan pola bisnis yang luar biasa, terutama dalam pemanfatan teknologi informasi. Teknologi informasi serta aplikasinya saat ini telah menjadi salah satu komponen penting dalam berbagai bidang dan industri, termasuk pariwisata. Pariwisata berbasis teknologi informasi dikenal dengan sebutan *E-Tourism* (*IT-enabled tourism*) [1]. Dengan *E-Tourism,* perusahaan pariwisata dapat melakukan transaksi kepada calon wisatawan melalui internet, mulai dari promosi, penawaran hingga penjualan/transaksi produk-produk pariwisata. *Internet Booking Engine* yang biasa disebut *Booking Engine System* (BES) sebagai salah satu produk dari teknologi *E-tourism* merupakan sebuah aplikasi yang mendukung industri travel dan pariwisata dalam melakukan pemesanan melalui fasilitas internet. Aplikasi tersebut membantu pelanggan dalam hal melakukan pemesanan tiket, pemesanan hotel, paket liburan, asuransi, dan layanan online lainnya.

BES merupakan inovasi dari penerapan teknologi dalam dunia jual beli secara *online* atau transaksi online. Dengan berbagai keunggulan transaksi secara *online*, diantaranya wisatawan dapat melakukan transaksi dimanapun dan kapanpun dengan hanya berbekal komputer maupun gawai, tentunya dengan dukungan koneksi internet. Dari sudut pandang industri teknologi informasi, *Internet Booking Engine* sebagai salah satu produk *e-commerce* dapat diartikan sebagai sebuah sistem informasi yang ditujukan pada transaksi komersial, yang melibatkan transfer dana elektronik, *emarketing*, *online transaction processing*, *supply chain management, electronic data interchange* (EDI), *online marketing*, sistem manajemen inventori terotomasi, dan sistem koleksi data terotomasi. Kemampuan dalam menyediakan informasi secara cepat dan akurat, serta integrasi yang dilakukan baik terkait pembayaran, penerbitan tiket, hingga laporan menjadikan BES sangat banyak digunakan saat ini. Disamping berbagai keuntungan yang diperoleh dari kehadiran BES sebagai sebuah sistem informasi yang mampu diakses secara publik baik yang dapat dirasakan konsumen maupun penyedia layanan, terdapat sisi lain yang sangat penting untuk diperhatikan yakni bagaimana keamanan data dapat terjaga dengan baik. *Security* menjadi isu utama dalam pengembangan teknologi keamanan transaksi online. Jumlah kejahatan komputer terutama berkaitan dengan sistem informasi yang dapat diakses online akan terus mengalami peningkatan yang diakibatkan oleh beberapa hal, yakni.

1. Semakin meningkatnya penggunaan aplikasi bisnis berbasis jaringan internet. Kehadiran jaringan internet menjadikan sebuah perusahaan yang besar mampu menyediakan desentralisasi server, sehingga akan mengakibatkan semakin banyak sistem yang harus ditangani dan membutuhkan lebih banyak operator yang handal.
2. Meningkatnya persaingan bisnis antar penyedia layanan maupun pengguna layanan, serta didukung oleh meningkatnya kemampuan pengguna komputer menjadikan benyak pemakai yang mencoba-coba membongkar, bahkan sengaja menjatuhkan kinerja aplikasi lawan bisnis.
3. Semakin kompleks sistem yang dibuat dalam upaya meningkatkan interaksi sistem dengan pengguna, menyebabkan semakin besarnya program (*source code*). Hal ini tentu mengakibatkan semakin besarnya peluang terjadinya lubang keamanan. Untuk itu sangat penting pengujian sistem dan audit sistem informasi secara berkala.
4. Semakin tinggi nilai informasi, mengakibatkan meningkatnya ancaman terhadap penyalahgunaan data bahkan sampai pada transaksi jual beli data secara ilegal.
5. Kesulitan penegak hukum dalam mengejar kemajuan dunia komputer dan internet, menyebabkan regulasi yang dikeluarkan sering tidak relevan dengan keadaan saat itu.

Beberapa kasus pernah terjadi di Indonesia yang menyedot perhatian masyarakat dunia, mulai dari peretasan sistus bank dan pemerintah, penjualan data pelanggan *e-comerce* di situs *dark web*, hingga kebocoran data pelanggan operator telekomunikasi yang dipergunakan untuk kejahatan dan pengancaman[2]. Resiko kebocoran data baik akibat dari kesalahatn manusia, maupun kegagalan sistem dalam menangani ancaman berakibat pada kerugian materiil maupun sosial, serta tidak jarang

berakhir pada kasus hukum. Sampai saat ini belum ada satupun pihak ketiga yang menyatakan bertanggung jawab terhadap produk atau layanan yang diberikan melalui jasa internet [3]. Kemanan dalam dunia internet mengacu pada rumusan standar ISO IEC 270002 2005 (ISO IEC 17799 2005). Dalam standar tersebut dijelaskan bahawa salah satu bentuk dari pengelolaan resiko aset informasi adalah dengan menyusun dan menerapkan kebijakan keamanan informasi, terutama dalam keamanan data dalam sistem informasi, khususnya data transaksi *online*. Penerapan metode enkripsi pada data pelanggan dapat menjadi salah satu solusi pencegahan penyalahgunaan data. Enkripsi data menggunakan metode kriptografi simetris dengan algoritma RC4. Algoritma RC4 digunakan dengan pertimbangan bahwa algoritma ini sangat efektif dan cukup aman untuk diterapkan pada pengamanan Basis Data[4] .

2. METODE

A. Literatur Review

Keamanan Informasi dapat diartikan sebagai sistem penjagaan informasi dari seluruh kemungkinan ancaman yang terjadi, dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis[5], serta meminimasi resiko bisnis (*reduce business risk*). Untuk itu standar pengamanan informasi terdiri dari perlindungan bebera hal. Pertama berkaitan dengan *Confidentiality (*kerahasiaan*)* merupakan aspek keamanan sistem informasi yang menjamin kerahasiaan informasi atau data untuk memastikan informasi hanya dapat diakses oleh pihak yang berwenang serta mampu menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Berikutnya adalah bagaimana sistem keamanan informasi yang mampu menjamin bahwa data atau informasi tidak dirubah tanpa ada ijin pihak yang berwenang (*authorized*), serta mampu menjaga keakuratan dan keutuhan informasi hal ini berkaitan dengan *Integrity* (integritas). Terakhir yang penting juga dijaga adalah berkaitan dengan a*vailability (*ketersediaan*)* yaitu aspek yang menekankan bahwa sistem keamanan informasi mampu menjamin bahwa data dapat tersedia saat dibutuhkan serta dapat memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait. Keamanan data memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar. Dengan adanya kebutuhan database yang semakin besar dan kompleks, secara otomatis akan diikuti dengan kebutuhan akan keamanan terhadap data yang tersimpan dari berbagai ancaman yang dapat berupa pengaksesan, perubahan serta perusakan data oleh pihak atau *user* yang tidak mempunyai kewenangan[6].

Pendekatan preventif yang bersifat mencegah, dan upaya pendeteksian perlu dilakukan untuk mengetahui sejauhmana aktivitas sistem berjalan. Itulah mengapa penting menggunakan *Intrusion Detection System* (IDS) untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan[7]. Begitu banyak peluang ancaman yang terjadi sebagai akibat dari meningkatnya nilai informasi dan persaingan bisnis, sehingga pengembang sistem dapat mengklasifikasikan lubang keamanan sistem informasi menjadi tiga yaitu pertama melalui jalur pembawa informasi dalam hal ini jaringan internet (*network*). Yang kedua melalui celah kelemahan aplikasi termasuk database (*application security*). Dan terakhir melalui celah keamanan keamanan dari komputer (*end system*), termasuk *operating system* (OS). Semakin tinggi pengguna sistem maka nilai informasi akan semakin tinggi, dan sumber daya yang diperlukan juga semakin meningkat. Untuk itu, pengamanan sumber daya paling standar yang dilakukan adalah *backup database* secara berkala. Namun hal tersebut juga belum cukup, mengingat pentingnya akan kerahasisaan data terutama berkaitan dengan data pelanggan, maka pengembang sistem juga harus memikirkan kondisi terburuk jika penyusup berhasil masuk kedalam sistem. Sebagai alternatif keamanan terakhir adalah menerapkan metode enkripsi data yang tersimpan dalam database. Metode yang disebut dengan kriptografi sudah banyak digunakan terutama dalam sistem transaksi onlie baik *e-comerce*, *e-tiket*, maupun *internet banking*.

Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia dengan menggunakan teknik-teknik metematika. Dalam menjaga kerahasiaan data dengan kriptografi, data sederhana yang dikirim (*plainteks*) diubah ke dalam bentuk data sandi (*cipherteks*), kemudian data sandi tersebut hanya dapat dikembalikan ke bentuk data sebenarnya menggunakan kunci (*key*)[4]. Tentunya hal ini dapat menghindari penyalahgunaan data oleh pihak yang tidak berhak. Kriptografi dibedakan menjadi tiga jenis berdasarkan penggunaan kunci, yakni kriptografi simetris, kriptografi asimetris, dan kriptografi *hybrid* [8]. Jika dalam kriptografi menggunakan satu buah kunci, maka kriptografi tersebut tergolong simetris. Kriptografi simetris banyak digunakan karena dapat bekerja secara cepat, sehingga konsumsi daya komputasipun lebih kecil. Beberapa contoh dari algoritma yang digunakan

pada kriptografi simetris *adalah Advanced Encryption Standard* (AES), Blowfish, Tripple *Data Encryption Standard* (DES), dan *Rivest Code 4* (RC4). Sedangkan yang dimaksud kriptografi asimetris, jika kriptografi menggunakan dua buah kunci berbeda yang digunakan saat enkripsi dan dekripsi. Satu kunci disebarkan ke publik dan satu kunci bersifat privat. Beberapa contoh algoritma yang bekerja pada kriptografi asimetris yakni algoritma *Rivest-Shamir-Adleman* (RSA) dan *Diffie-Hellman*. Berikutnya adalah kriptografi *hybrid* yaitu kriptografi yang menerapkan beberapa algoritma berbeda untuk memperoleh kelebihan dari masing-masing algoritma. Algoritma ini menggabungkan kecepatan enkripsi dari algoritma simetris, dan kemampuan algoritma asimetris dalam mengamankan proses pertukaran kunci.

Konsep matematis yang menjadi dasar proses enkripsi dan dekripsi dalam Kriptografi adalah relasirelasi himpunan yang berisi elemen plainteks dan himpunan yang berisi elemen cipherteks. Enkripsi dan dekripsi menerapkan fungsi transformasi antara dua himpunan tersebut. Bila himpunan plainteks dinotasikan dengan P dan himpunan cipherteks dinotasikan dengan C, serta fungsi enkripsi dinotasikan dengan E dan fungsi dekripsi dinotasikan dengan D maka proses enkripsi dan dekripsi dapat dinyatakan dalam notasi matematis sebagai berikut.

$$E(P) = C \qquad (1)$$
$$D(C) = P \qquad (2)$$

Relasi antara himpunan plainteks dengan himpunan cipherteks merupakan korespondensi satu-satu. Hal ini menjadi keharusan untuk mencegah/meminimalisir terjadinya ambigu dalam dekripsi yaitu satu elemen cipherteks menyatakan lebih dari satu elemen plainteks. Karena proses dekripsi bertujuan untuk memperoleh kembali data asal dari proses enkripsi, maka.

$$D\big(E(P)\big) = P \qquad (3)$$

Pada metode kriptografi simetris hanya menggunakan satu buah kunci untuk proses enkripsi dan dekripsi. Bila kunci dinotasikan dengan k, maka proses enkripsi dan dekripsi kriptografi simetris dapat dinyatakan sebagai berikut.

$$E_k(P) = C$$
$$D_k(C) = P, \qquad Maka$$
$$D_k\big(E_k(P)\big) = P \qquad (4)$$

RC4 sebagai salah satu algoritma enkripsi *stream chiper* yang dirancang untuk dapat diimplementasikan secara efektif dan efisien. Oleh karena itu RC4 sangat populer untuk aplikasi internet, antara lain RC4 digunakan dalam standard WEP (*wireless equivalent privacy*) dan TLS *(transport layer security*)[9]. Algoritma kriptografi Rivest Code 4 (RC4) dibuat oleh RSA *Data Security Inc* (RSADSI) berbentuk *stream chipper*. Algoritma RC4 sukses menjadi salah satu algoritma *Stream Cipher* yang banyak digunakan dalam metode kriptografi. Kepopuleran algoritma ini sangat didukung oleh kecepatan, efisiensi, dan keefektifan dalam penggunaan sumber daya sehingga sangat baik untuk diimplementasikan pada *hardware* maupun *software*[10]. Algoritma RC4 mengenkripsi dengan mengombinasikan *plainteks* menggunakan *bit-wise* Xor yang memiliki panjang kunci dari 1 sampai 256 byte. Kombinasi kunci tersebut digunakan untuk menginisialisasikan tabel sepanjang 256 byte yang berfungsi sebagai generasi dari *pseudo random* untuk kemudian di operasikan XOR dengan *plaintext* untuk menghasilkan *ciphertext*[11]. Setiap elemen dalam tabel saling ditukarkan minimal sekali. Proses dekripsi dilakukan dengan cara yang sama seperti halnya proses enkripsi dengan kunci yang sama. Untuk menghasilkan *keystream cipher* menggunakan *state* internal yang meliputi dua proses yakni.

1. Tahap *key scheduling algorithm* (KSA). Pada tahap ini *state automaton* diberi nilai awal berdasarkan kunci enkripsi. *State* yang diberi nilai awal berupa *array* yang merepresentasikan suatu deret permutasi dengan 256 elemen, sehingga hasil dari algoritma KSA adalah permutasi awal dengan indeks 0 sampai 255 dinamakan State. Berikut dapat ditampilkan algoritma KSA dalam bentuk *pseudo-code* dimana *key* merupakan kunci enkripsi dan *keylength* merupakan besar kunci enkripsi dalam bytes[12].

```
for i=1 to 255
    State[i]=i
    j=0
    for i=0 to 255
        j=(j + State[i] + key[i mod keylength]) mod 256
        swap(State[i],State[i])
```

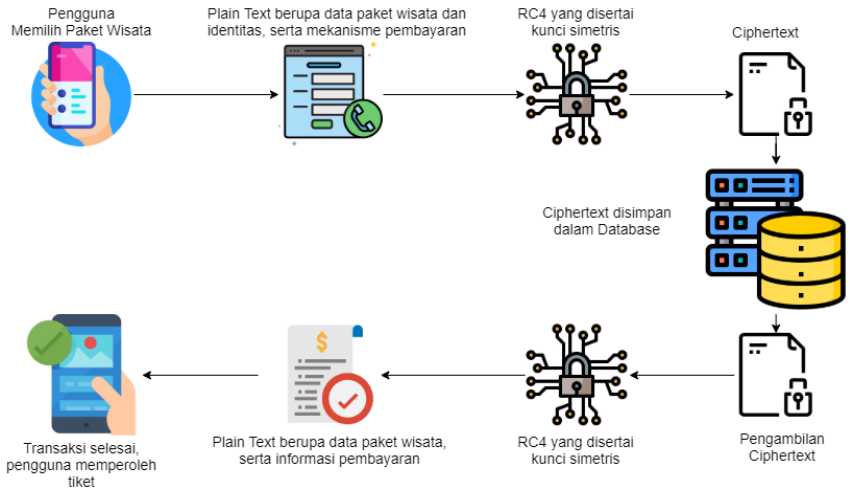
2. Tahap *pseudo-random* generation *algorithm* (PGRA) bertujuan untuk menghasilkan *keystream*. Setiap putaran, bagian *keystream* sebesar 1 b*yte* dengan nilai antara 0 sampai dengan 255 dioutput oleh PRGA berdasarkan *state* S[9]. Tahap ini menjadi penting karena akan banyak membutuhkan iterasi untuk momodifikasi *state* dari *keystream*. Setiap perulangan, PGRA melakukan *increament* terhadap i, kemudian menambah *State* yang terdiri dari matriks i dan j. Selanjutnya matrik tersebut ditukar antara *State*[i] dengan *State*[j]. Lalu mengembalikan nilai berupa elemen S terbaru di alamat State[i] + State[j] mod 256.

```
i=0
j=0
  loop
      i=(i + 1) mod 256
      j=(j + State[i]) mod 256
      swap(State[i],State[j])
      output S[(State[i] + State[j]) mod 256]
```

Setelah terbentuk *keystream*, selanjutnya *keystream* tersebut dimasukkan dalam operasi XOR dengan plaintext yang ada untuk menghasilkan *chipertext.* Sampai pada tahap ini proses enkripsi telah selesai, data *chipertext* dapat disimpan dalam database namun belum bisa digunakan sebelum di dekripsi. Untuk proses dekripsi menggunakan algoritma dan kunci yang yang sama, hanya saja *chippertext* berperan sebagai *plaintext.* Proses yang dilaluipun sama seperti enkripsi, sehingga pada tahap ini data atau pesan sudah bisa dikembalikan ke bentuk aslinya dan dapat dibaca.

B. Metode yang Diusulkan

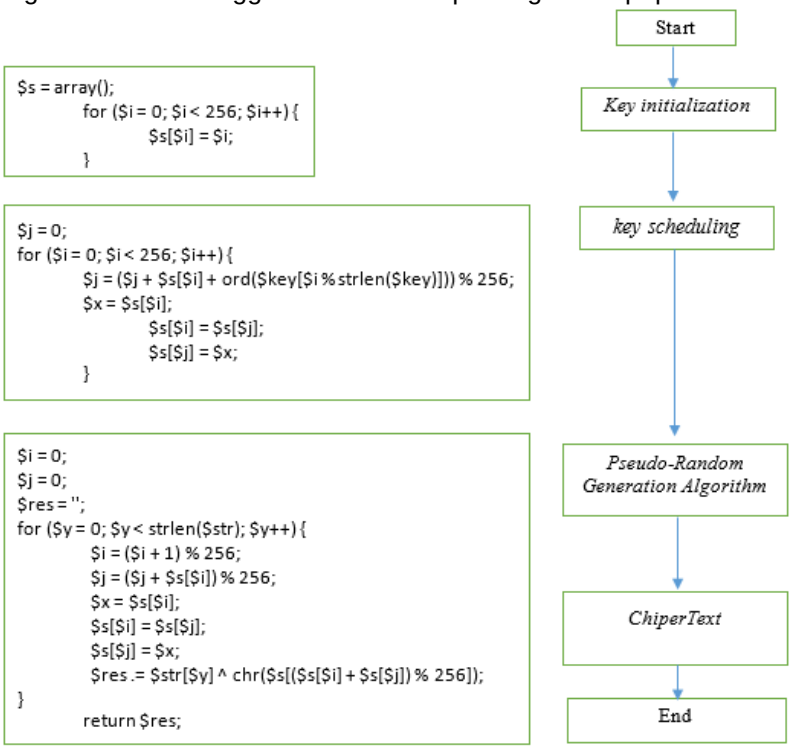
Penelitian bertujuan untuk mengamankan data pengguna yang dihasilkan dari proses penjualan paket wisata oleh salah satu agent pariwisata di Bali menggunakan BES berbasis Website. Proses Kriptografi akan disisipkan pada proses penyimpanan informasi pembelian paket wisata. Dimana pada informasi transaksi pembelian (*plaintext*) yang dilakukan oleh pengguna akan dienkripsi dengan sebuah kunci kedalam data sandi (*ciphertext*) yang tidak dapat dikenali, kemudian disimpan kedalam basis data. Sehingga informasi yang tersimpan di dalam database adalah informasi yang tidak bisa dibaca secara langsung. Berikut dapat dilihat pada gambar 1 mengenai proses kriptografi yang dilakukan.



Gambar 1. Alur Kriptografi pada BES

Kriptografi dilakukan guna meminimalisir terjadinya kebocoran informasi akibat serangan terhadap keamanan sistem informasi, berupa pengambilan informasi secara langsung ke dalam database. Kendatipun kondisi terburuk yaitu database mampu ditembus penyusup, maka data pelanggan dan transaksi tetap tidak dapat dipergunakan penyusup. Disisi lain sistem harus mampu menampilkan data transaksi tersebut seperti aslinya untuk dapat digunakan pada proses lainnya. Proses lain yang dimaksud seperti pengiriman tiket melalui email, laporan transaksi, serta informasi lainnya yang tetap membutuhkan informasi yang sebenarnya. Untuk itu, maka informasi berupa

chipertext harus dikembalikan ke informasi sebenarnya atau *plaintext* melalui proses deskripsi dengan algoritma dan kunci yang digunakan sebelumnya. Berikut dapat dijelaskan melalui gambar 2 mengenai proses algoritma RC4 menggunakan bahasa pemrograman php.



Gambar 2. Proses RC4

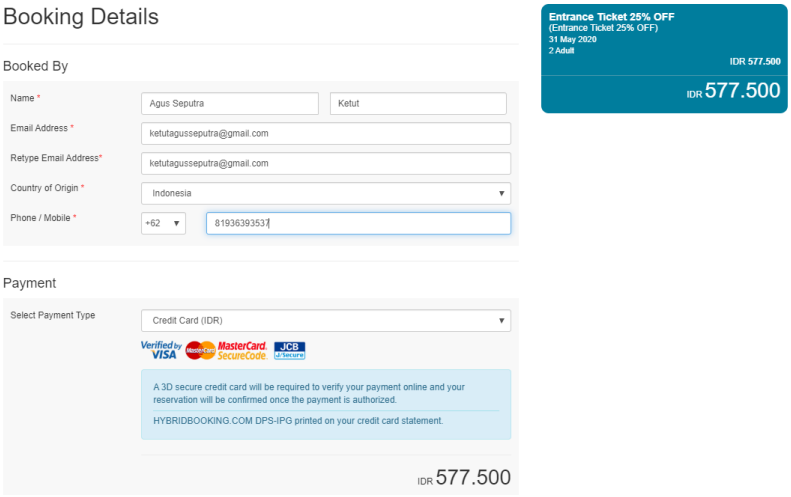
Atribut berupa invoice pembayaran, kode voucher tiket, produk yang dibeli, nama pembeli, email pemesan, alamat pemesan, tanggal pembelian dan tanggal aktivitas, serta jumlah pembayaran dienkripsi melalui proses diatas dengan sebuah kunci berupa string. Proses tersebut juga berlaku untuk proses deskripsi dengan menggunakan kunci yang sama.

3. HASIL DAN PEMBAHASAN

A. Implentasi Sistem

Modul kriptografi disisipkan pada bagian akhir transaksi sebelum data tersimpan dalam database. BES berbasis website yang dikembangkan dengan *framework codeigniter* memudahkan peneliti untuk menyisipkan modul kriptografi, sehingga kriptografi dapat berjalan dengan baik. Berikut ini adalah hasil implementasi kriptografi pada BES sesuai dengan metode yang diusulkan, mulai dari pemesanan produk, hingga proses penyimpanan data transaksi.

1. Pengunjung melakukan pemesanan produk pada salah satu perusahaan diving di Bali melalui BES yang diakses secara *online*. Data konsumen seperti nama, email, IDcard, idProduk, harga, dan Credit Card diinputkan oleh pengguna pada bagian akhir transaksi.
2. Pesanan tersebut selanjutnya disimpan pada *cartlist*. Pengguna bisa melakukan pesanan kembali, atau langsung mengakhiri transaksi melalui tahap pembayaran. Setelah pengguna selesai melakukan pemesanan produk, maka pelanggan diarahkan kehalaman *detail and payment*. Pelanggan mengisikan beberapa identitas yang diperlukan, seperti nama, email, no telp, serta asal negara. Kemudian pelanggan mengisikan detail *participant* sesuai dengan jumlah pesanan. Setelah lengkap pelanggan melakukan pembayaran melalui *credit card* atau ATM transfer seperti pada gambar 3.



Gambar 3. Proses Pemesanan

3. Data pesanan pelanggan tersebut dienskripsi pada sistem menggunakan algoritma RC4 dengan sebuah kunci string. Data hasil enskripsi tersebut tersimpan didalam basis data *mysql.* Dapat dilihat pada tabel 1 mengenai perbandingan linearitas *chipertext*. Dapat dikatakan linearitas jika panjang karakter *chipertext* sama dengan panjang karakter *plaintext*. Data tersebut tidak dapat dipergunakan langsung oleh siapapun termasuk administrator database. Mengingat modul kriptografi disisipkan pada sisi aplikasi mengakibatkan data tersebut harus didekripsi dulu oleh aplikasi tentu dengan menggunakan sebuah kunci. Sehingga pengembangan maupun administator database kesulitan untuk mengolah data melalui *query* langsung. Nah inilah yang menjadi salah satu contoh bahwa kenyamanan berbanding terbalik dengan keamanan sistem informasi.

Tabel 1. Contoh Data Enksripsi

Field	Plaintext	Length	Chipertext	Length
Nama	Agus Seputra Ketut	18	ﷺs8NW>ʒN﷽tGQ 5﷽	18
KTP	80515899000134	14	{﷽6~_1c﷽﷽﷽﷽?	14
Telp	081936393537	12	{﷽7r]2h﷽﷽ ﷽	12
Invoice	8965049200083520	16	s﷽0~^0b﷽﷽﷽﷽9 P	16
Email	ketutagusseputra@gmail.com	26	﷽r> e<ϽHl﷽﷽xF ﷽﷽`JX﷽﷽	26

4. Untuk dapat menggunakan data terenkripsi seperti gambar 3 pada proses lainnya, maka data tersebut harus melalui proses deskripsi dengan modul kriptografi dan kunci yang sama. Hasil deskripsi harus sama dengan data yang sebenarnya yang dimiliki oleh pelanggan, seperti pada proses pengiriman email pembayaran pada gambar 4.

Gambar 4. Pengiriman Email Pembayaran

B. Pengujian Performa Algoritma

Pengujian ditujukan untuk mengetahui kemampuan sistem dalam melakukan kriptografi. Data yang digunakan merupakan data json yang berjumlah 922 baris dengan dua kolom [13]. Pengujian dilakukan dengan membandingkan waktu eksekusi data (*Elapsed Time*) dan alokasi memori untuk memproses data (*Memory Usage*). Uji coba dilakukan menggunakan panjang kunci berbeda-beda, hal ini dilakukan untuk mengetahui apakah panjang kunci berpengaruh secara signifikan terhadap waktu eksekusi dan alokasi memori. Dari pengujian diperoleh hasil seperti pada tabel 2. Pengujian juga dilakukan dengan menyandingkan performa sistem dengan kriptografi dan sistem tanpa kriptografi.

Tabel 2. Pengujian Performa Algoritma

Key Length	Elapsed Time	Memory Usage (MB)	Decryption Percentage
Tanpa Kriptografi	3.7247	3.48	
2	4.7955	3.49	100%
4	5.2758	3.49	100%
16	6.4754	3.49	100%
60	7.2866	3.49	100%

Berdasarkan hasil pengujian yang disajikan pada tabel 2, diperoleh hasil bahwa implementasi kriptografi pada sistem berpengaruh terhadap waktu eksekusi data dan alokasi memori. Panjang kunci yang digunakan dalam kriptografi juga menentukan waktu eksekusi, semakin panjang kunci maka waktu yang diperlukan juga semakin lama. Keberhasilan algoritma dalam melakukan dekripsi juga penting untuk diuji. Dari semua pengujian terhadap 922 baris data pada sistem yang disisipkan kriptografi, memperoleh hasil bahwa 100% data berhasil didekripsi sama seperti data aslinya.

C. Pengujian Black Box

Modul kriptografi yang disisipkan pada proses transaksi pembelian diuji untuk memastikan fungsionalitas sistem yang telah berjalan tidak terganggu sebagai akibat dari penyisipan modul tersebut. Pengujian dilakukan terhadap modul transaksi BES menggunakan *black box testing*. Adapun tipe pengujjian yang digunakan adalah *sample testing* dan *behaviour testing*. Sample testing digunakan untuk memastikan sistem mengeluarkan data yang valid sesuai inputan pengguna. Berikut disajikan pada tabel 3. beberapa hasil pengujian *sample testing* berdasarkan test case yang digunakan.

Tabel 3. Hasil Pengujian *Sample Testing*

Input	Hasil Harapan	Output	Kesimpulan
Menginputkan detail transaksi pembelian paket wisata pada BES	Sistem menerima Semua Data	Sistem meyimpan data sesuai inputan data user	Berhasil
Sistem mengirimkan detail pembayaran melalui email	Sistem dapat mengirimkan detail pembayaran ke pengguna melalui email	Pengguna menerima email pembayaran yang sesuai dengan transaksi pembelian pengguna	Berhasil
Admin melihat laporan transaksi	Sistem dapat menampilkan laporan transaksi pengguna	Sistem dapat menampilkan laporan transaksi pengguna secara benar	Berhasil

Pengujian juga dilakukan menggunakan behaviour testing untuk memastikan sistem secara konsisten menghasilkan data yang valid dalam beberapa percobaan. Pengujian dilakukan dengan membuat transaksi baru sebanyak 10 kali berdasarkan *test case* yang telah digunakan pada *sample testing*. Adapun hasil pengujian dapat dilihat pada tabel 4.

Tabel 4. Hasil Pengujian *Behaviour Testing*

Input	Hasil Harapan	Output	Kesimpulan
Melakukan transaksi pembelian paket wisata sebanyak 10 kali	Sistem menerima semua data baru	Sistem meyimpan data sesuai inputan data user	Berhasil
Sistem mengirimkan detail pembayaran melalui email sesuai transaksi yang berhasil sebanyak 10 kali	Sistem dapat mengirimkan detail pembayaran ke pengguna melalui email sesuai data transaksi	Pengguna menerima email pembayaran yang sesuai dengan transaksi pembelian pengguna	Berhasil

4. SIMPULAN DAN SARAN

Algoritma RC4 merupakan algoritma enkripsi *stream chiper* yang dirancang untuk dapat diimplementasikan pada perangkat lunak secara sangat efisien. Metode kriptografi disisipkan pada proses penyimpanan data pembelian tiket pada website *booking engine* salah satu agent wisata. Kriptografi ditujukan untuk menyembunyikan data transaksi pelanggan. Data transaksi pembelian (*plaintext*) yang dilakukan oleh konsumen akan ditransformasikan kedalam data sandi (*ciphertext*) yang tidak dapat dikenali, baru kemudian disimpan kedalam basis data. Sehingga resiko bocornya informasi akibat adanya serangan terhadap keamanan sistem informasi dapat diminimalisir. Hasil pengujian performa algoritma menunjukkan bahwa algoritma RC4 berhasil melakukan enkripsi dan dekripsi 100% terhadap 922 baris data. Panjang kunci juga mempengaruhi estimasi waktu eksekusi data, semakin panjang kunci tentu semakin lama waktu yang diperlukan. Walaupun jika dibandingkan, waktu pemrosesan data dengan modul kriptografi lebih lama yaitu 3.7247 s dibandingkan dengan tanpa modul kriptografi yaitu 4.7955 s. Adapun hasil pengujuan berdasarkan blackbox testing adalah sebagai berikut.

1. Transaksi pembelian dapat berjalan dengan baik. Pengguna tidak merasa kesulitan dalam melakukan transaksi hingga proses pembayaran.
2. Pengguna memperoleh informasi terkait pemesanan tiket baik diakhir transaksi maupun berupa voucher yang dikirim ke email.
3. Administrator sistem dapat melihat laporan transaksi melalui modul admin pada BES.

Sebagai akibat dari implementasi modul kriptografi pada sisi aplikasi, menyebabkan pengelola harus melalui aplikasi untuk melakukan manajemen data baik berupa laporan maupun operasional harian. Hal ini tentu menyulitkan pengembang aplikasi untuk melakukan operasi *query* pada database. Saran yang dapat diberikan peneliti adalah menyisipkan modul kriptografi pada sisi database berupa fungsi. Sehingga akan diperoleh kenyamanan dalam hal pengelolaan data secara langsung. Namun dengan catatan kerahasiaan kunci dekripsi dapat terjaga dengan baik.

DAFTAR PUSTAKA

[1] T. Wellem and E. D. I. I. Dan, “Semantic Web Sebagai Solusi Masalah Dalam E-Tourism Di Indonesia,” vol. 2009, no. Snati, 2009.
[2] Yudha Pratomo, “Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di Dark Web,” *Kompas.com*.
[3] U. Ungkawa, I. A. Dewi, and K. R. Putra, “Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking,” *Tek. Inform. Fak. Teknol. Ind. Inst. Teknol. Nas. Bandung*, pp. 2–11, 2013.
[4] W. H. Haji and S. Mulyono, “Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data,” *Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data*, vol. 2012, no. Snati, pp. 15–16, 2012.
[5] M. I. A. Ermana Fine, Tanuwijaya Haryanto, “Audit Keamanan Sistem Informasi Berdasarkan Standar Iso 27001 Pada Pt. Bpr Jatim,” *Stikom*, pp. 1–8, 2012.
[6] Y. Ariyanto, “Algoritma Rc4 Dalam Proteksi Transmisi Dan Hasil Query Untuk Ordbms Postgresql,” *J. Inform.*, vol. 10, no. 1, pp. 53–59, 2010.
[7] B. Fachri and F. H. Harahap, “Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer,” *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020.
[8] B. Dan and A. Rsa, “ANALISIS PERFORMA KRIPTOGRAFI HYBRID ALGORITMA,” vol. VI, no. 1, 2019.
[9] T. D.B.Weerasinghe, “Analysis of a Modified RC4 Algorithm,” *Int. J. Comput. Appl.*, vol. 51, no. 22, pp. 12–16, 2012.
[10] a T. A. Bastari, “Analisis Perbandingan Stream Cipher RC4 dan SEAL,” *Jti*, 2011.
[11] O. Setiawan, R. Fiati, and T. Listyorini, “Algoritma Enkripsi Rc4 Sebagai Metode Obfuscation Source Code Php,” *Pros. SINATIF*, vol. 1, pp. 113–120, 2014.
[12] T. D.BWeerasinghe, “Improving Throughput of RC4 Algorithm using Multithreading Techniques in Multicore Processors,” *Int. J. Comput. Appl.*, vol. 60, no. 16, pp. 45–51, 2012.
[13] U.S. Government Work, “SBA Public Datasets,” *U.S. Small Business Administration*, 2015. [Online]. Available: https://www.sba.gov/sites/default/files/data.json.