Nama : Andri Firman Saputra

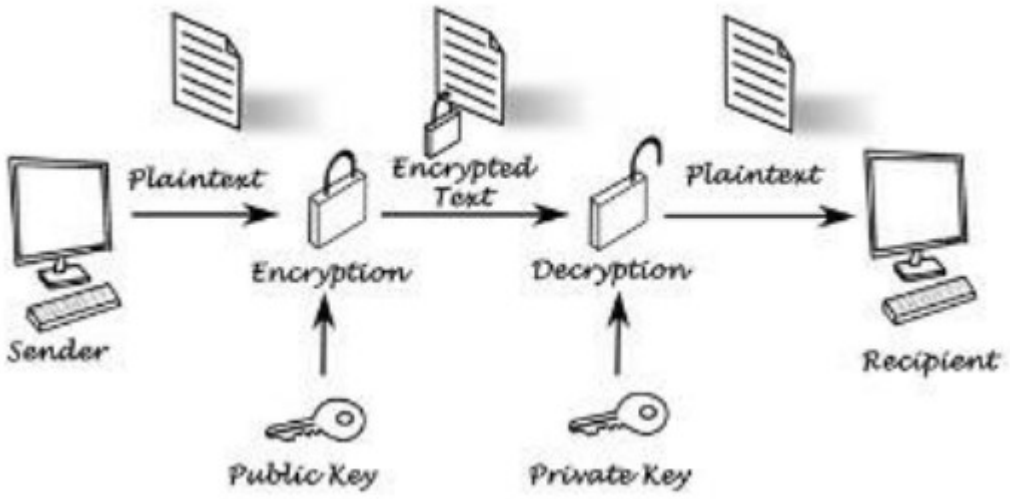
NIM : 2010114025

Kelas : 07TPLP016

Tugas : E-Commerce

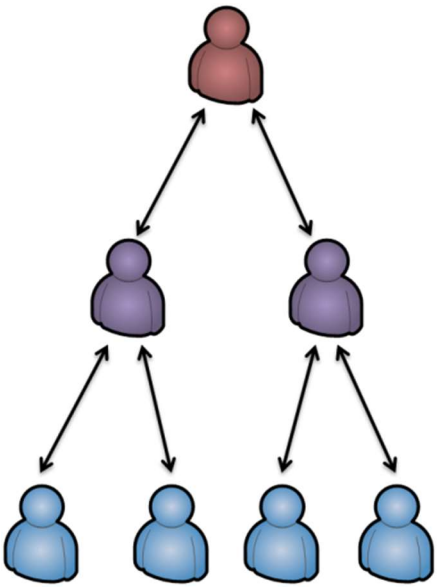
---

1. Gambarkan metode Enkripsi dan Certification Authority/Digital Signature berikan penjelasan!
   a. Gambar Enkripsi



Kriptografi asimetris atau juga dikenal sebagai kriptografi kunci publik, menggunakan dua kunci yang berbeda: satu publik dan satu privat yang saling terkait secara matematis. Kunci publik bisa dibagi dengan semua orang, sedangkan kunci privat harus dirahasiakan.

   b. Gambar Certificate authory



Certificate Authority adalah entitas terpercaya yang menerbitkan sebuah dokumen elektronik yang memverifikasi suatu identitas dari suatu entitas di internet, dokumen elektronik yang dimaksud adalah Digital Certificate.

2. Gambarkan proses Enkripsi RSA berikan contoh dan penjelasannya!

   Contoh Penghitungan RSA Misalnya kita mau mengenkripsi kata “SECRET” dengan RSA, lalu kita dekripsi kembali ke dalamplaintext. Karenapdanqberjumlah minimal 100 digit atau lebih, nilaiddanebisa berjumlah sama dengan 100 digit dan nilaiNakan berjumlah 200 digit. Untuk itu di contoh pemakaian berikut, kita akan memakai angka-angka yang kecil agar mudah dalam penghitungan. Cara pengerjaannya adalah :

   1) Kita pilihp= 3 danq= 5
   2) HitungN=pq= 3*5 = 15
   3) Nilaieharus merupakan bilangan prima yang lebih besar dan relatif dekat dengan (p-1)(q-1) =(2)(4) = 8, sehingga kita pilihe= 11. Angka 11 adalah bilangan prima terdekat dan lebih besar daripada 8
   4) Nilai d harus dipilih sehingga (ed- 1) (p-1)(q-1) adalah sebuah integer. Lalu nilai (11d - 1) / [(2)(4)] = (11d - 1) / 8 juga merupakan integer. Setelah melalui proses penghitungan, salah satu nilai yang mungkin adalah d = 3.
   5) Lalu kita masukkan kata yang akan dienkripsi, “SECRET”. Kita akan mengkonversi string ini kerepresentasi desimal menggunakan nilai karakter ASCII, yang akan menghasilkan nilai ASCII 83 69 67 82 69 84

6) Pengirim akan mengenkripsi setiap digit angka pada saat yang bersamaan menggunakan nilai kunci publik (e,n) = (11,15). Lalu setiap karakterciphertextakan masuk ke persamaan Ci = Mid mod 15 Yang akan menghasilkan nilai digit masukan adalah 0x836967826984 yang akan dikirim sebagai 0x2c696d286924
7) Penerima akan mendekripsi setiap digit angka menggunakan nilai kunci privat (d,n) = (3, 15). Lalu, setiap karakter plaintext akan masuk persamaan Mi = Ci3mod 15 String masukan yang bernilai 0x2c696d286924, akan dikonversi kembail menjadi 0x836967826984, dan akhirnya angka-angka tersebut akan diubah kembali menjadi bentuk stringplaintextyang bernilai “SECRET”

3. Untuk melindungi kegiatan bisnis online atau eCommerce pelaku yang terlibat didalam mendapat perlindungan dari pemerintah dengan terbitnya UU TEI, cobalah anda cari UU TEI yang terkait dengan kegiatan eCommerce!

   Undang-Undang No 7 Tahun 2014 Tentang Perdagangan (UU Perdagangan) dan UU No 8 tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen) merupakan acuan bagi setiap pelaku usaha dalam melakukan transaksi perdagangan, baik perdagangan konvensional maupun perdagangan melalui online atau e-commerce. Dalam UU Perdagangan, diatur mengenai sistem perdagangan elektronik

   dengan ketentuan bahwa setiap orang atau badan usaha yang memperdagangkan barang atau jasa wajib menyediakan data dan informasi secara lengkap dan benar.

   E-commerce diatur dalam UU Perdagangan Bab VIII mengenai Perdagangan Melalui Sistem Elektronik pada pasal 65 dan 66. Sementara untuk ketentuan lebih lanjut akan diatur dalam Peraturan Pemerintah yang hingga saat ini masih didorong penyelesaiannya. UU Perlindungan konsumen merupakan pedoman pelaku usaha dan konsumen dapat menjalankan usahanya secara fair dan tidak merugikan konsumen. Perlindungan konsmen dalam era digital e-commerce ini menjadi hal yang penting dan dibutuhkan, ketika penjual dan pembeli hanya bermodalkan asas kepercayaan dalam melakukan transaksi perdagangan elektronik. Jangan sampai perdagangan elektronik dijadikan alat bagi orangorang yang tidak bertanggung jawab dalam memasarkan produknya.

   Dalam konteks hukum perlindungan konsumen yang berlaku di Indonesia, yaitu UU No 8 Tahun 1999 tentang Perlindungan Konsumen, hak dan kewajiban konsumen dan pelaku usaha telah diatur dengan jelas dan tegas. Untuk hak dan kewajiban konsumen diatur dalam

Pasal 4 dan 5 UU. UU Perlindungan Konsumen, sedangkan untuk hak dan kewajiban pelaku usaha diatur dalam Pasal 6 dan 7 UU Perlindungan Konsumen. Dalam pasal-pasal tersebut diatur bagaimana proporsi atau kedudukan konsumen dan pelaku usaha dalam suatu mekanisme transaksi bisnis atau perdagangan. Dalam konteks transaksi e-commerce, aspek hukum perlindungan konsumen yang berkaitan langsung dengan konsumen adalah yang mengenai aspek perbuatan yang dilarang bagi pelaku usaha dan tanggung jawab pelaku usaha. Aspek perbuatan yang dilarang bagi pelaku usaha dalam UU Perlindungan Konsumen diatur dalam Pasal 8 sampai dengan Pasal 17. Aspek ini dapat diberlakukan apabila dapat dibuktikan bahwa barang dan/jasa yang diperdagangkan melalui e-commerce melanggar ketentuan ini.

Dalam UU Perdagangan telah diberikan batasan hal-hal apa saja yang merupakan tugas pengawasan dari amanat UU Perdagangan ini. Dalam Pasal 100 ayat (3) disebutkan:14 (3) Petugas Pengawas sebagaimana dimaksud pada ayat (2) dalam melaksanakan kewenangannya paling sedikit melakukan pengawasan terhadap: a. Perizinan di bidang Perdagangan. b. Perdagangan Barang yang diawasi, dilarang, dan/atau diatur. c. Distribusi Barang dan/atau Jasa. d. Pendaftaran Barang Produk Dalam Negeri dan asal Impor yang terkait dengan keamanan, keselamatan, kesehatan, dan lingkungan hidup.

4. Selain kejahatan dalam dunia maya yang sudah dijelaskan sebelumnya, cyber-crime apa saja yang bisa terjadi atau kemungkinan terjadi, jelaskan dan bagaimana penanggunalangannya, Anda dapat berdiskusi dalam kelompok. Presentasikan hasilnya pada kegiatan pembelajaran selanjutnya.
   Selain kejahatan dalam dunia maya yang sudah saya jelaskan sebelumnya, ada beberapa jenis kejahatan siber lainnya yang dapat terjadi atau kemungkinan terjadi. Berikut adalah beberapa contoh cybercrime beserta penanganannya:

   Phishing (Penipuan Online):

   Penjelasan: Phishing adalah upaya untuk memperoleh informasi pribadi, seperti kata sandi dan informasi keuangan, dengan menyamar sebagai entitas tepercaya melalui email, situs web palsu, atau pesan teks.
   Penanganan: Penting untuk waspada terhadap email dan situs web yang mencurigakan. Selalu verifikasi sumber informasi sebelum memberikan informasi pribadi. Perusahaan dan individu perlu memberikan pelatihan keamanan siber kepada karyawan dan pengguna akhir.

Ransomware:

Penjelasan: Ransomware adalah jenis perangkat lunak berbahaya yang mengenkripsi data korban dan meminta tebusan untuk mendekripsi data tersebut.
Penanganan: Backup rutin data dan perangkat lunak keamanan yang kuat sangat penting. Jangan membayar tebusan, karena itu mendorong kejahatan siber lebih lanjut. Langkah-langkah pencegahan, seperti memperbarui perangkat lunak dan mengamankan email, juga diperlukan.
Malware (Perangkat Lunak Berbahaya):

Penjelasan: Malware mencakup virus, trojan, worm, dan sebagainya yang dapat merusak atau mencuri data dari sistem komputer.
Penanganan: Gunakan perangkat lunak antivirus dan antispyware yang terbaru, serta perbarui sistem operasi dan perangkat lunak dengan patch keamanan. Penggunaan firewall dan pendidikan keamanan siber penting.
Identitas Pencurian:

Penjelasan: Ini terjadi ketika seseorang mencuri informasi pribadi, seperti nomor KTP atau informasi kartu kredit, dan menggunakannya untuk tindakan kriminal.
Penanganan: Lindungi informasi pribadi dengan kuat, seperti menggunakan kata sandi yang kuat dan berbagai untuk berbagai akun, serta memonitor aktivitas keuangan secara rutin. Juga, waspada terhadap tindakan penipuan identitas.
Serangan DDoS (Denial of Service):

Penjelasan: Serangan DDoS bertujuan untuk mengganggu ketersediaan situs web atau layanan online dengan banjir lalu lintas internet palsu.
Penanganan: Penggunaan firewall, perangkat lunak deteksi serangan, dan penyedia layanan internet yang kuat dapat membantu mengurangi dampak serangan DDoS. Pengguna juga perlu memonitor lalu lintas dan memblokir lalu lintas yang mencurigakan.
Untuk mengatasi berbagai jenis kejahatan siber ini, pendekatan yang efektif melibatkan kombinasi tindakan teknis dan pelatihan kesadaran keamanan bagi individu dan organisasi. Penggunaan perangkat lunak keamanan yang kuat, pembaruan sistem, dan praktik keamanan yang baik adalah kunci dalam melindungi diri dari ancaman siber. Selain itu, kerjasama dengan penegak hukum dan lembaga keamanan siber dapat membantu

mengidentifikasi dan menindak pelaku kejahatan siber. Dalam kelompok diskusi, dapat dibahas strategi dan praktik terbaik dalam melindungi diri dari berbagai jenis kejahatan siber ini.

5. Sebutkan dan jelaskan apa saja standar keamanan untuk aplikasi web, Email dan jaringan!

   Berikut adalah beberapa standar keamanan umum yang digunakan untuk aplikasi web, email, dan jaringan:

   1. Aplikasi Web:

   OWASP Top Ten: Standar ini dikeluarkan oleh Proyek Keamanan Aplikasi Web Terbuka (OWASP) dan mencakup sepuluh kerentanan keamanan yang paling umum dalam aplikasi web, seperti SQL injection, cross-site scripting (XSS), dan kerentanan CSRF (Cross-Site Request Forgery). Standar ini memberikan panduan tentang cara mengidentifikasi, mencegah, dan memitigasi risiko ini.

   HTTPS (SSL/TLS): Menggunakan koneksi aman dengan HTTPS untuk melindungi data yang ditransmisikan antara pengguna dan server. Ini melibatkan penggunaan sertifikat SSL/TLS untuk mengenkripsi data.

   Kebijakan Keamanan: Menerapkan kebijakan keamanan yang kuat, termasuk manajemen kata sandi yang baik, kontrol akses, dan pelatihan keamanan bagi pengembang dan pengguna.

   2. Email:

   DMARC (Domain-based Message Authentication, Reporting, and Conformance): DMARC adalah standar yang digunakan untuk memvalidasi pengiriman email yang berpura-pura berasal dari domain tertentu. Ini membantu melindungi domain dari phishing dan spoofing.

   SPF (Sender Policy Framework): SPF adalah standar yang mengotentikasi pengiriman email dengan memeriksa alamat IP yang diizinkan untuk mengirim email atas nama domain tertentu.

DKIM (DomainKeys Identified Mail): DKIM adalah metode autentikasi yang memungkinkan pengirim email untuk menandatangani pesan email dengan tanda tangan digital, yang dapat diverifikasi oleh penerima untuk memastikan email belum diubah selama pengiriman.

Penggunaan Alat Anti-Spam: Menggunakan alat anti-spam yang kuat untuk mengidentifikasi dan mengisolasi email berbahaya atau spam.

3. Jaringan:

Firewall: Penggunaan firewall untuk mengontrol lalu lintas masuk dan keluar dari jaringan dan mencegah akses yang tidak sah.

VPN (Virtual Private Network): Penggunaan VPN untuk mengamankan koneksi jaringan yang tidak aman, seperti saat mengakses jaringan dari lokasi jauh.

Intrusion Detection and Prevention Systems (IDS/IPS): Penggunaan IDS/IPS untuk mendeteksi dan mencegah serangan terhadap jaringan. Ini mencakup deteksi intrusi (IDS) dan pencegahan intrusi (IPS).

Pemantauan Jaringan: Pemantauan lalu lintas jaringan secara teratur untuk mendeteksi aktivitas mencurigakan atau ancaman keamanan.

Pembaruan Rutin: Memastikan perangkat keras dan perangkat lunak jaringan diperbarui secara teratur untuk mengatasi kerentanan keamanan yang telah diidentifikasi.

Penting untuk menyadari bahwa standar keamanan ini hanya sebagian kecil dari berbagai langkah yang dapat diambil untuk melindungi aplikasi web, email, dan jaringan. Selalu penting untuk memahami lingkungan yang lebih luas, menganalisis risiko yang mungkin, dan mengikuti praktik terbaik keamanan yang relevan untuk masing-masing kasus.

6. Apa yang anda ketahui tentang SET (Security Elektronic Transaction), jelaskan proses kerjanya, dan berikan contoh!

   Security Electronic Transaction (SET) adalah sebuah protokol keamanan yang dikembangkan pada tahun 1996 oleh Visa, MasterCard, dan beberapa perusahaan teknologi

lainnya untuk meningkatkan keamanan transaksi pembayaran elektronik melalui internet. Tujuan utama SET adalah melindungi informasi keuangan dan identitas konsumen selama proses transaksi online. Meskipun konsep SET masih relevan dalam konteks keamanan transaksi online, namun standar tersebut tidak begitu umum digunakan saat ini. Penggunaan SSL/TLS dalam HTTPS telah menjadi metode keamanan yang lebih umum digunakan untuk transaksi online.

Berikut adalah cara kerja SET:

Pendaftaran:

Konsumen mendaftarkan diri dengan otoritas sertifikat (CA, Certificate Authority) untuk mendapatkan sertifikat digital. CA mengeluarkan sertifikat digital yang digunakan oleh konsumen untuk mengidentifikasi diri secara elektronik.
Pembuatan Pesanan:

Konsumen membuat pesanan melalui situs web atau aplikasi e-commerce dan memilih opsi pembayaran melalui SET.
Sertifikat digital konsumen digunakan untuk mengidentifikasi mereka pada saat pesanan dibuat.
Pembayaran:

Penjual (merchant) mengirim informasi pesanan dan jumlah pembayaran ke bank akuisisi (acquiring bank) dan CA.
CA menghasilkan sertifikat pembayaran dan mengenkripsi informasi pembayaran tersebut dengan kunci publik penjual.
Informasi tersebut dikirimkan ke konsumen.
Konsumen mengenkripsi informasi tersebut dengan kunci publik bank pembeli (issuing bank) dan mengirimkannya kembali ke bank pembeli.
Bank pembeli mendekripsi informasi tersebut dengan kunci privatnya dan mengotentikasi konsumen.
Bank pembeli mengesahkan transaksi dan mengirimkan persetujuan ke penjual.
Konfirmasi Pembayaran:

Penjual menerima persetujuan dari bank pembeli dan mengirimkan barang atau layanan yang telah dibeli kepada konsumen.
Konsumen menerima barang atau layanan tersebut.
Contoh penggunaan SET adalah saat seseorang berbelanja secara online dan memilih metode pembayaran yang diatur menggunakan SET. Informasi pembayaran, seperti nomor kartu kredit, dikirimkan dalam format terenkripsi antara konsumen, penjual, dan bank pembeli. SET membantu mengamankan informasi ini selama transit dan memberikan keamanan tambahan terhadap penggunaan ilegal.

Namun, seiring berkembangnya teknologi keamanan dan pergeseran ke penggunaan HTTPS yang mencakup enkripsi data dalam transaksi, SET tidak lagi menjadi standar utama yang digunakan secara luas dalam transaksi online. Penggunaan sertifikat digital dan infrastruktur kunci publik (PKI) tetap penting dalam konteks keamanan internet, tetapi banyak aspek keamanan tersebut sekarang diatur melalui metode keamanan yang lebih umum seperti Transport Layer Security (TLS) yang digunakan dalam HTTPS.