**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

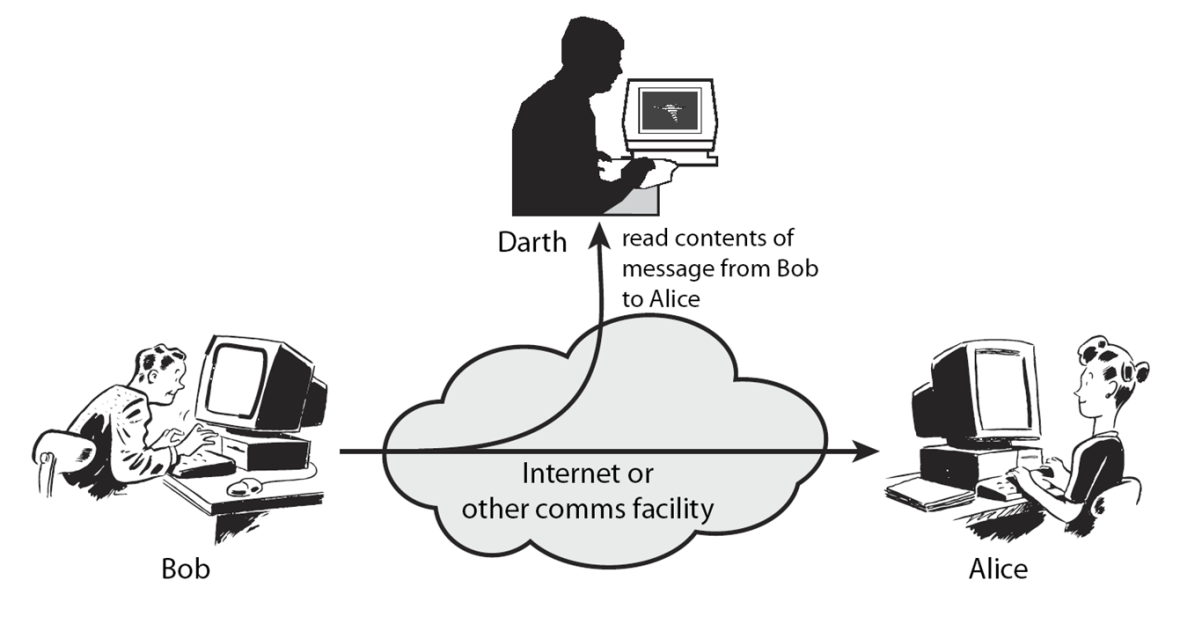
**Session 05**

**Technical aspect of Information Security**

**Cryptography**

Mengamankan Internet adalah sesuatu hal yang menyajikan tantangan besar dan kesempatan untuk melakukan penelitian. Aplikasi aplikasi yang sangat berguna seperti voting secara internet, catatan medis yang tersedia pada internet, dan e-commerce dapat menjadi masalah besar karena masalah keamanan dan privasi yang serius. Serangan hacker pada komputer pribadi dan situs web hanya menyoroti kerentanan yang melekat pada komputer dan jaringan infrastruktur. Seharusnya untuk menangani masalah keamanan dan privasi memerlukan kombinasi pendekatan teknis, sosial, dan hokum, yang mana salah satunya adalah masalah otentikasi dan enkripsi.

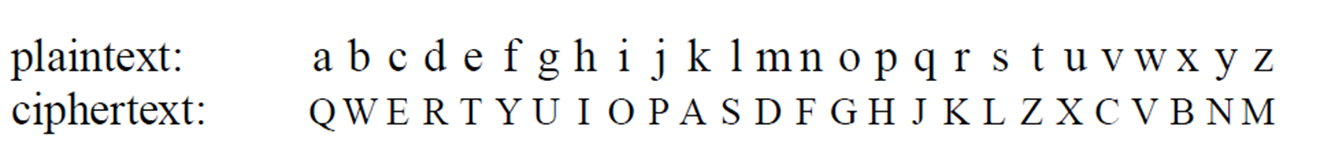
Pada gambar 1 terlihat bagaimana data yang dikirimkan dapat di cegat dan dibaca oleh seseorang yang tidak berhak yang ingin berbuat jahat.



Gambar 1. Intruder mengambil data saat pengiriman

Kriptografi adalah landasan dari teknologi keamanan elektronik modern yang digunakan saat ini untuk melindungi informasi di intranet, extranet, dan Internet. Kriptografi dikhususkan untuk menjaga data dan komunikasi yang aman. Ini adalah bidang inti dari teknologi informasi dan komunikasi. Kriptografi menggabungkan beberapa disiplin ilmu, yaitu matematika, fisika, ilmu komputer, dan engineering. Pada saat ini individu dan organisasi di seluruh dunia tergantung pada kemampuan untuk memastikan data dan sistem komunikasi yang aman dan terpercaya. Keamanan informasi memungkinkan pengguna untuk mengakses layanan, memverifikasi identitas pengguna lain dan organisasi, dan autentikasi asal dan integritas perangkat lunak dan data lainnya. Memahami dasar konsep, komponen, dan risiko keamanan berbasis kriptografi adalah sangat penting dalam memilih dan merencanakan jaringan dan sistem informasi keamanan yang sesuai untuk organisasi Anda.

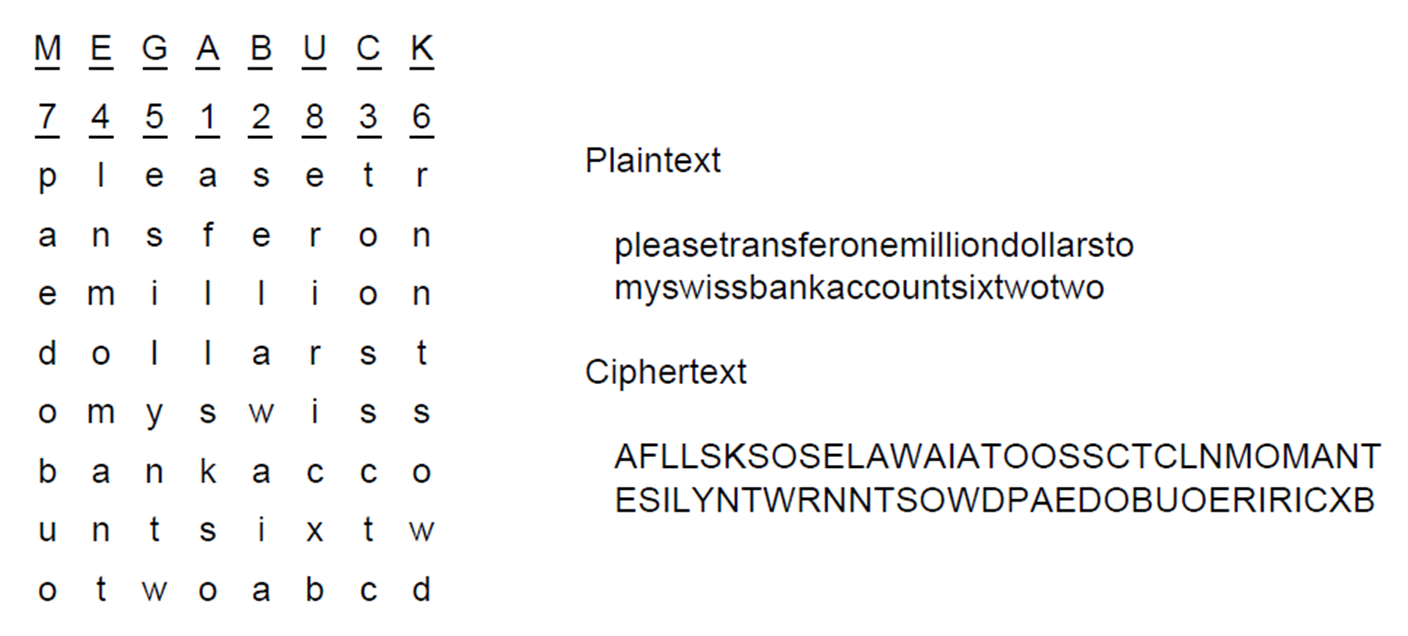
Pada awalnya enkripsi dilakukan dengan sangat sederhana seperti gambar 2 dibawah ini yang disebut substitution.



Gambar 2. Substitution

Pada teknik ini apabila kita mengenkrip kata pagi maka menjadi HQUO. Teknik sangat sederhana sehingga mudah untuk di ketahui.

Selanjutnya dengan perkembangan dalam ilmu cryptography, kemudian dikenalkan teknik transposition seperti gambar 3.



Gambar 3. Tramsposition

Pada gambar 3, pertama-tama kita harus menentukan kunci dari enkripsi dalam contoh ini kunci nya adalah MEGABUCK dimana huruf M adalah urutan ke tujuh dari system alphabet, kemudian karena total jumlah character tersebut ada delapan buah maka kita buat blok 8 x 8, kesamping 8 dan kebawah 8. Masukkan kata yang akan di enkrip secara mendatar atau kesamping, setelah itu cipher text nya adalah urutan kata dari atas kebawah berdasarkan nomor seperti gambar 2.

**Asymmetric Cryptography**

Pada tahun 1978, Ron Rivest, Adi Shamir, dan Leonard Adelman (RSA) mengenalkan sebuah metode yang menggunakan dua kunci untuk melindungi dan data yang digunakan secara bersama-sama. Dua kunci tersebut adalah public key dan dan private key. Organisasi atau orang dapat mendistribusikan kunci public-nya kepada orang orang secara bebas. Namun, untuk kunci pribadi atau private key harus disimpan dan dijaga dan jangan pernah dibagikan. Kunci kunci ini digunakan untuk proses yang dikenal sebagai enkripsi asimetris dan dekripsi.

Seperti ditunjukkan dalam Gambar 4 (sumber: Microsoft 2005), pengirim data atau informasi menggunakan kunci publik punya penerima untuk mengkonversi plaintext ke ciphertext. Ciphertext yang dikirim dan diterima oleh penerima dapat dikembalikan menjadi plaintext. Penerima dapat menggunakan kunci pribadinya untuk mengembalikan data atau informasi menjadi plaintext. Hanya orang dengan kunci pribadi yang sesuai dengan kunci publik yang dapat mendekripsi data, informasi, dokumen, dan lain lainnya. Ini terjadi karena dua kunci tadi, yang dapat dibuktikan secara matematis.

Membuat kunci public dan private key dapat dilakukan dengan menggunakan bilangan prima, step step nya adalah sebagai berikut:

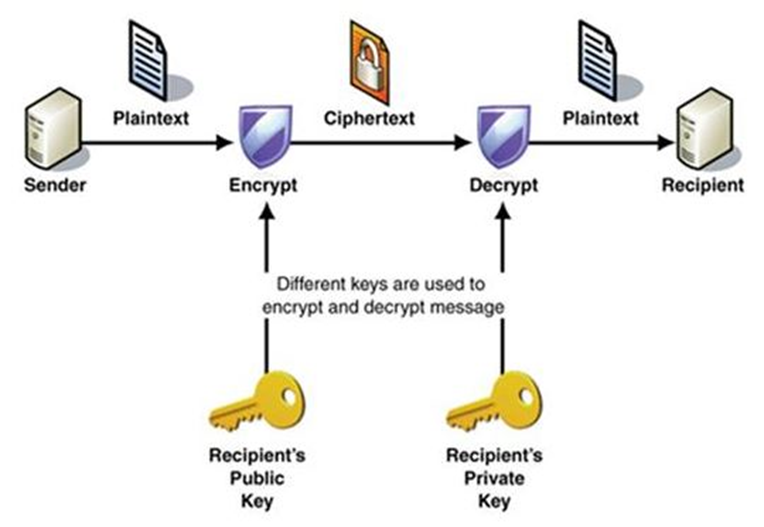
* Tentukan dua bilangan prima yang sangat besar secara random dan tidak sama, p dan q.
* Kedua bilangan prima dikalikan bersama-sama dan hitung z.

n = p x q and z = (p - 1) x (q – 1)

* Pilih angka relatively prima untuk z.
* Secara acak pilih angka atau nilai e (huruf e digunakan karena kita akan menggunakan nilai ini selama enkripsi) yang lebih besar dari 1, kurang dari z, dan relatif prima untuk z. Dua nomor dikatakan relatif prima jika mereka tidak memiliki faktor prima yang sama. Perhatikan bahwa e tidak perlu harus prima. Nilai e digunakan bersama dengan nilai n untuk mewakili kunci publik yang digunakan untuk enkripsi.
* Tentukan e sehingga e x d = 1 mod z.

Hitung nilai unik d (yang akan digunakan selama dekripsi) yang memenuhi persyaratan bahwa, jika d • e dibagi dengan z, maka sisa pembagian adalah 1. Notasi matematika untuk ini adalah d • e = 1 ( mod z). Dalam jargon matematika, kita mengatakan bahwa d adalah kebalikan perkalian dari e modulo z. Nilai d adalah harus dirahasiakan. Jika Anda tahu nilai z, nilai d dapat dengan mudah diperoleh dari e menggunakan teknik yang dikenal sebagai algoritma Euclidean. Jika Anda tahu n (yang umum), tapi tidak p atau q, maka nilai z sangat sulit untuk ditentukan. Nilai rahasia d bersama-sama dengan nilai n merupakan kunci pribadi.

Pilih salah satu kunci menjadi kunci public dan yang satunya private key

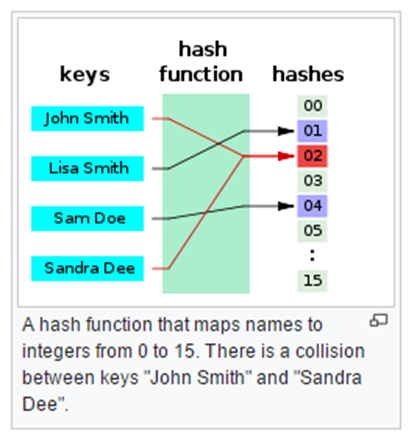


Gambar 4. Asymetric Cryptography

**Hash Function**

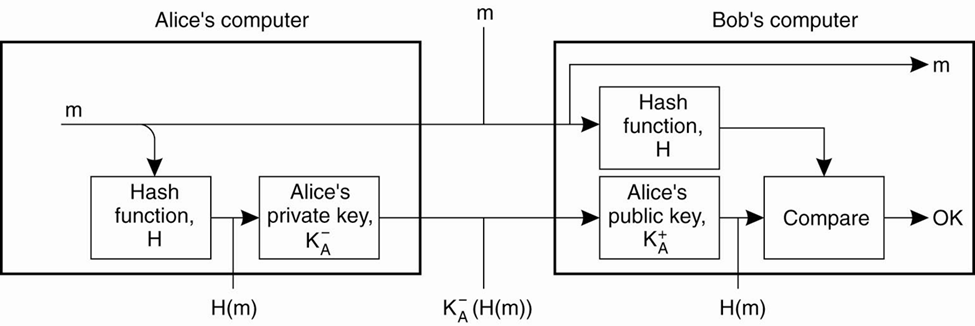
Sebuah fungsi hash adalah fungsi yang dapat digunakan untuk mapping atau merubah data dengan ukuran yang bermacam macam menjadi data dengan ukuran yang sama. Nilai-nilai yang dihasilkan oleh fungsi hash disebut nilai hash, hash code, atau hanya disebut hash saja. Salah satu penggunaannya adalah data struktur yang disebut tabel hash, banyak digunakan dalam perangkat lunak komputer untuk pencarian data yang cepat. fungsi hash mempercepat tabel atau database lookup.

Pada dasarnya hash function akan merubah input dengan jumlah character yang berbeda dan menjadikannya semua dengan jumlah karakter yang sama. Seperti contoh pada gambar 5 dibawah. Input dari Hash function adalah john smith, lisa smith, sam doe dan Sandra dee, setelah masuk ke hash fuction maka kempat input tersebut di enkrip atau di hash menjadi hanya 2 karakter, yaitu 01, 02 dan 04.



Gambar 5. Hash function

Dalam contoh ini terdapat collision karena input yang berbeda menghasilkan nilai hash yang sama, yaitu input john smith dan Sandra dee menghasilkan nilai hash yang sama yaitu 02. Hal ini tidak boleh terjadi dan memang kemungkinan terjadi collision sangat kecil sekali.



Gambar 6. Digital signature

Digital signature adalah standar yang paling dasar untuk kriptografi, dan biasanya digunakan untuk distribusi perangkat lunak, transaksi keuangan, perangkat lunak manajemen, dan dalam kasus lain di mana penting untuk mendeteksi pemalsuan atau attack. Sebuah digital signature atau tanda tangan digital adalah skema matematis untuk menunjukkan keaslian pesan digital atau dokumen. Sebuah tanda tangan digital yang valid memberikan alasan penerima untuk percaya bahwa pesan itu dibuat oleh pengirim yang sudah dikenal (otentikasi), bahwa pengirim tidak dapat menyangkal telah mengirim pesan (non-repudiation), dan bahwa pesan itu tidak diubah dalam transit (integritas).

Pada gambar 6 diatas adalah mekanisme tanda tangan digital yang paling sederhana dengan menggunakan private dan public key. Alice ingin mengirimkan pesan kepada Bob, maka alice akan mengenkrip pesan yang dia ingin kirimkan dengan private key Alice. Kemudian hasil encrypt tersebut dienkrip lagi kunci public dari bob. Barulah pesan tersebut dikirim kepada Bob. Setelah sampai di Bob maka untuk mengembalikan pesan tersebut supaya dapat dibaca oleh Bob, maka Bob pertama tama harus mendekrip pesan tersebut dengan private key Bob, kemudian hasil decrypt ini di decrypt kembali dengan menggunakan kunci public Alice. Dengan demikian maka Bob dapat membaca pesan dari Alice. Ini disebut digital signature karena yang mengetahui private key Alice hanyalah Alice sendiri.

**SIMPULAN**

1. Kritografi atau enkripsi adalah merupakan dasar utama dari teknologi keamanan elekronik saat ini.
2. Enkripsi sangat diperlukan untuk melindungi data yang penting, terutama pada saat di transmisikan baik dalam media kabel ataupun nirkabel.

**DAFTAR PUSTAKA**

1. Stallings, William. (2006). Cryptography and Network Security. 4th edition. Pearson Education.Whitman, M.E., Mattoro, H.J. (2013).
2. Scambray, Joel; Liu, Vincent; Sima, Caleb. (2011). Hacking Exposed Web Applications: Web Application Security Secrets and Solutions. 3rd Edition. McGraw-Hill. ISBN: 9780071740647.
3. Slay, Jill and Andy Koronios. (2006). Security and Risk Management. John Wiley & Sons, Inc.