



Isu dan prinsip proteksi TI (pak eng)

⌚ Created	@February 7, 2022 2:06 PM
🕒 Class	KULIAH
🕒 BLOCK	Block Chain
📎 Materials	
☑ Reviewed	<input checked="" type="checkbox"/>
☰ Column	
📅 Property	
☰ Property 1	
☰ Property 2	
☰ author	Cakra Darma

Content

Important Points

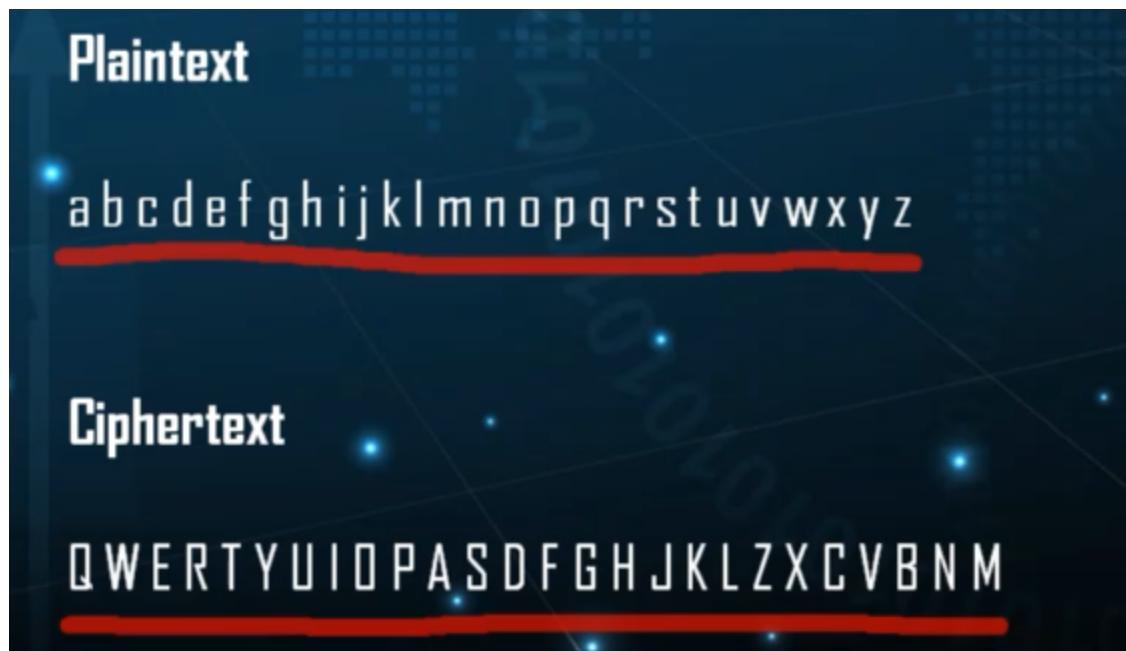
- pertemuan 1 : perkenalan mata kuliah bagaimana sistem perkuliahan saat offline atau online

pertemuan 2 : contoh hash : md5 dan SHA-256

- latarbelakang terdapat beberapa masalah keamanan pada bidang TI salah satunya yaitu pencurian data yang bisa diakibatkan oleh bug atau terdapat celah keamanan

pada suatu software

- jadi kita perlu mempelajari prinsip isu proteksi ti untuk mencegah masalah keamanan dalam bidang TI
- pembagian masalah kemanan
 - secrecy (kerahasiaan)
 - authentication(otentikasi)
 - nonrepudiation (bukti ttd digital sebagai tanda bukti tidak bisa disangkal)
 - integrity control (keaslian)
- cryptography digunakan untuk menyembunyikan pesan atau teks agar tidak dapat di baca atau dimengerti orang lain secara langsung
- cipher : transformasi karakter untuk karakter atau bit untuk bit tanpa memperhatikan bahasa penulisan dari struktur pesan
- code : menggantikan kata dengan kata lain atau simbol
- enkripsi kunci simetrik
 - setelah plain teks telah di enkripsi dengan keynya
 - key diperlukan untuk mendecrypt agar menjadi plain teks semula
 - setelah melewati internet maka akan di decrypt oleh key dan menjadi seperti semula
 - passive intruder : cuma ngintip , activie intruder ngintip dan merubah pesan menjadi berbeda jika enkripsinya lemah
- substitution cipher
 - mengganti serangkain huruf lainatau serangkaian huruf lain (caesar cipher)



- transposition cipher : mengatur ulang posisi huruf tanpa menyembunyikan menjadi huruf lain. harus tau kuncinya baru bisa dikembalikan

M E G A B U C K	Plaintext
7 4 5 1 2 8 3 6	
p l e a s e t r	please transfer one million dollars to
a n s f e r o n	my swiss bank account six two two
e m i l l i o n	
d o l l a r s t	
o m y s w i s s	
b a n k a c c o	
u n t s i x t w	
o t w o a b c d	

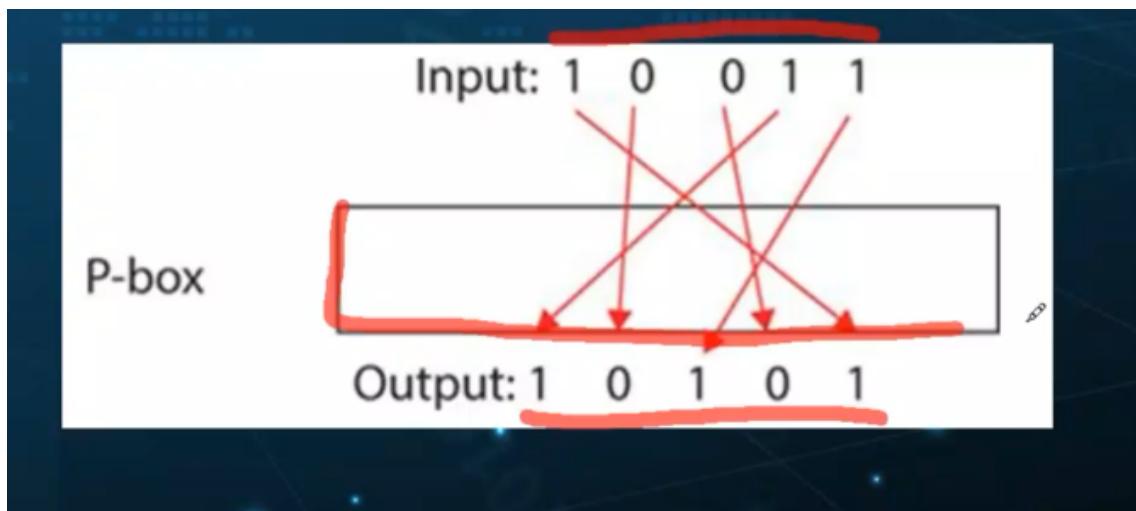
Ciphertext

AFLLSKSOSELAWAIATO OSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

- one time pads
 - komputasi xor tiap bit dari teks dengan kunci random

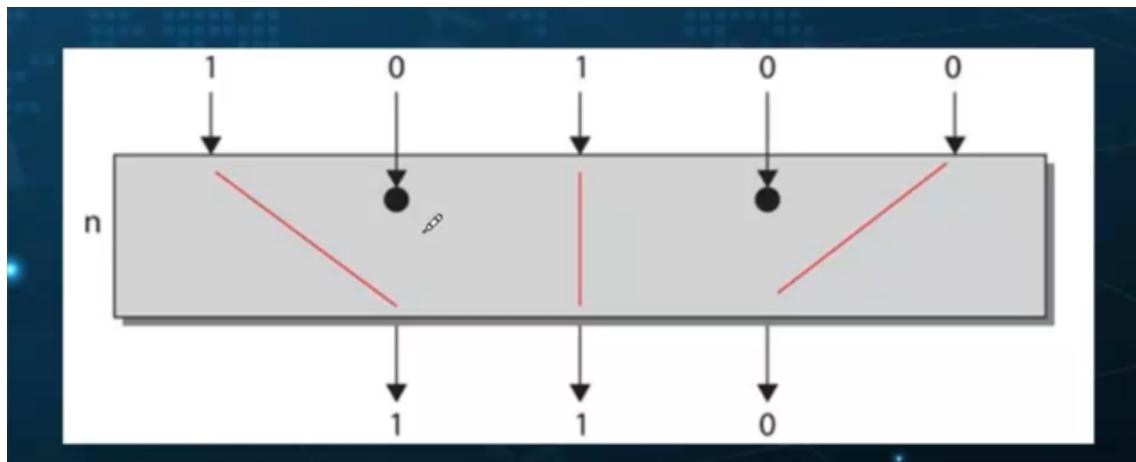
pertemuan 2

- terdapat dua jenis kriptografi yaitu modern cryptography saat ini menggunakan software/hardware dan tradisional crypography pada jaman dulu
 - tradisional
 - engima seperti mesin ketik menggunakan mekanis digunakan untuk komunikasi pada saat perang
 - modern
 - menggunakan teknologi terbaru dan lebih kuat keamanannya
- simemetric key algorithms
 - symmetric key
 - menggunakan kunci yang sama untuk membuka dan mengunci
 - block chipper
 - menggunakan n-bit block dari plaintext sebagai input yang menghasilkan n-bit block chipper text
 - p-box/permuation box
 - berfungsi untuk melakukan transposisi n-bit input
 - terjadi perubahan posisi tanpa merubah nilainya

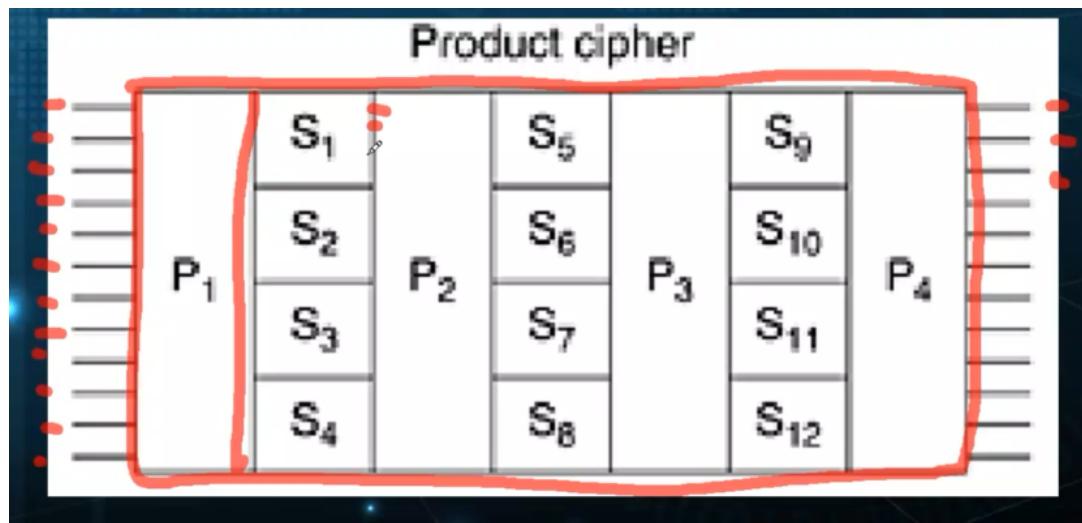


- s-box/ substitution/compression

- berfungsi melakukan substitusi n bit input ke n bit output
- terjadi proses kompresi tapi kontennya tidak berubah caranya tergantung algoritma

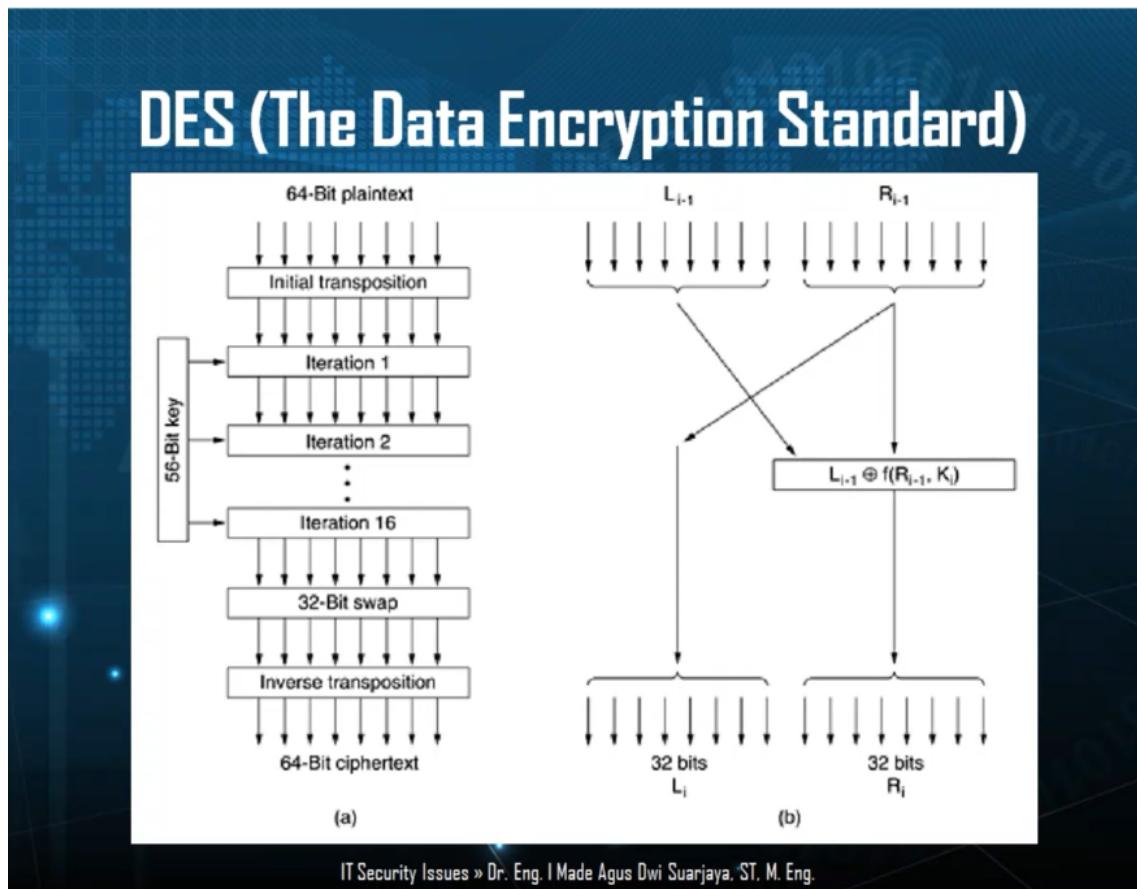


- product cipher
 - kunci diperlukan untuk menyimpan box supaya dapat dikembalikan lagi
 - jika tidak dapat dikembalikan enkripsi berarti merusak data
 - sebagai besar algoritma seperti ini ada pergantian bit data dari proses substitusi



- DES (the data encryption standard)

- standar awal yang dikembangkan oleh us government yang mengembangkan enkripsi pada january 1977 oleh ibm untuk komunikasi secara aman
- kalau sinyal radio (perang) ditangkap musuh suaranya cuma gak jelas
- diffie and helman mendesain mesin membongkar des dengan dana 20 juta dollar
-



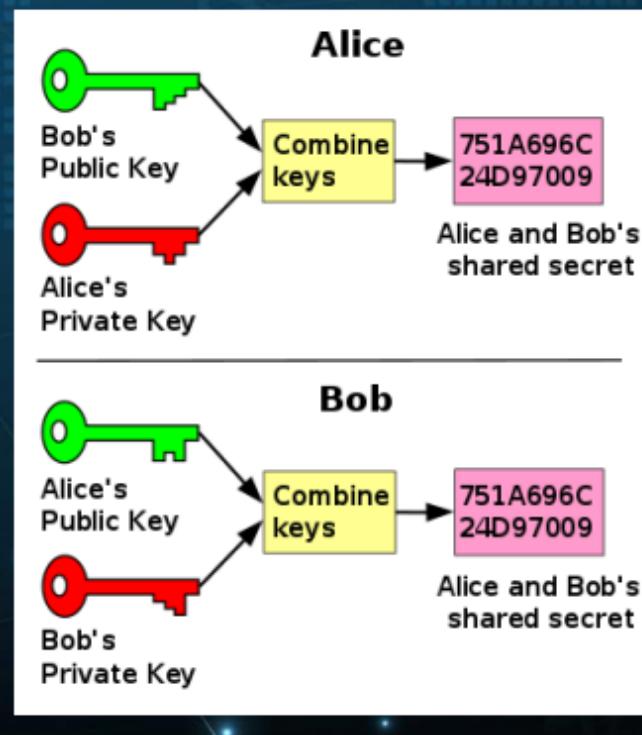
- AES (the advanced encryption standard)
 - NIST (national institute of standards and technology)
 - january 1997. kontes standar enkripsi baru
 - open source semua orang bisa mengimplementasikan dan tahu kelemahannya

- algoritma harus symmetric block cipher
- algoritma bisa diakses publik
- mendukung 128 192 256 bits semakin tinggi semakin aman brute force
- dimplementasikan dalam software dan hardware
- aes adalah nama algoritma yang akan nanti dipilih pada saat kontes yang menang adalah rijndael

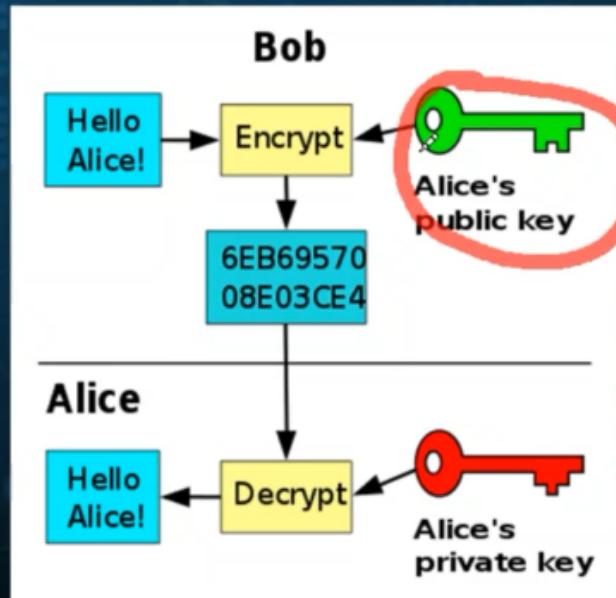
pertemuan 3

- asymmetric encryption
 - mengatasi kelemahan enkripsi symmetric karena hanya memiliki satu kunci saja
 - diperlukan public key untuk bertukar informasi
- public key algorithms
 - diffie and hellman tahun 1976
 - public key dapat diakses umum
 - private key hanya diakses pemilik
 - key dikeluarkan oleh key generator program dengan random number yang besar
 - lama vs baru

- **Diffie-Hellman** key exchange scheme



- **Asymmetric** key exchange scheme (RSA)



IT Security Issues » Dr. Eng. I Made Agus Dwi Suariaya, ST, M. Eng.

- **RSA** (Rivest, Shamir, Adleman) 1978

- Metode

- Pilih 2 bilangan prima besar, p dan q (biasanya 1024 bits).
- Hitung $n = p \times q$ dan $\phi = (p - 1) \times (q - 1)$.
- Pilih bilangan prima relatif dari ϕ lalu beri nama e .
- Temukan d dari $e \times d = 1 \pmod{\phi}$.

▪ RSA

- $p = 3$ dan $q = 11 \rightarrow n = 33$ dan $\phi(n) = 20$.
 - $d = 7$, karena 7 dan 20 tidak memiliki faktorisasi prima yang sama.
 - $7e \equiv 1 \pmod{20} \rightarrow e = 3$.

Plaintext (P)		Ciphertext (C)			After decryption	
Symbolic	Numeric	P^3	$P^3 \pmod{33}$		C^7	$C^7 \pmod{33}$
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	12800000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

IT Security Issues » Dr. Eng. I Made Agus Dwi Suarjaya, ST, M. Eng.

- public key lebih kecil karen dipertukarkan
 - private key lebih besar
 - kalau bukan block chipper encryptnya cuma 1 mengikuti jumlah plain text (rc4)

Pertemuan 4

Digital Signatures

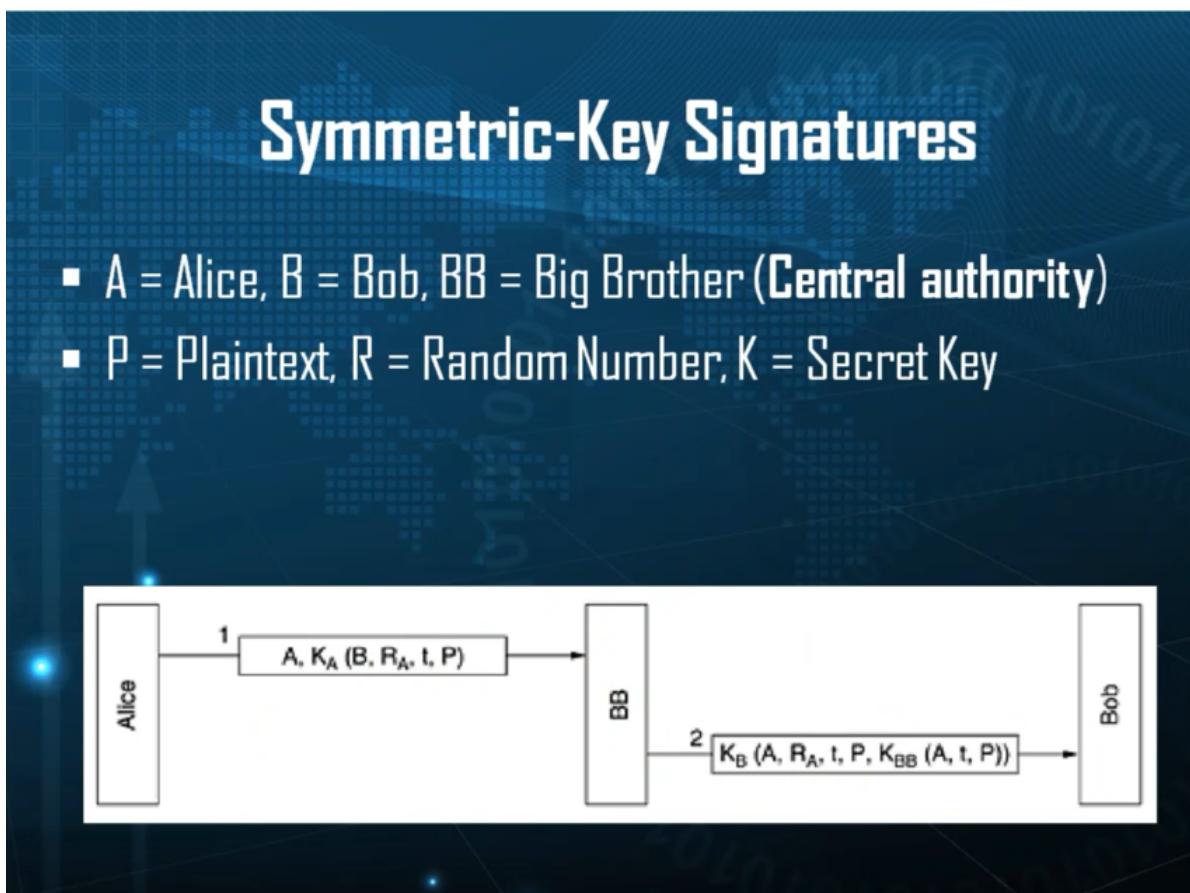
- introduction
 - suatu dokumen dikatakan sah jika ada tanda tangan (perjanjiannya) untuk memastikan keaslian dari suatu surat atau dokumen
 - tanda tangan pada digital bisa dimanipulasi tetapi bisa dicek apakah layak dengan menggunakan mekanisme seperti
 - verifikasi pengirim (verification)
 - pengirim tidak memungkiri (jadi jika pernah mengirim sudah ada buktinya) (repudiate)
 - tidak bisa dirubah penerima (concocted)

- diperlukan signatures

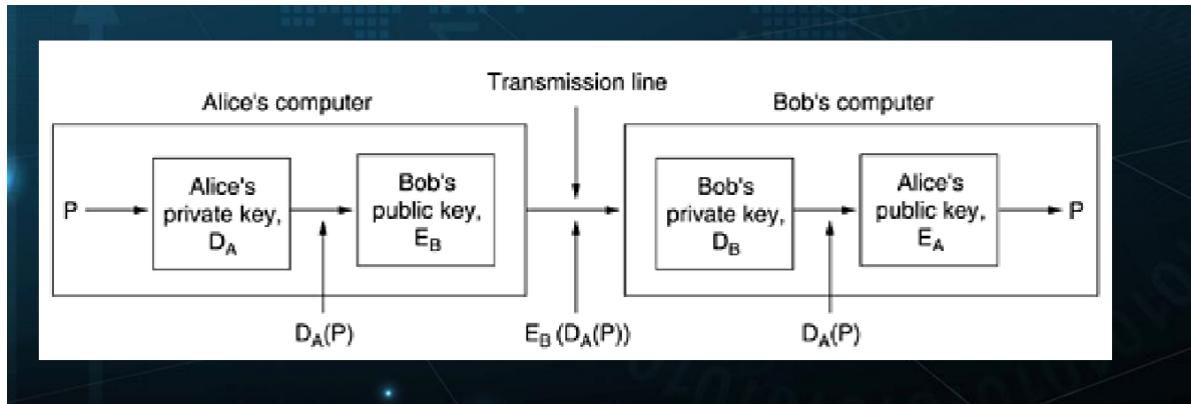
metode digital signature

- symmetric-key signatures

- algoritma ini jika digunakan untuk mengecek sah dokumen diperlukan pihak ketiga yang single authority BB(hal 3)
- BB itu seperti perantara yang mengetahui kedua kunci



- harus ada pihak ketiga pada symmetric key ini yang dapat melihat
- public key signatures
 - tidak memerlukan pihak ketiga sehingga menghindari oknum
 - diperlukan public atau private key untuk membuka isi konten



- rsa adalah defacto yang menggunakan public key signatures
- bagaimana jika pesan tidak harus rahasia maka muncul message digest
- message digest
 - dipastikan pembuatnya siapa dan bahwa dokumen asli tanpa perubahan dan bisa dilihat semua orang
 - sedangkan jika signatures harus rahasia
 - tidak bisa di dekripsi dan bisa dipastikan keasliannya
 - syarat

Message Digests

- Syarat Message Digest

- Diketahui P , sangat mudah mengkomputasi $MD(P)$. ✓
- Diketahui $MD(P)$, tidak mungkin mendapatkan P . ✗
- Diketahui P , tidak mungkin mendapatkan P' , $MD(P') = MD(P)$.
- Perubahan 1 bit pun akan mengubah output.

- **MD5** (Rivest, 1992) dan **SHA-1** (NIST, 1993) .

Manajemen Public key

- intro
 - tidak memerlukan kunci yang sama untuk berkomunikasi rahasia tetapi harus kenal orangnya dan mengetahui public keynya
 - memang public key disebar cara memastikan public key adalah..
- cara komunikasi
 - bisa ditaruh di public key di website
 - masalahnya bisa kena phising
 - akhirnya diperlukan ada certificate dan pihak ketiga yang memastikan bahwa public key benar
 - on demand atau taruh di server
 - memunculkan masalah karena server harus hidup dan erkoneksi inernet

- certificate authority (CA)
 - bisa dilakukan offline karena sudah ada tanda tangan ca yang bisa memeriksa pemilik
 - Ca tugas untuk memverifikasi data pemilik dengan CA private key yang bisa saat offline
 - contoh pada browser bisa memverifikasi saat offline karena ada ca pada file browser atau sistem operasi
- x.509 adalah standard certificate untuk mencegah peredaan certificate yang mungkin terjadi
- public key infrastructure (PKI) untuk mengatasi banyaknya ca dengan memanajemennya
- uts
 - minggu depan online
 - merekam dari kanan mengconver semua dan memegang kertas tangan kiri tanpa contekan
 - 13.30 sampai jam 4
 - pastikan cerita dari materi 2 -6 ada 5 dalam waktu 5 menit

Pertemuan 7

Communication Security

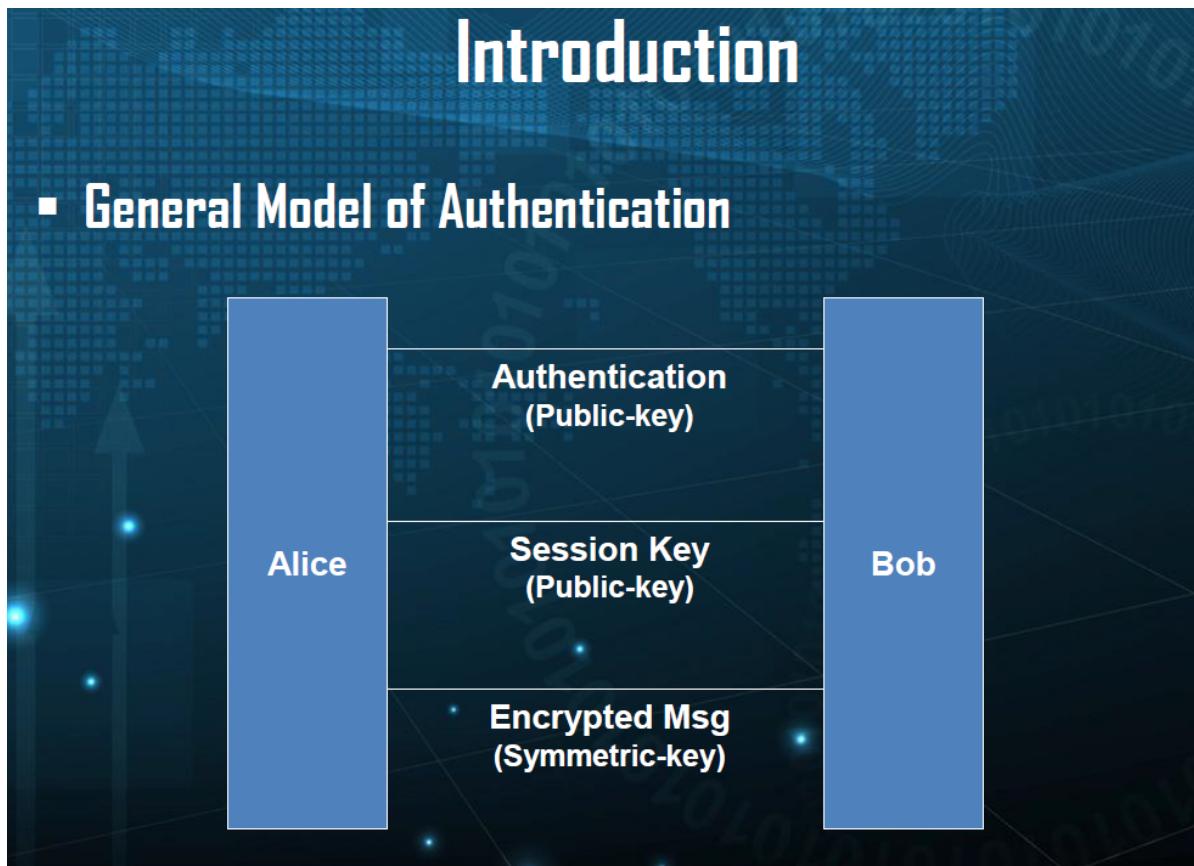
- Ip sec
 - IETF (internet engineering task fore) membuat standar yang berhubungan dengan internet
 - Ip security
 - RFC 2401, 2402 dan 2406
 - RFC 2410 : digunakan untuk testing saja
 - Multiple services

- alacarte sesuai keperluan yang bisa disesuaikan sesuai algoritma contoh des, aes dll
- multiple algorithms
 - menghindari dipecahkannya algirtma agar framework bisa bertahan. jadi seperti menyetting algoritma
- multiple granularities
 - melindungi trafik TPC dari ujung ke ujung (proses saat melewati jaringan sajas) tidak termasuk didalam komputer misalnya https untuk mengamankan jaringan
- IPsec authentication header (transport mode)
 - AH (authentication header) : berukuran 32 bit jadi dalam 4 byte ada next header, payload len dan reserved
 - HMAX(hashed message authentication code) : yang menggunakan IPsec akan berubah strukturnya seperti digambar. intinya sususann 0101 akan berubah menjadi seperti digambar
- ESP (encapsulating security payload)
 - ipsec authentication header (transport mode)
 - ipsec authentication header (tunnel mode)
 - ESP ini intinya liat di data link layer
- firewalls
 - packet filter : fungsinya seperti bucket filter. membiarkan bit yang bagus dan mengeluarkan bit yang buruk
 - pada gateway akan ada filter yang membatasi yang masuk dan keluar
 - bisa juga menutup port tertentu
 - pada firewalls ada settingan port dan juga ip
 - tidak bisa mengatasi karena bukan solusi yang paling bagus
 - serangan DOS(denial of service)
 - TCP SYN > SYN + AcK

- melumpuhkan target dan menghabiskan source
- DOOS (distributed denial of service)
 - hampir sama tetapi serangan dari banyak sumber
 - contoh main game komputer kita menyerang komputer lain tanpa sepengetahuan pengguna. komputer kita menyerang dengan connect ke server kita tapi tidak melakukan apapun
 - mesin penyerang > malware
 - paling banyak ditemui di internet sekarang . bisa jadi jika layanan down maka diserang DOOS
 - dapat diatasi dengan sejenis layanan cloud yang multi region. jadi lokasi server ada di banyak region
- VPN
 - awalnya bertujuan untuk menggabungkan dua jaringan local yang normalnya kita harus enarik kabel kedua tempat. contoh gunain vpn maka jaringan kita seperti berada pada jaringan di amerika
 - leased line private network
 - virtual private network
- 802.11 security
 - sudah expired tidak dipakai lagi
 - WEP (wired equivalent privacy)
 - WPA / WPA II (Wi-fi protected access)
- Bluetooth security
 - kelemahan
 - jarak dekat
 - tanpa passkeys
 - hanya device

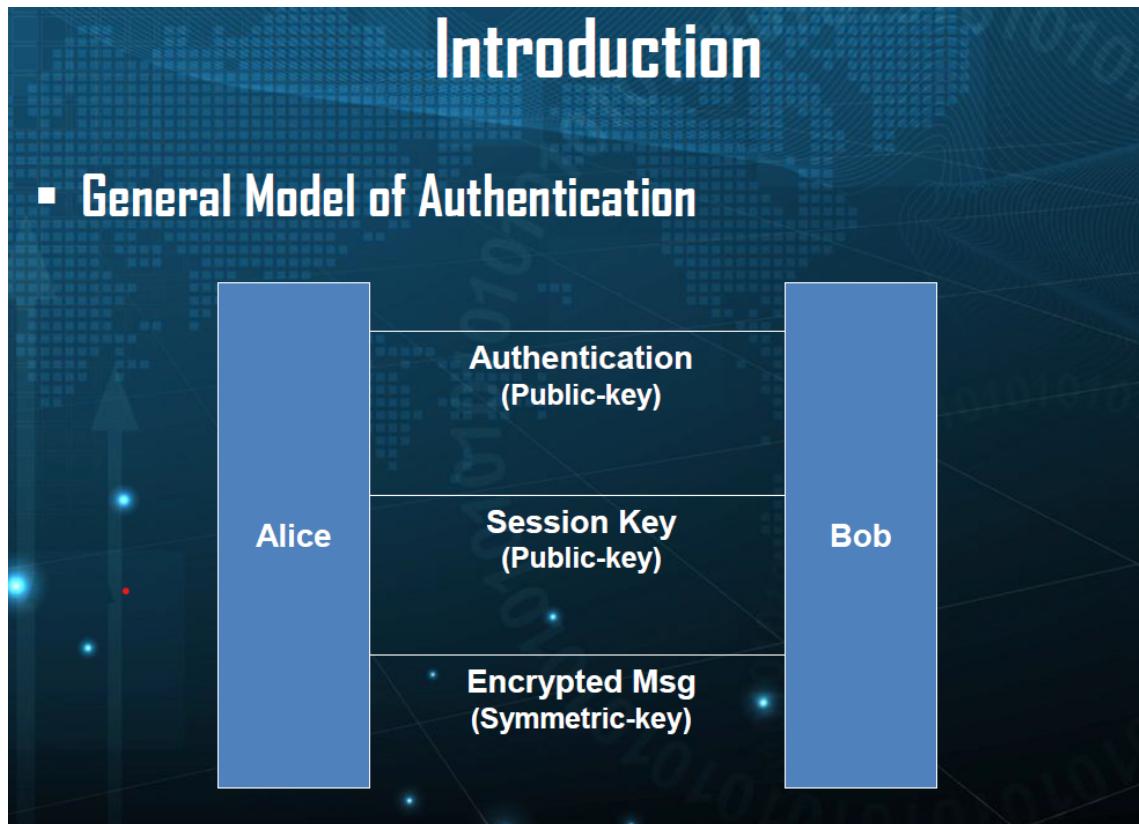
Pertemuan 8

- authentication
 - memastikan lawan bicara
 - apakah ini proses miliki scott
- authorization
 - memberikan hak akses
 - apakah scott bisa menghapus book old
 - di linux setiap folder ada owner tapi beberapa folder ownernya itu root semua bisa mengakses nya



- ketika terhubung harus memakai public key dimana kita tidak secara nyata mengirimkan kunci lewat jaringan. jadi publickey itu hanya untuk berinterkasi kunci public key
 - untuk kenalan pake public key. Jadi setelah kenal maka akan pake symmetric key

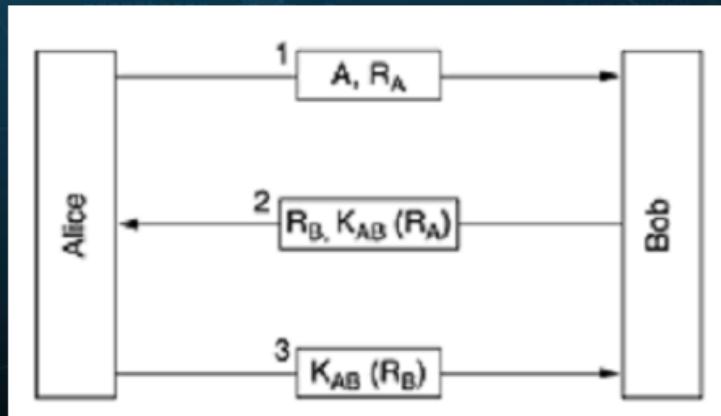
- bertukar session key
- encrypted msg(symmetric-key)
- shared secret key
 - normal authentication (sudah ada shared key)



- nanti bakal ada number random untuk bertukar session.
- karena tiap sessionn bisa berbeda challengenya bisa random number bisa lainnya
- shortened sauthentication (sudah ada shared key)

Shared Secret Key

- Shortened Authentication (Sudah ada shared key)
 - A = Alice ID, B = Bob ID
 - R = challenges, K = Key



IT Security Issues » Dr. Eng. I Made Agus Dwi Suarjaya, ST, M. Eng.

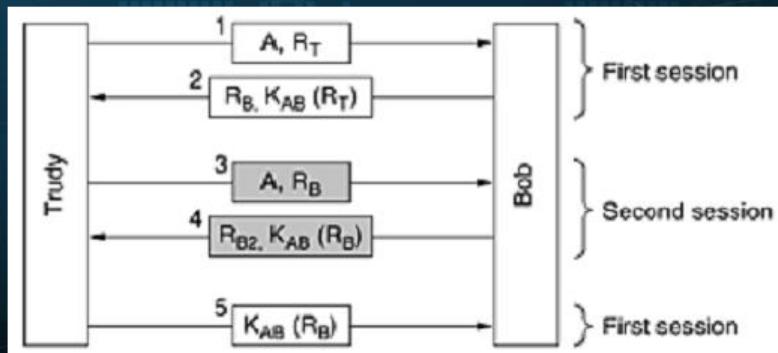
- cuma ada tiga langkah tapi konsepnya sama saja.
- bisa kena retraction/reflection text
 - reflection attack (sudah ada shared key)

Shared Secret Key

- Reflection Attack (Sudah ada shared key)

- A = Alice ID, B = Bob ID, T = Trudy

- R = challenges, K = Key

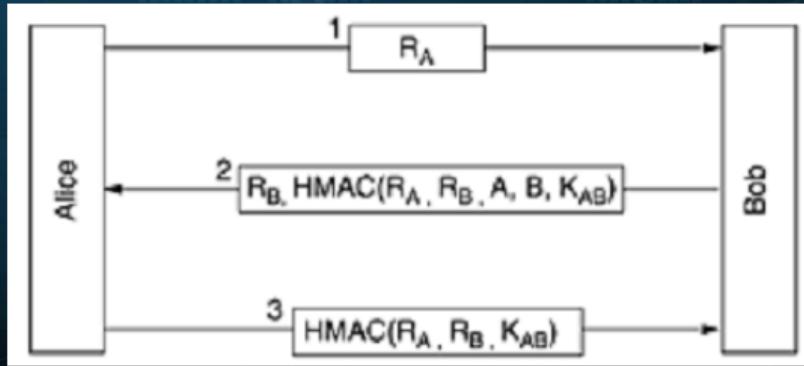


IT Security Issues » Dr. Eng. I Made Agus Dwi Suarjaya, ST, M. Eng.

- session pertama didiamkan kemudian ketika dibuka session baru
- secara bersamaan membuka dua session
- contohnya kita ditelpon penipu dan ngaku orang kita kenal kecelakaan. dan kita dipancing memberi jawaban dimana penipunya akan sering bertanya.
- jawaban dari bob menjadi seolah seolah menjadi alice. dimana bob meng acc jawabannya sendiri
- ada pencegahannya
 - HMAC(sudah ada shared key)

Shared Secret Key

- HMAC (Sudah ada shared key)
 - A = Alice ID, B = Bob ID, T = Trudy
 - R = challenges, K = Key

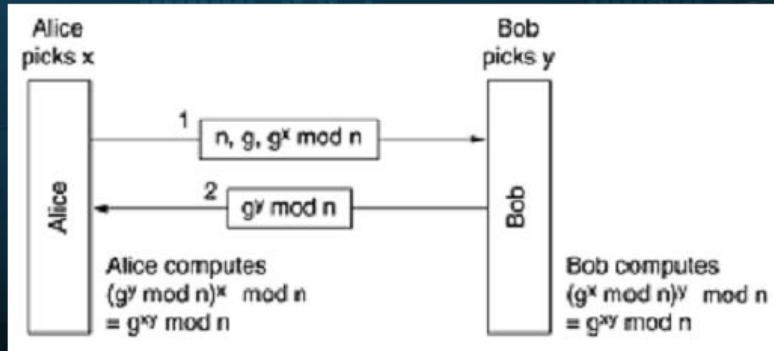


IT Security Issues » Dr. Eng. I Made Agus Dwi Suarjaya, ST, M. Eng.

- solusi pencegahan dan lebih aman
 - diffie hellman key exchange (belum ada shared key)

Shared Secret Key

- Diffie-Hellman Key Exchange (Belum ada shared key)
 - $n, g = \text{large number (prime number, } (n - 1)/2)$
 - $x = \text{Alice secret (large number 512-bit)}$, $y = \text{Bob secret}$

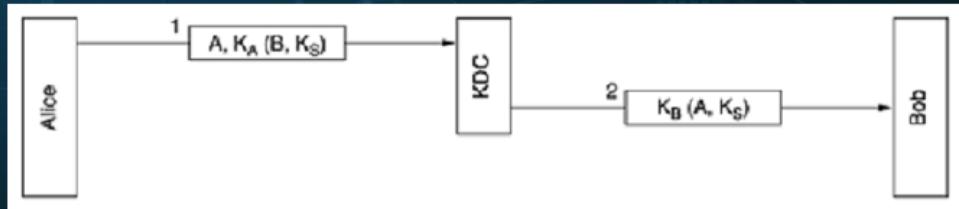


IT Security Issues » Dr. Eng. I Made Agus Dwi Suarjaya, ST, M. Eng.

- kita tidak mengirim kunci angka 4
 - angka 4 di generate sendiri dimana tidak melewati jaringan
 - trusted key distribution center (KDC)

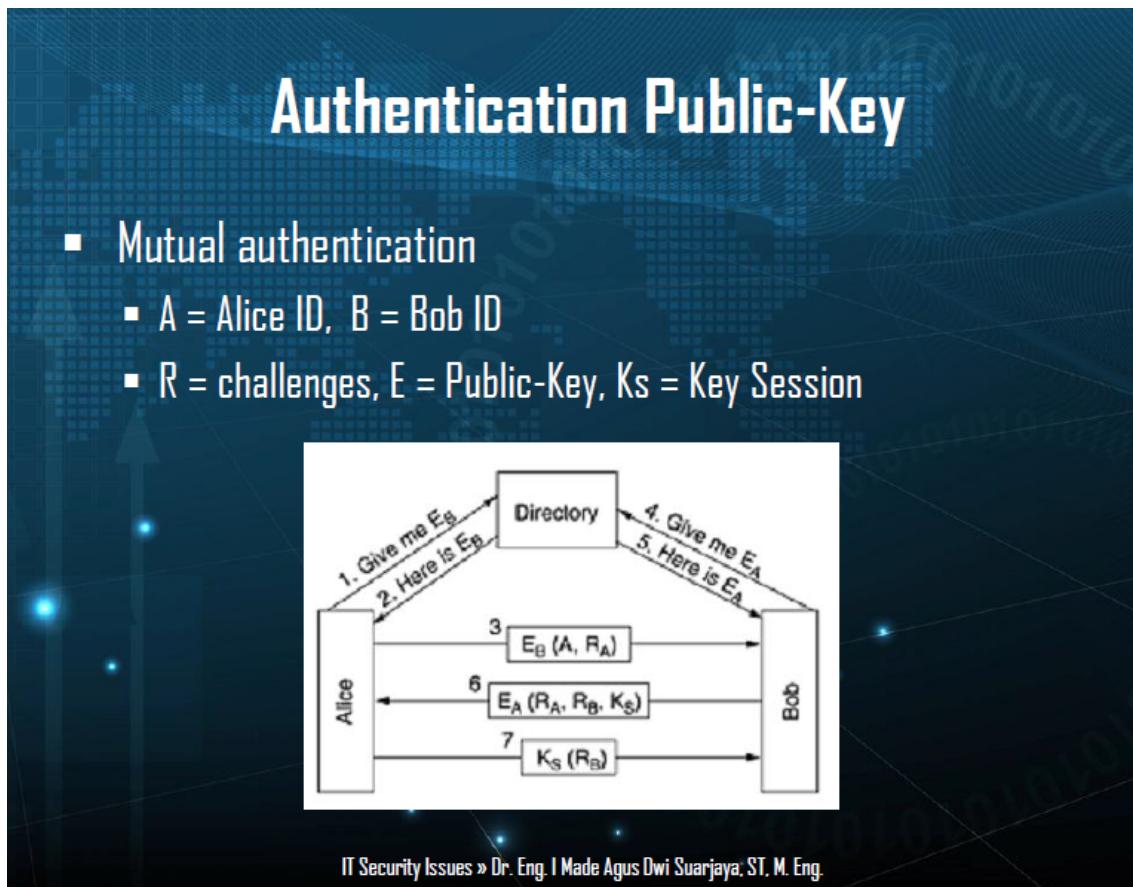
Shared Secret Key

- Trusted Key Distribution Center (KDC)
 - A = Alice ID, B = Bob ID, T = Trudy
 - K = Key, K_S = Key Session



- ada server centernya
- ada pihak ketiga yang melakukan komunikasi sebelum memperbolehkan komunikasinya KDC
- authentication kerberos
 - authentication server (as), ticket granting server (tgs)
 - alice untuk berkomunikasi dengan bob atau orang tertentu harus melewati beberapa proses seperti login untuk memastikan bahwa ini memanglah si alice
 - bisa ngecek di login server
 - TGS akan memberikan ks kb supaya bisa koneksi ke bobnya
 - cara yang paling sering dilihat jika melihat di layanan internet. contohnya kita buka imissu kita di redirect ke halaman lain tapi kita login di imissunya. jadi sistem imissunya itu cuma login
 - authentication public key

- o mutual authentication



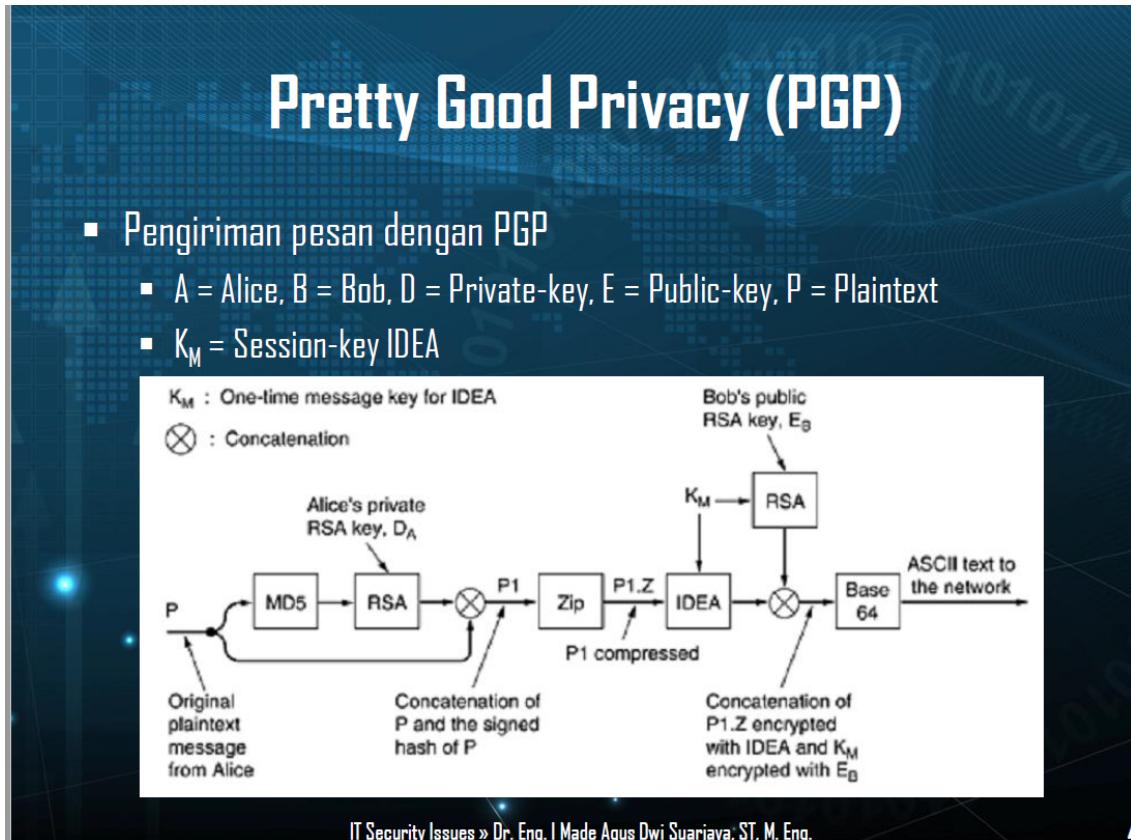
- public key ditaruh dimana gitu misal di web server lalu saat ada request orang ngeresponse sambil nyertain public keynya itu
- tanpa pihak ketiga untuk ngecek
- proses ini hanya untuk di tempat tertentu saja
- o conclusion
 - authentikasi pasti berhubungan dengan hak akses
 - Metode Authentication, shared secret key, Kerberos dan Public Key
 - Metode berbagi Secret Key, Diffie-Hellman Key Exchange, Trusted Key Distribution Center (KDC)

Pertemuan 10

Email Security

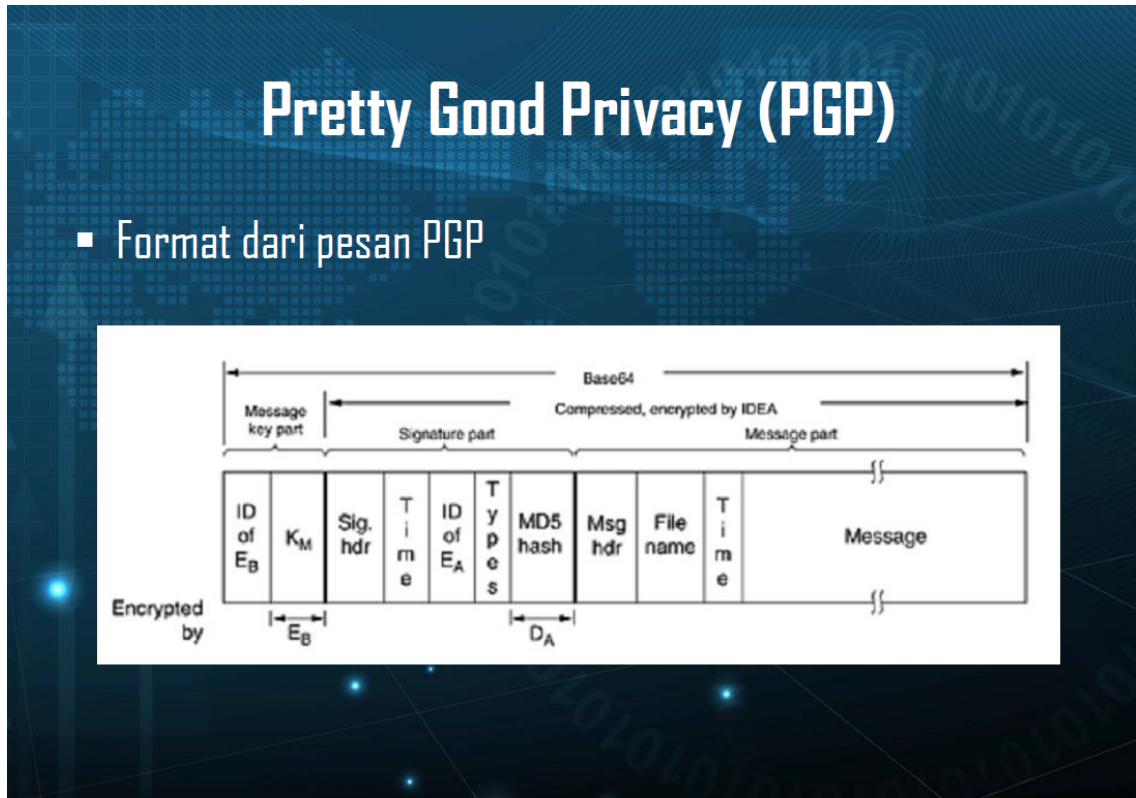
- introduction
 - Email
 - email adalah komunikasi jarak jauh menggunakan elektronik mail yang transit melewati banyak komputer sampai ke tujuannya dan tiap komputer dapat menyimpan dan membaca.
 - pada awalnya ucma ngirim file text dan keamanannya sangat rendah. jadi perlu keamanan
 - keamanan
 - hanya bisa dibaca penerima
 - tidak bisa dibaca atasan maupun pemerintah
- pretty good privacy (pgp)
 - phil zimmermann, 1991
 - konten dari pengirim ke server sampai ke penerima pasti terlindungi dari awal. yang tidak hanya keamanan pada protokol saja karena protokol hanya mengamankan di di jaringannya saja
 - keamanan lengkap
 - privacy
 - authentication
 - digital signatures
 - compression
 - block cipher menggunakan IDEA (International Data Encryption Algorithm), 128 bit keys
 - pengiriman dengan pgp
 - awalnya plain text dari alice

- lalu dibagi dua jalur yang menggunakan private key dari alice. lalu digabung kembali pada p1. ada proses kompresi lalu ada proses idea dan lainnya sampai ke proses base 64.
- bisa diotak atik di bagian ideanya
- proses lumayan rumit karena ada proses enkripsi dan penggabungan



- dapat menggunakan 4 key-length strength RSA
 - casual (384 bits) : mudah dipecahkan (gak juga)
 - commercial (512 bits) : bisa dipecahkan organisasi 3 huruf (NSA)
 - military (1024 bits) : tidak bisa dipecahkan siapapun di bumi
 - Alien (2048 bits): tidak bisa dipecahkan siapapun bahkan yang dari planet lain
- alien strength key, rekomendasi yang seharusnya dipakai
- format dari pesan PGP

- nantinya seluruhnya akan dikirim dalam bentuk base 64. dan nanti akan ada id dari kunci publik, kunci session, signature, dll yang semuanya dienkripsi.
- nantinya ada proses pembacaan base 64 yang bisa dimengerti oleh penerima.



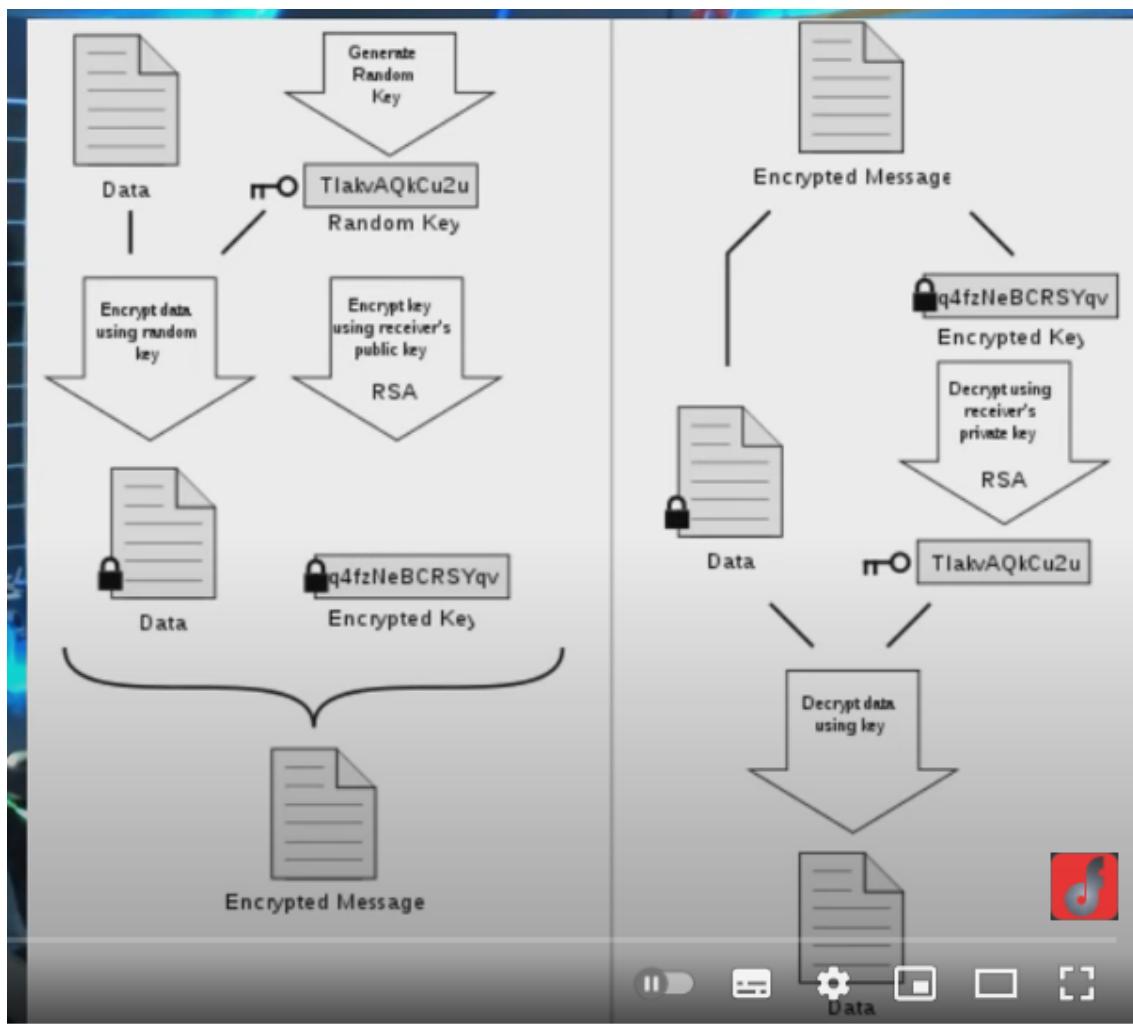
- privacy enhanced mail (PEM)
 - merupakan standar keamanan email yang lebih lama dibandingkan dengan S/MIME
 - 1980
 - RFC 1421 - RFC 1424
 - memerlukan CA
 - ditinggalkan
 - tidak ada yang mau menjadi root karena menghabiskan resource.
 - politik (mungkin ada pengembangan baru dll)
- S/MIME

- secure/mime
- IETF (international engineering task force)
- RFCs 2632 -2643
- fitur
 - authentication
 - data integrity
 - secrecy
 - nonrepudiation
- conclusions
 - Email security diperlukan untuk memberikan keamanan pada email yang intinya agar hanya bisa dibaca oleh penerima
 - gak pasti kalau gak pake email security memang mungkin saat dikirim dalam internet menggunakan kemanan protokol tapi belum tentu di enkrip saat dikirim dan diterima.
 - contoh email security, pretty good privacy (PGP), pricary enhanced mail (PEM) dan secure/MIME jadi diamankan di kirim dan disimpan ke server dan komputer lainnya karena saat mengirimkan email kita melalui banyak komputer
 - nanti akan ada tugas menggunakan pgp ini.

menggunakan mailvelope

- PGP
 - pretty good privacy
 - salah satu contoh yaitu mailvelope
 - PGP menggunakan public key dan private key
 - kita bisa mengrim dan menerima encrypted message

- menambahkan ekstra layer security dari pada hanya menggunakan protokol smtp (end to end encryption)
- ..
- pgp merupakan program enkripsi yang membantu melakukan enkripsi terhadap pesan dan email ke orang lain. bisa juga untuk mendatangani, enkripsi dan dekripsi, file, direktori sampai partisi hardisks
- pada kriptografi modern ada dua kunci yaitu public dan private key. yang digunakan pada pgp.
- kunci public di share ke orang lain. private disimpan dan tidak boleh orang lain tau
- cara kerja



- pertama kali dibangun ada random key yang bisa hanya sekali pakai. pesan akan dikunci menggunakan random key tadi yang menjadi enkripsi. nanti hasil enkripsi tadi akan dienkripsi lagi menggunakan public key. hasil enkripsi akan digabungkan antara data enkripsi hasil random key dengan kunci random key (digabung menjadi satu baru disebut encrypted data)
- key management
 - generate key : buat private dan public key
 - import key : mengimport key teman public key untuk mengirim asymmetric key
 - advanced untuk menggunakan algoritma
 - password untuk menyimpan key
 - tidak boleh share private key hanya public key untuk yang mau sharing saja. public key kalau bocor gak masalah karena hanya digunakan untuk enkripsi data sedangkan private digunakan untuk decrypt data.
 - jadi intinya kita tukaran kunci public terus untuk buka pesan itu kita perlu kunci public yang ditukar itu dan private key milik kita

Pertemuan 11

- keamanan
 - komunikasi
 - email
 - web
 - objek dan sumber daya dinamai harus aman agar tidak nyasar ke website lain
 - bagaimana koneksi aman terotentikasi dibentuk
 - bagaimana bila website mengirim kode eksekusi jadi tidak ada celah untuk disisipi kode oleh orang lain
- threats

- hacker/cracker
 - yahoo, the U.S.Army, the CIA,
 - Deface > Yahoo, U.S.Army, CIA,NASA
 - DDOS : walaupun web sudah aman ada faktor external yang menghabiskan resource
 - Cracker Swedia, 1999, Microsoft Hotmail
 - Cracker rusia, maxim, e commerce 300000 CC :kasus carding
 - USA, email web berita, saham emulex corp short selling :mengirim email pake nama ceo ngasi tau suatu kondisi yang membuat saham emulex corp short selling
- secure naming
 - DNS spoofing (normal/spoofing)
 - normal
 - ketika ingin browsing ke alamat tertentu maka akan ngontak ke DNS server tertentu
 - jadi bisa nyari ip saj alalu dikembalikan index html lalu memberikan home page
 - spoofing
 - yang dikirimkan bukan tujuan tapi ip orang lain yang memberikan fake home page
 - makanya ada secure DNS
 - Secure DNS
 - hampir semua dns server sudah mengaplikasikan ini
 - bukti sumber data
 - distribusi public key
 - autentikasi transaksi dan request
 - Secure Sockets Layer (SSL)

- 1995, Netscape COnnected Communications
- 1996, TLS (SSL 3.1)
- fitur
 - negosiasi parameter antara server dan client
 - otentikasi mutual antara server dan client
 - komunikasi rahasia
 - proteksi integritas data
- https (secure http)
 - http port 80 over ssl
 - port 443 httpsnya
- mobile code security
 - java applets
 - bugg, security policy (allow /reject) misal website yang punya java applets bakal ada notif mau jalan atau gak
 - activeX
 - mirip seperti java applets tapi di windows,
 - trusted > bisa melakukan apapun tanpa melihat kode tapi sekarang sudah gak ada
 - sering mengalami masalah keamanan
 - JavaScripts
 - kode asing berjalan pada PC > masalah (alert, iklan)
 - sudah sangat mandatori javascript di website
 - bisa ngehandle alret dan iklan jadi gak ada spam
 - viruses
 - ineksi executable, reproduce, kerusakan sistem
 - dulu otomatis ketika colok flashdisk pake fitur auto run

- conclusions
 - web security, mengurangi ancaman threats dengan menamai objek dan sumber daya dengan nama secure naming, membentuk koneksi aman terotentikasi ssl, dan solusi bila website mengirim kode eksekusi (mobile code security)

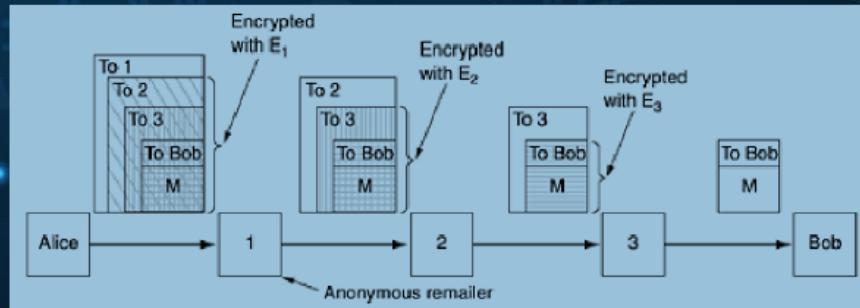
Social Issue

- privacy
 - hak untuk Privasi
 - diatur undang-undang
 - pemerintah harus punya surat resmi
 - alasan yang kuat
 - keadaan real
 - bisa memata-matai tanpa datang geledah
 - provider telepon dan internet
 - cryptography
 - mempersulit pemerintah
 - muncul aturan pemerintah mengatur kunci supaya bisa dijebol oleh mesin pemerintah
 - perdebatan
 - banyak digunakan kegiatan melanggar hukum
- Anonymous remailers
 - PGP, SSL
 - memberikan keamanan
 - antara 2 pihak yang saling kenal

- pengirim dan penerima bisa mengkhianati
- anonymous
 - kadang lebih baik
 - tidak diketahui sumber
 - whistleblowers : membierkna informasi yang diperlukan tanpa melampirkan sumberr
- cypherpunk remailers
 - jasa email
 - cipher public key
 - tanpa info pengirim
 - tanpa log/pencatatan
 - tanpa akun login
 - tanpa jejak
 - cara kerja
 - tidak bisa mentrakcing kebelakang
 - penerima tidak tahu siapa pengirim akibatnya

Anonymous Remailers

■ Cypherpunk Remailers



IT Security Issues » Dr. Eng. I Made Agus Dwi Suarjaya, ST, M. Eng.

6

- freedom of speech
 - pembatasan (tergantung pemerintah berkuasa)
 - materi tidak cocok untuk remaja
 - kebencian berbau sara
 - informasi demokrasi atau komunis
 - sejarah berbeda dari versi pemerintah
 - dokumentasi cara membongkar kunci, membuat senjata, dll
- steganography
 - ilmu menyembunyikan pesan
 - ada warna bit yang lian yang hanya bisa di deteksi oleh komputer

- misal mata manusia juga tidak bisa membedakan fps pada layar
- gambar 1024 x 768 pixels (8bit)
 - low order bit untuk menyimpan informasi rahasia
 - terkompresi dan terenkripsi ide
 - bisa disisipkan informasi rahasia
 - selain gambar bisa audio/video
 - bisa untuk watermarking
- copy right
 - perlindungan hak cipta
 - seumur hidup pencipta
 - ditambah 50-57 tahun setelah kematian untuk corporate
 - bebas untuk publik setelah kadaluarsa
 - munculnya dmca
 - perlindungan hak cipta di internet
 - mengurangi pertukaran data digital ilegal
- conclusion
 - privacy. kerahasiaan warga negara dijamin pemerintah dselama tidak terjadi pelanggaran atau kepentingan negara
 - anonymous remailers, jasa pengiriman email tanpa informasi pengirim
 - freedom of speech, adanya pebatasan untuk kebebasan berbicara di internet tergantung pemerintah yang berkuasa
 - steganography, ilmu menyembunyikan pesan pada media lain
 - copyright, munculnya perlindungan hak cipta di internet (DMCA)

Quiz

- tgl 30 pertemuan 8 -12