SLIDE MATA KULIAH KRIPTOGRAFI PROGRAM STUDI TEKNOLOGI INFORMASI

VISI PROGRAM STUDI TEKNOLOGI INFORMASI

Menjadi Program Studi yang unggul dalam pengembangan keilmuan teknologi informasi untuk mendukung ekonomi kreatif tahun 2033.

MISI PROGRAM STUDI TEKNOLOGI INFORMASI

1. Menyelenggarakan pendidikan pada bidang teknologi informasi yang berkualitas.
2. Menyelenggarakan Penelitian di bidang teknologi informasi yang berkualitas.
3. Menyelenggarakan pengabdian masyarakat di bidang teknologi informasi dalam rangka meningkatkan kualitas sumber daya manusia.
4. Mengelola Program Studi secara mandiri dengan tata kelola yang baik.

PROFIL LULUSAN PROGRAM STUDI TEKNOLOGI INFORMASI

1. System Administrator

Mampu dalam melakukan analisa terhadap kebutuhan pengguna sistem jaringan komputer, mengindentifikasi sistem jaringan dengan teknologi yang sesuai, mampu merancang arsitektur, sistem keamanan dan pengujian server, mampu menginstall dan mengkonfigurasi sistem operasi server, file sharing pada server, virtual server serta common network and application services server, membuat kode program server, memgimplementasikan dan memantau kinerja dan keamanan sistem, menginvestigasi dan memperbaiki kerusakan sistem serta mampu mengevaluasi dan melakukan restore system.

PROFIL LULUSAN PROGRAM STUDI TEKNOLOGI INFORMASI

2. Cyber Security Analyst

Mampu menerapkan prinsip perlindungan informasi, prinsip keamanan informasi untuk penggunaan jaringan internet, prinsip keamanan informasi pada transaksi elektronik, mampu menyusun dan melaksanakan dokumen kebijakan keamanan informasi, mampu mengaplikasikan ketentuan/persyaratan keamanan informasi, mengelola log dan Melaksanakan pencatatan asset, Mampu Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan mampu Mengidentifikasi serangan-serangan terhadap kontrol akses dan mampu melakukan instalasi software aplikasi

PROFIL LULUSAN PROGRAM STUDI TEKNOLOGI INFORMASI

3. Object Programmer

Mampu melakukan identifikasi library, komponen atau framework yang diperlukan, dan menggunakan struktur data, Mampu mengimplementasikan user interface dan rancangan entitas serta keterkaitan antar entitas, Mampu menerapkan pemecahan permasalahan menjadi subrutin, menulis kode dengan prinsip sesuai guidelines dan best practices, dan membuat dokumen kode program, Mampu melakukan migrasi ke teknologi baru, debugging, dan menerapkan pemrograman paralel, Mampu melaksanakan pengujian kode program secara statis dan pengujian oleh pengguna (UAT), Mampu memberikan petunjuk teknis kepada pelanggan dan menganalisis dampak perubahan terhadap aplikasi serta menerapkan alert notification jika aplikasi bermasalah.

CAPAIAN PEMBELAJARAN LULUSAN

CPL Program Studi yang dibebankan pada Mata Kuliah	
S8	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri
P1	Mampu mengaplikasikan bidang keahliannya dan memanfaatkan IPTEKS pada bidangnya dalam penyelesaian masalah serta mampu beradaptasi terhadap situasi yang dihadapi.
KK3	Mampu menerapkan konsep dan teori algoritma dan pemograman untuk membangun dan mengembangkan aplikasi TIK
KU2	Mampu menunjukkan kinerja mandiri, bermutu, dan terukur
KU5	Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data.

Kontrak Perkuliahan

- Pertemuan 1 s.d 6 disampaikan dengan Metode Ceramah, Metode Diskusi dan Latihan Soal.
- Pertemuan 7 review materi dan Quiz
- Pertemuan 9 disampaikan dengan Metode Ceramah Metode diskusi dan latihan soal.
- Pertemuan 10 s.d 14 mahasiswa diharapkan dapat menjelaskan project program contoh kriptografi dalam bentuk presentasi kelompok.

Project Kriptografi (Nilai UTS dan UAS)

1. Membentuk kelompok. Satu kelompok 5 mahasiswa atau disesuaikan dengan jumlah mhs keseluruhan.
2. Project kriptografi berupa makalah dan program.
3. Hasil program dikumpulkan ke email dosen pengajar.
4. Presentasi project pertemuan 10-14

Outline makalah Kriptografi

LEMBAR JUDUL
KATA PENGANTAR
DAFTAR ISI

BAB I PENDAHULUAN
- 1.1. Latar Belakang Masalah
- 1.2. Identifikasi Permasalahan
- 1.3. Perumusan Masalah
- 1.4. Tujuan dan Manfaat
- 1.5. Metode Penelitian
- 1.6. Ruang Lingkup

BAB II LANDASAN TEORI
- 2.1. Tinjauan Pustaka
- 2.2. Penelitian Terkait

BAB III PEMBAHASAN
- 3.1. Analisis Kebutuhan
- 3.2. Rancangan Algoritma
- 3.3. Desain
- 3.4. *Software Architecture*
- 3.5. *User Interface*
- 3.6. *Code Generation*
- 3.7. *Testing*
- 3.8. *Support*
- 3.9. Spesifikasi *Hardware* dan *Software*

BAB IV PENUTUP
- 4.1 Kesimpulan
- 4.2 Saran

DAFTAR PUSTAKA
DAFTAR RIWAYAT HIDUP
LAMPIRAN

Penilaian akhir

Absen	: 20 %
Tugas	: 25 %
Project	: 55 %

PERTEMUAN 01

PENGENALAN KRIPTOGRAFI

Sub Pembahasan

1. Pengertian kriptografi
2. Terminologi
3. Sejarah Kriptografi
4. Kriptanalisis

Pengertian kriptografi

Kriptografi berasal dari bahasa Yunani yaitu crypto (rahasia) dan graphia (tulisan/writing).

Menurut terminologi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi

Secara etimologi kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan (Prayudi, 2005).

Awal mula kriptografi dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012), tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi (Diffie, 1976).

- Kriptografi berkembang sehingga ia tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain.
- Definisi baru Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan [Schneier, 1996].
- Pembuat sistem kriptografi disebut kriptografer (cryptographer).

Terminologi

- Pesan: data atau informasi yang bisa dibaca dan dimengerti maknanya.

  disebut plaintext atau cleartext
- Pesan dapat berupa: text, gambar, video, audio

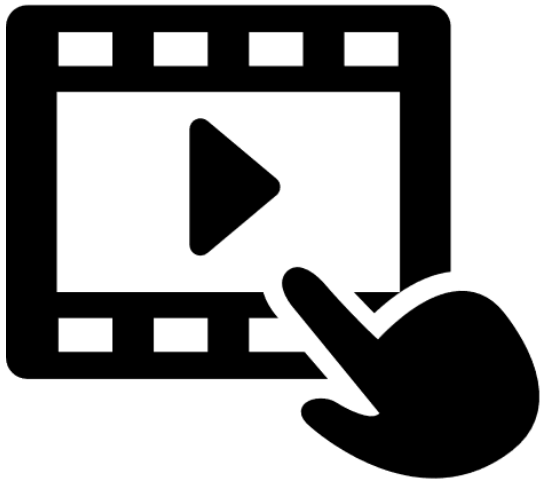
Pesan

1. Teks, contoh: “ Tidak ada balasan bagi kebaikan, selain kebaikan itu sendiri.”

2. Gambar→

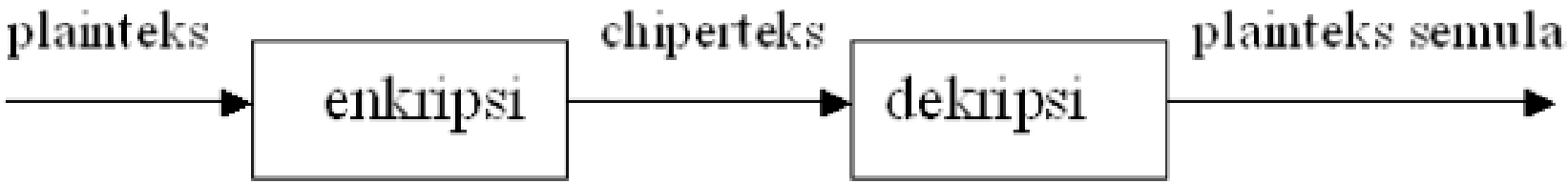
Pesan

3. Audio→ 

4. Video→ 

- Ciphertext / kriptogram : pesan yang telah disandikan sehingga terlihat tidak bermakna lagi.
- Tujuannya agar pesan tidak dapat dimengerti oleh pihak lain
- Ciphertext harus bisa diubah kembali menjadi plaintext

- Enkripsi (encryption): proses menyandikan plainteks menjadi ciphertek.
- Dekripsi (decryption): Proses mengembalikan cipherteks menjadi plainteksnya.



Gambar 1.1 Enkripsi dan dekripsi

- Pengirim (sender): pihak yang mengirim pesan
- Penerima (receiver): pihak yang menerima pesan
- Pengirim/penerima bisa berupa orang, komputer, terminal
- Pengirim ingin pesan dapat dikirim secara aman, yaitu pihak lain tidak dapat membaca isi pesan.

Penyadap (eavesdropper): orang yang mencoba menangkap pesan selama ditransmisikan.

Nama lain: enemy, adversary, intruder, interceptor, bad guy

Sejarah Kriptografi

- Sejarah penulisan rahasia tertua dapat ditemukan pada peradaban Mesir kuno, yakni tahun 3000 SM. Bangsa Mesir menggunakan ukiran rahasia yang disebut dengan *hieroglyphics*

Sumber: Amazine.co(2019)

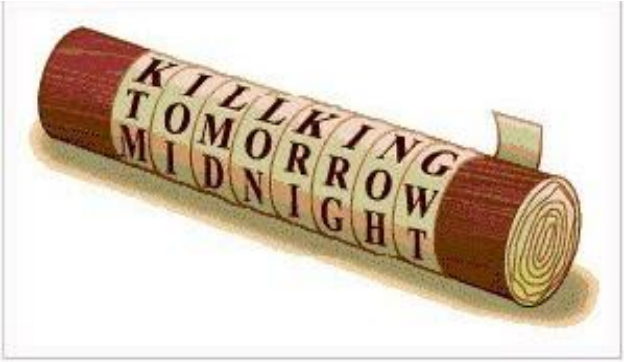
Pada zaman Romawi kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang dengan mengganti susunan alfabet dari:

a b c d e f g h i j k l m n o p q r s t u v w x y z.

Menjadi:

d e f g h i j k l m n o p q r s t u v w x y z a b c

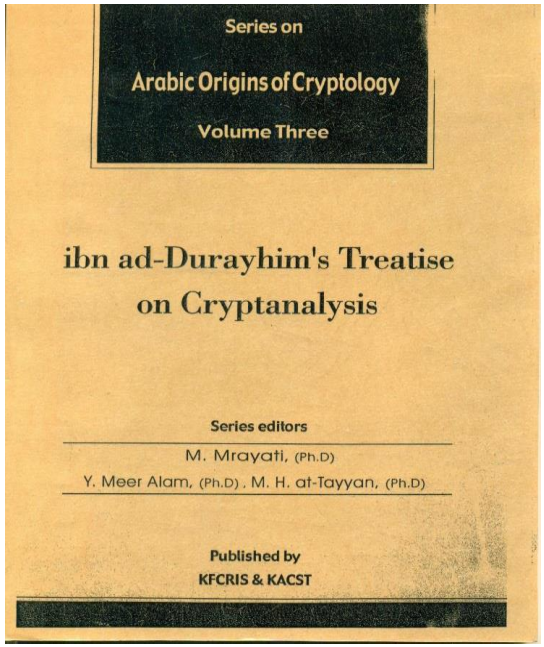
- Awal tahun 400 SM bangsa Spartan di Yunani memanfaatkan kriptografi di bidang militer dengan menggunakan alat yang disebut *scytale*, yakni pita panjang berbahan daun papyrus yang dibaca dengan cara digulungkan ke sebatang silinder



Sumber: ilmu-kriptografi (2019)

Sejarah kriptografi bangsa Arab dapat dibaca pada seri buku Arabic Origins of Cryptology, yang diterbitkan oleh King Faisal Center for Research and Islamic Studies, Arab Saudi

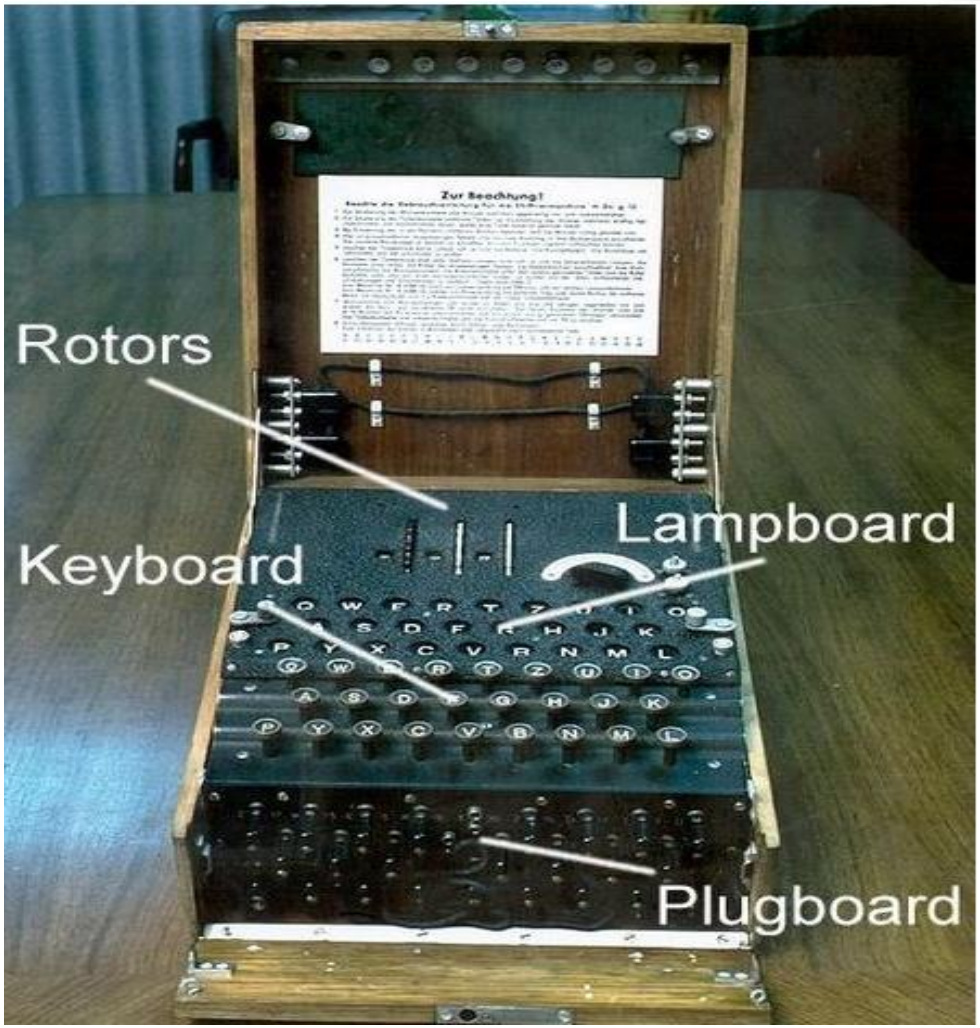
- Seri pertama menyajikan manuskrip kuno tentang kriptanalisis yang ditulis oleh Al-Kindi
- Seri kedua tentang risalah Ibn Adlan yang berisi manual kriptanalisi yang ditulis abad ke 13
- Seri ketiga adalah risalah Ibn Ad-Durayhim



- Pada abad ke 17, sejarah kriptografi mencatat korban di Inggris
- Queen Mary of Scotland, dipancung setelah pesan rahasianya dari balik penjara pada abad pertengahan berhasil dipecahkan oleh Thomas Phelippes, seorang pemecah kode
- Isi pesan terenskripsi adalah rencana membunuh ratu

- Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan Enigma.
- Enigma cipher berhasil dipecahkan oleh pihak Sekutu.
- Keberhasilan memecahkan Enigma sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2

Mesin anigma beserta bagian-bagiannya.



Sumber: wikipedia

Empat kelompok orang yang menggunakan dan berkontribusi pada kriptografi adalah:

1. Militer (intelijen dan mata-mata)
2. Korp diplomatik
3. Diarist
4. Lovers

Kriptanalisis

- Sejarah kriptografi paralel dengan sejarah kriptanalisis (cryptanalysis), yaitu bidang ilmu dan seni untuk memecahkan cipherteks
- Teknik kriptanalisis sudah ada sejak abad ke-9.

Kriptanalisis

- Dikemukakan pertama kali oleh seorang ilmuwan Arab pada Abad IX bernama Abu Yusuf Yaqub Ibnu Ishaq Ibnu As-Sabbah Ibnu 'Omran Ibnu Ismail Al-Kindi, atau yang lebih dikenal sebagai Al-Kindi.

Portrait of Al-Kindi

Sumber: wikipedia

- Al-Kindi menulis buku tentang seni memecahkan kode, buku yang berjudul ‘Risalah fi Istikhraj al-Mu'amma (Manuscript for the Deciphering Cryptographic Messages)
- Al-Kindi menemukan frekuensi perulangan huruf di dalam Al-Quran. Teknik yang digunakan Al-Kindi kelak dinamakan analisis frekuensi.
- Yaitu teknik untuk memecahkan cipherteks berdasarkan frekuensi kemunculan karakter di dalam pesan

The first page of al-Kindi's manuscript "On Deciphering Cryptographic Messages", containing the oldest known description of cryptanalysis by frequency analysis.

Sumber: wikipedia

Sumber Referensi

- https://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html
- https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/
- https://slideplayer.info/slide/2482842/
- https://en.wikipedia.org/wiki/Al-Kindi
- https://www.komputerdia.com/2017/10/pengertian-kriptografi-sejarah-dan-jenis-kriptografi.html

PERTEMUAN 02

SERANGAN TERHADAP KRIPTOGRAFI

Sub Pembahasan

1. Kriptanalis
2. Tujuan Kriptografi
3. Serangan Kriptografi
4. Kompleksitas Serangan

Kriptanalisis dan kriptologi

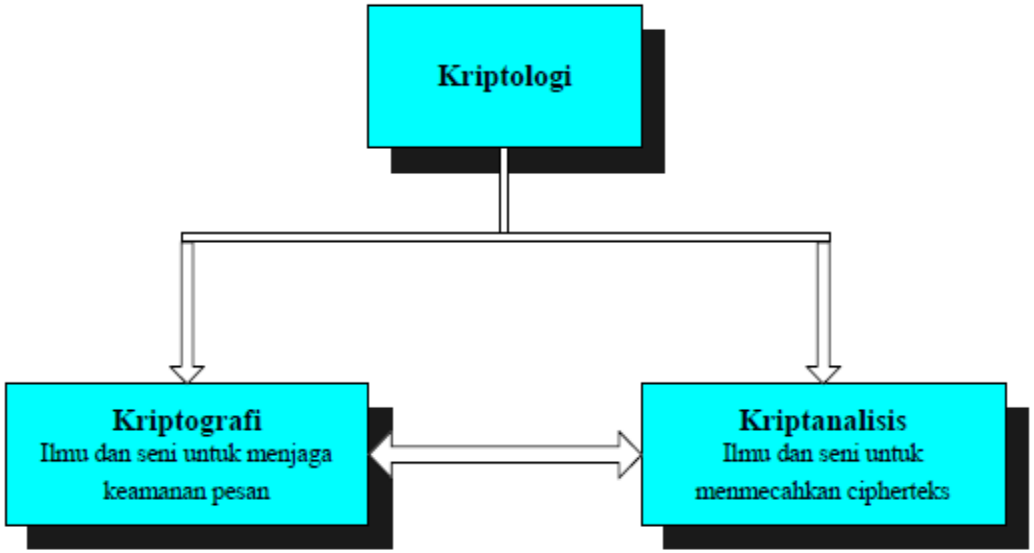
Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis.

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis.

Jika seorang kriptografer (cryptographer) mentransformasikan plainteks menjadi cipherteks dengan suatu algoritma dan kunci maka sebaliknya

seorang kriptanalis berusaha untuk memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci.

Kriptologi (cryptology) adalah studi mengenai kriptografi dan kriptanalisis. Baik kriptografi maupun kriptanalisis keduanya saling berkaitan, dapat dilihat seperti gambar dibawah ini :



Sumber: Renaldi Munir

Tujuan Kriptografi:

Tujuan kriptografi adalah memberikan layanan keamanan. Aspek keamanan sebagai berikut:

1. Kerahasiaan (confidentiality)

Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya

Tujuan kriptografi:

2. Integritas data(data integrity)

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

“Apakah pesan yang diterima masih asli atau tidak mengalami perubahan(modifikasi)?”.

Tujuan kriptografi:

3. Otentikasi (authentication)

Layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*).

“Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?”

Tujuan kriptografi:

4. Nirpenyangkalan (non-repudiation)

Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Serangan terhadap kriptografi:

Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu:

A. **Serangan pasif (passive attack)**

Pada serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuannya adalah untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis.

Beberapa metode penyadapannya antara lain:

1. Wiretapping: penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.
2. Electromagnetic eavesdropping: penyadap mencegat data yang ditrasmisikan melalui saluran wireless, misalnya radio dan microwave.
3. Acoustic eavesdropping : menangkap gelombang suara yang dihasilkan oleh suara manusia.

Serangan terhadap kriptografi:

B. **Serangan Aktif (Active attack)**

Pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya.

Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-replay pesan lama, mengubah informasi yang tersimpan, dan sebagainya.

Serangan terhadap kriptografi:

Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:

1. Ciphertext-only

Adalah jenis serangan yang paling umum namun paling sulit, karena informasi yang tersedia hanyalah cipherteks saja. Kriptanalis memiliki beberapa cipherteks dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama.

2. Known-plaintext
Adalah jenis serangan dimana kriptanalis memiliki pasangan plainteks dan cipherteks yang berkoresponden.

3. Chosen-plaintext
Serangan jenis ini lebih hebat dari pada known-plaintext attack, karena kriptanalis dapat memilih plainteks yang dimilikinya untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

4. Chosen-ciphertext attack

Adalah jenis serangan dimana kriptanalis memilihcipherteks untuk didekripsikan dan memiliki akses ke plainteks hasil dekripsi.

5. Chosen-text

Adalah jenis serangan yang merupakan kombinasi chosen-plaintext attack dan chosen-chiphertext attack.

Serangan terhadap kriptografi:

Berdasarkan teknik yang digunakan dalam menemukan kunci, maka serangan dapat dibagi menjadi 4, yaitu:

1. Exhaustive attack atau brute force attack

Adalah serangan untuk mengungkap plainteks atau kunci dengan menggunakan semua kemungkinan kunci.

Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Selain itu kriptanalis memiliki sejumlah cipherteks dan plainteks yang bersesuaian.

2. Analytical attack

Pada jenis serangan ini, kriptanalis tidak mencoba-coba semua kemungkinan kunci tetapi menganalisis kelemahan algoirtma kriptografi untuk mengurangi kemungkinan kunci yang tidak ada.

Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Analisis dapat menggunakan pendekatan matematik dan statistik dalam rangka menemukan kunci.

3. Related-key attack

Kriptanalis memiliki cipherteks yang dienkripsi dengan dua kunci berbeda.
Kriptanalis tidak mengetahui kedua kunci tersebut namun ia mengetahui hubungan antara kedua kunci, misalnya mengetahui kedua kunci hanya berbeda 1 bit

4. Rubber-hose cryptanalysis

Ini mungkin jenis serangan yang paling ekstrim dan paling efektif.
Penyerang mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan.

Kompleksitas serangan

Kompleksitas serangan dapat diukur dengan beberapa cara, yaitu :

1. Kompleksitas data (data complexity)

Jumlah data (plainteks dan cipherteks) yang dibutuhkan sebagai masukan untuk serangan. Semakin banyak data yang dibutuhkan untuk melakukan serangan, semakin kompleks serangan tersebut, yang berarti semakin bagus sistem kriptografi tersebut.

2. Kompleksitas waktu (time complexity)

Waktu yang dibutuhkan untuk melakukan serangan. Semakin lama waktu yang dibutuhkn untuk melakukan serangan, berarti semakin bagus kriptografi tersebut

3. Kompleksitas ruang memori (space/storage complexity)

Jumlah memori yang dibutuhkan untuk melakukan serangan. Semakin banyak memori yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut.

Daftar Pustaka

- http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-003.pdf

PERTEMUAN 03

ALGORITMA KRIPTOGRAFI KLASIK

Sub Pembahasan

1. Algoritma
2. Ciri-Ciri
3. Alasan
4. Jenis-Jenis Kriptografi Klasik

Algoritma Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan menggunakan pensil dan kertas.

Algoritma kriptografi (cipher) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan.

Semua algoritma klasik termasuk ke dalam sistem kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan.

Kriptografi klasik memiliki beberapa ciri:

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada computer
3. Termasuk ke dalam kriptografi kunci simetris

Tiga alasan mempelajari algoritma klasik:

1. Memahami konsep dasar kriptografi
2. Dasar algoritma kriptografi modern
3. Memahami kelemahan sistem kode.

(Ariyus, Dony. 2008)

Algoritma kriptografi klasik

Algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu :

1. Cipher substitusi (substitution cipher)

Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu “unit” disini berarti satu huruf, pasangan huruf, atau dikelompokkan lebih dari dua huruf.

Algoritma substitusi tertua yang diketahui adalah Caesar cipher yang digunakan oleh kaisar Romawi , Julius Caesar (sehingga dinamakan juga casear cipher), untuk mengirimakan pesan yang dikirimkan kepada gubernurnya.

2. Cipher transposisi (transposition cipher)

Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah.

Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks.

Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.(Munir.2006)

Jenis-Jenis Cipher Substitusi

- Cipher substitusi abjad-tunggal (Monoalphabetic Cipher)
- Cipher Substitusi Homofonik (Homophonic Substitution Cipher)
- Cipher Substitusi Abjad-Majemuk (Polyalphabetic Substitution Cipher)
- Cipher Substitusi Poligram (Polygram Substitution Cipher)

Cipher substitusi abjad-tunggal

(Monoalphabetic Cipher)

Jenis cipher substitusi ini sering juga disebut cipher substitusi sederhana.

Ide cipher substitusi abjad-tunggal adalah menggantikan satu karakter pada plainteks menjadi satu karakter pada cipherteks dengan aturan tertentu.

Fungsi ciphering-nya merupakan fungsi satu ke satu. (mengganti setiap huruf pada plainteks dengan huruf yang bersesuaian).

Pada metode ini string kunci menjadi huruf-huruf awal subtitusi dari plaintext. Setiap huruf dalam kunci hanya diperkenankan muncul sekali.

Berikut contoh penggunaan monoalphabetic chiper.

Contoh kunci: PASSWORD RAHASIAKU

Dikarenakan setiap huruf dalam kunci hanya diperkenan muncul sekali, kunci tersebut kita sederhanakan menjadi: PASWORDHIKU

Plain alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	A	S	W	O	R	D	H	I	K	U	B	C	E	F	G	J	L	M	N	Q	T	V	W	X	Y

Cipher alphabet

Contoh:

Plain text : Ku titipkan rindu pada langit yg kau tatap

Cipher text: Uq ninigupe liewq gpwp bpedin xd upq npnpg

Jenis-Jenis Kriptografi Klasik

1. Vigènere cipher
2. Autokey Cipher
3. Reverse Cipher
4. Zig-Zag Cipher
5. Segitiga Cipher
6. Super Enkripsi
7. Enigma Machine

Vigènere cipher

Vigenere cipher mungkin adalah contoh terbaik dari cipher alphabet-majemuk ‘manual’.

Algoritma ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) perancis, Blaise de Vigènere pada abad 16.

Vigènere cipher dipublikasikan pada tahun 1586. Cipher ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. Vigènere cipher digunakan oleh tentara Konfiderasi (Confederate Army) pada perang sipil Amerika (American Civil war).

Vigènere cipher sangat dikenal karena mudah dipahami dan diimplementasikan. Cipher menggunakan bujursangkar Vigènere untuk melakukan enkripsi. Kolom paling kiri dari bujursangkar menyatakan huruf-hurf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris dalam bujursangkar menyatakan huruf-huruf cipherteks, yang mana jumlah pergesaran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, A = 0, B = 1, C = 2,…, Z = 25).

- Bujursangkar vigènere digunakan untuk memperoleh cipherteks dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari pada panjang plainteks, maka kunci diulang penggunaanya (sistem periodik). Bila panjang kunci adalah m, maka periodenya dikatakan m.
- Contoh, plainteks: PENJAGA HATI
- Kunci adalah smile
- maka penggunaan kunci secara periodik adalah sebagai berikut:

- Plainteks : PENJAGA HATI
- Kunci : SMILESM ILES
- Cipherteks: HQVEYM OLXA

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Autokey Cipher

Kriptografi Autokey adalah pengembangan dari kriptografi Caesar dan Vigenere.

Cara melakukan enkripsi sama seperti kedua kriptografi sebelumnya.

Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi.

Rumus yang berlaku untuk kriptografi Autokey sama seperti Caesar dan Vigenere.

Contoh

Plaintext: INI PESAN RAHASIA

Kunci: BESOK

Maka kata BESOK akan disisipkan di depan plaintext INI PESAN RAHASIA.

Kemudian enkripsi dilakukan sama dengan enkripsi Caesar dan Vigenere.

Reverse Cipher

- Adalah contoh kriptografi klasik yang menggunakan substitusi yaitu mengganti satu huruf dengan huruf lain ataupun mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Ini contoh yang paling sederhana dari transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Contoh Kriptografi Reverse:
- Plaintext : KU TITIP RINDU PADA HUJAN
- Ciphertext : UK PITIT UDNIR ADAP NAJUH

Pada kriptografi kolom (column cipher), plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam kelompok ini dituliskan kembali kolom per kolom, dengan urutan kolom yang bisa berubah-ubah.

- Contoh Kriptografi Kolom:
- Kalimat ‘ AYAH SUDAH TIBA KEMARIN SORE ’, jika disusun dalam kolom 7 huruf, maka akan menjadi kolom - kolom berikut :

AYAHSUD
AHTIBAK
EMARINS
OREAAAA

- Untuk melengkapi kolom terakhir agar berisi 7 huruf, maka sisanya diisi dengan huruf ‘A’atau bisa huruf apa saja sebagai huruf pelengkap. Kalimat tesebut setelah dienkripsi dengan 7 kolom huruf dan urutan kunci 6725431, maka hasil enkripsinya:
- DKSAATAEUANASBIAHIRAAAEOYHMR

Zig-Zag Cipher

- Pada kriptografi kolom zig-zag, plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam uruta kolom yang dimasukkan secara pola zig-zag.

Segitiga Cipher

- Pada kriptografi kolom Triangle, plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam urutan kolom yang dimasukkan secara pola segitiga.

Super Enkripsi

- Kombinasi Antara Cipher Substitusi (Caesar Cipher) dan Cipher Tranposisi (Column Cipher). Sehingga memperoleh Cipher yang lebih kuat (Super) dari pada Satu Cipher saja.

Daftar Pustaka

- https://www.alfianaramadhani.web.id/2016/10/kriptografi-2-pertemuan-4.html
- https://asyafaat.files.wordpress.com/2009/05/achmadsyafaat-perbandingan_kriptografi_cipher_substitusi_homofonikpoligram_dg_caesar-cipher.pdf

TUGAS INDIVIDU

Membuat contoh kriptografi klasik

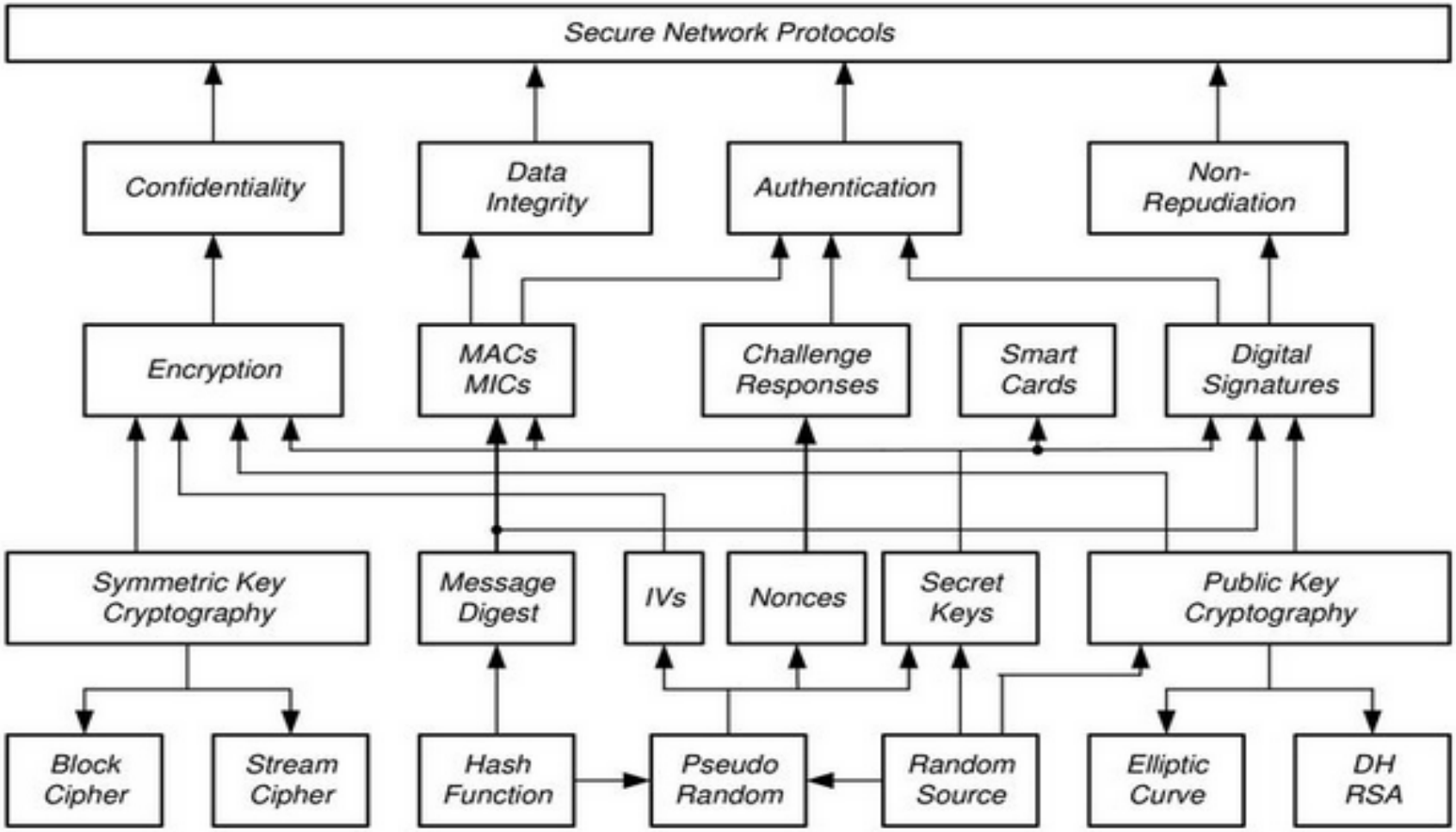
PERTEMUAN 04

ALGORITMA KRIPTOGRAFI MODERN

Sub Pembahasan

- Rangkaian Bit dan Operasinya
- Cipher Aliran
- Pembangkit Aliran-Kunci (Keystream Generator)
- Linear Feedback Shift Register (LFSR)
- Serangan Terhadap Cipher Aliran
- Cipher Blok
- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

Blok Kriptografi Modern



Rinaldi Munir

- ✓ Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit memecahkan cipherteks tanpa mengetahui kunci.
- ✓ Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter (algoritma kriptografi klasik).
- ✓ Kunci, plaintext maupun ciphertext dinyatakan dalam rangkaian bit binner, 0 dan 1.

- ✓ Algoritma enkripsi dan deskripsi memproses semua data dan informasi dalam bentuk mode bit.
- ✓ Rangkaian bit yang menyatakan plaintext di enkripsi menjadi ciphertext dalam bentuk rangkaian bit, demikian sebaliknya
- ✓ Operasi bit **XOR** paling banyak digunakan

Enkripsi modern sudah menggunakan komputer untuk pengoperasiannya, berfungsi untuk mengamankan data baik yang ditransfer melalui jaringan komputer maupun yang bukan.

Hal ini sangat berguna untuk melindungi *privacy*, *data integrity, authentication,* dan *non-repudiation.* Perkembangan algoritma kriptografi modern berbasis bit didorong oleh penggunaan komputer digital yang merepresentasikan data dalam bentuk biner.

Algoritma Kriptografi Modern

1. Algoritma Simetris

- ✓ Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan deskripsinya.
- ✓ Algoritma kriptografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal atau algoritma satu kunci dan megharuskan pengirim dan penerima menyetujui suatu kunci tersebut.

- ✓ Kelebihan dari kriptografi simetris waktu proses untuk enkripsi dan deskripsi relatif cepat.
- ✓ Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci.
- ✓ Proses relative cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara *real time* seperti GSM.

Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma dibawah ini :

- Data Encryption Standar (DES)
- Advance Encryption Standar (AES)
- International Data Encryption Algoritma
- A5
- RC4

Algoritma Kriptografi Modern

2. Algoritma Asimetris

- ✓ Adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi deskripsi.
- ✓ Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki kunci rahasia, untuk melakukan pembongkaran terhadap kode yang dikirim untuknya.
- ✓ Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (merupakan singkatan dari nama penemunya, yaitu Rivest, Shamir dan Adleman).

3. Algoritma Hibrida

Adalah algoritma yang memanfaatkan dua tingkatan kunci, yaitu kunci rahasia (simetri) yang disebut juga session key (kunci sesi) untuk enkripsi data dan pasangan kunci rahasia adalah kunci publik untuk pemberian tanda tangan digital serta melindungi kunci simetris.

Rangkaian Bit dan Operasinya

- ✓ Pesan dalam bentuk rangkaian bit dipecah menjadi beberapa blok
- ✓ Contoh plainteks: 100111010110
- ✓ Dibagi blok bit yang panjangnya 4 menjadi

  1001 1101 0110
- ✓ Setiap blok menyatakan bilangan bulat dari 0 sampai 15, yaitu

  9 13 6

- Bila *plainteks* dibagi menjadi blok-blok yang berukuran 3 bit, maka rangkaian bit di atas menjadi:

  100 111 010 110

- Setiap blok menyatakan bilangan bulat dari 0 sampai 7, yaitu

  4 7 2 6

- *Padding bits:* Bit-bit tambahan jika ukuran blok terakhir tidak mencukupi panjang blok.
- Panjang rangkaian bit tidak habis dibagi dengan ukuran blok yang ditetapkan, maka blok yang terakhir ditambah dengan bit-bit semu.
- *Padding bits* dapat mengakibatkan ukuran plainteks hasil dekripsi lebih besar daripada ukuran plainteks semula.
- Misalnya rangkaian bit diatas dibagi blok 5-bit menjadi

10011 10101 **000**10

Representasi Dalam Hexadesimal

- Cara lain untuk menyatakan rangkaian bit adalah dengan notasi heksadesimal (HEX).
- Rangkaian bit dibagi menjadi blok yang berukuran 4 bit dengan representasi dalam HEX:

0000 = 0	0001 = 1	0010 = 2	0011 = 3
0100 = 4	0101 = 5	0011 = 6	0111 = 7
1000 = 8	1011 = 9	1010 = A	1011 = B
1100 = C	1101 = D	1101 = E	1111 = F

- Contoh plainteks: 100111010110 dibagi menjadi blok 4 bit:

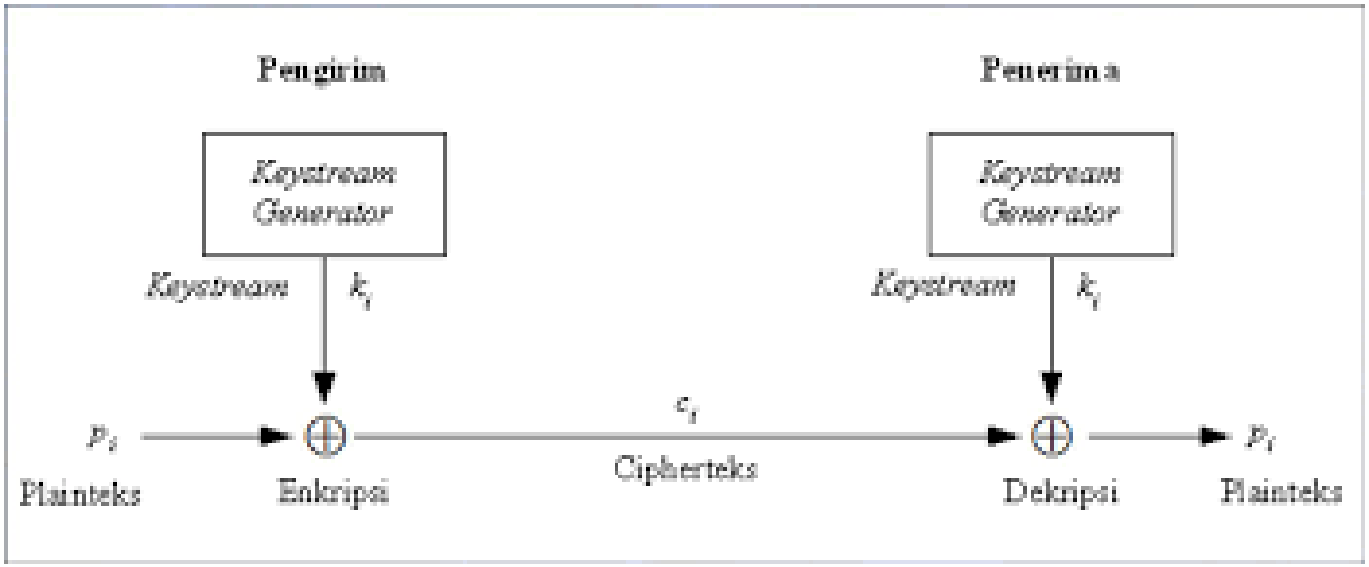
  1001 1101 0110
- Notasi HEX adalah 9 D 6

Kategori Algoritma (*cipher*) Berbasis Bit

1. ***Cipher* Alir (*Stream Cipher*)**
   - ✓Beroperasi pada bit tunggal
   - ✓Penkripsi/dekripsi bit per bit atau byte per byte
2. ***Cipher* Blok (*Block Cipher*)**
   - ✓ Beroperasi pada blok bit
     (contoh: 64-bit/blok = 8 karakter/blok)
   - ✓ Enkripsi/dekripsi blok per blok

1. Cipher Aliran (*Stream Cipher*)

- Mengenkripsi plainteks menjadi chiperteks bit per bit.
- Diperkenalkan oleh Vernam melalui algoritmanya, **Vernam *Cipher***
- Vernam *cipher* diadopsi dari *one-time pad cipher*, yang dalam hal ini karakter diganti dengan bit (0 atau 1).



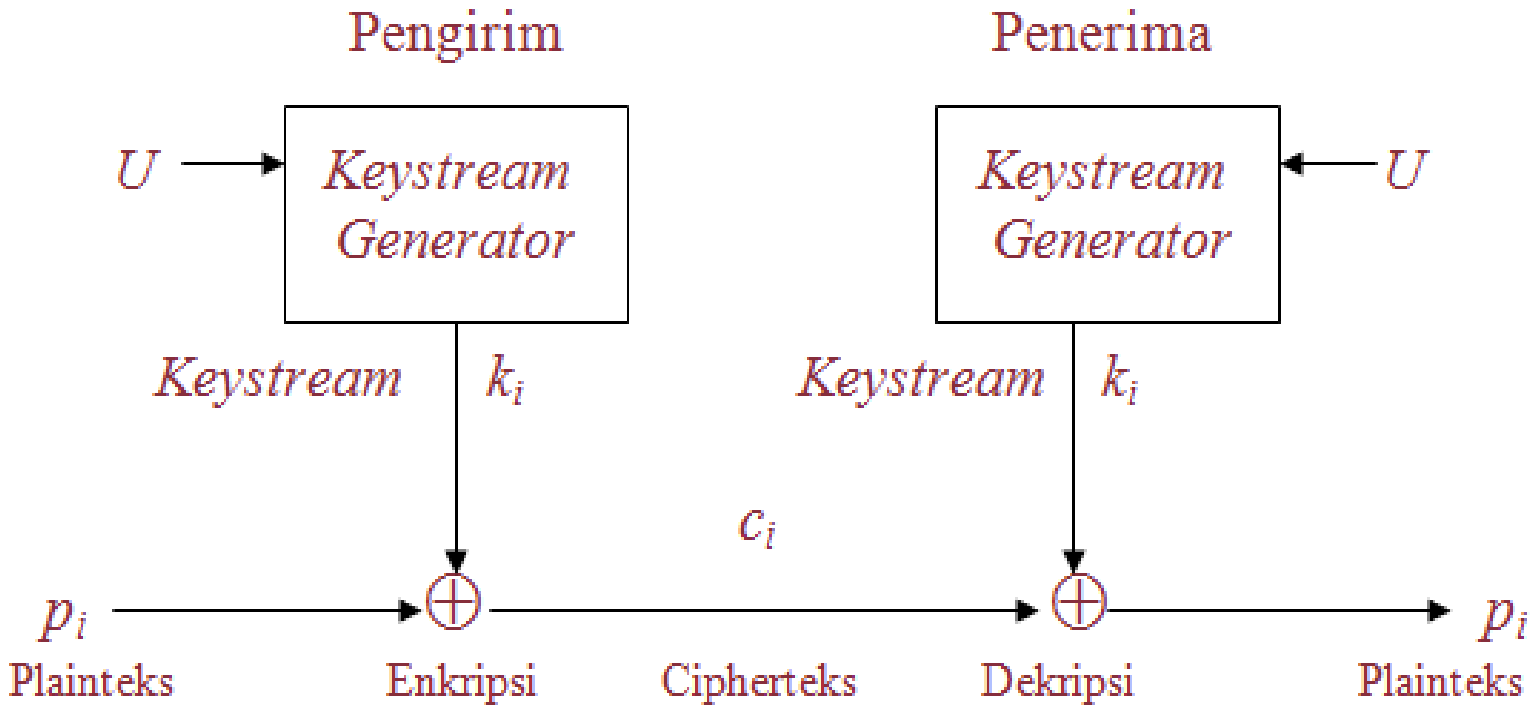
Konsep Cipher Alir

- ✓ Bit-bit kunci untuk enkripsi/dekripsi disebut *keystream.*
- ✓ Keystream dibangkitkan oleh *keystream generator.*

Keystream Generator

- *Keystream generator* diimplementasikan sebagai prosedur yang sama disisi pengirim dan penerima pesan.
- *Keystream generator* dapat membangkitkan *keystream* berbasis bit per bit atau dalam bentuk blok-blok bit.
- Jika *keystream* berbentuk blok-blok bit, *cipher* blok dapat digunakan untuk memperoleh *cipher* aliran.

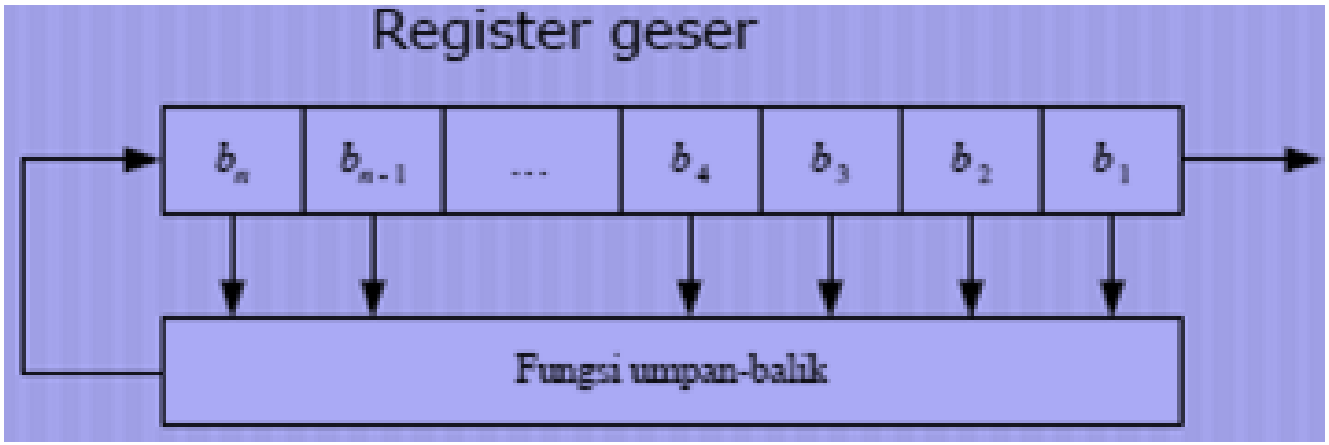
- Prosedur menerima masukan sebuah kunci *U*. Keluaran dari prosedur merupakan fungsi dari *U.*
- Pengirim dan penerima harus memiliki kunci *U* yang sama. Kunci *U* ini harus dijaga kerahasiaanya.
- Pembangkit harus menghasilkan bit-bit kunci yang kuat secara kriptografi.



Cipher aliran dengan pembangkit bit-aliran-kunci yang bergantung pada kunci *U* (Rinaldi Munir)

Linear Feedback Shift Register (LFSR)

- *FSR* adalah contoh sebuah *keystream generator*.
- *FSR* terdiri dari dua bagian: register geser (n bit) dan fungsi umpan balik



Sumber: Rinaldi Munir

Serangan pada Cipher Aliran

1. Known-plaintext attack

   Kriptanalis memiliki potongan plainteks(P) dan cipherteks(C) yang berkoresponden. Sehingga ia dapat menemukan bagian aliran kunci(K) dengan meng-XOR-kan bit-bit plainteks & cipherteks.

Serangan pada Cipher Aliran

2. Ciphertext-only attack

Serangan ini terjadi jika keystream yang sama digunakan dua kali terhadap potongan plainteks yang berbeda. Serangan semacam ini disebut juga keystream reuse attack.

Contoh: Kriptanalis memiliki dua potongan cipherteks berbeda (C1 dan C2) yang dienkripsi dengan bit-bit kunci yang sama. Ia meng-XOR-kan kedua cipherteks tersebut dan memperoleh dua buah plainteks yang ter-XOR-kan satu sama lain.

Serangan pada Cipher Aliran

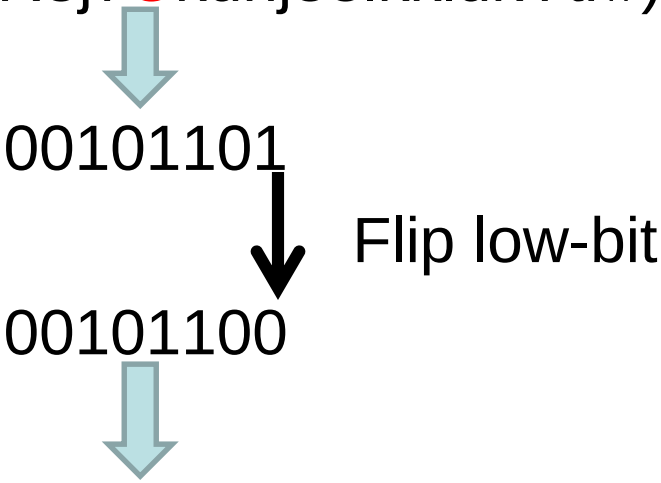
3. Flip Bit Attack
Tujuan: mengubah bit cipherteks tertentu sehingga hasil dekripsinya berubah.
Pengubahan dilakukan dengan membalikkan (*flip*) bit tertentu (0 menjadi 1, atau 1 menjadi 0).

Contoh:
Seseorang mentransfer uang antar-rekening bank dengan jumlah 10 USD

Contoh:

P : QT-TRNSFR US $00010,00 FRM ACCNT 123-67 TO

C: uhtr07hjLmkyR3j7**U**kdhj38lkkldkYtr#)oknTkRgh



C: uhtr07hjLmkyR3j7**T**kdhj38lkkldkYtr#)oknTkRgh

P : QT-TRNSFR US $10010,00 FRM ACCNT 123-67 TO

Pengubahan 1 bit U dari cipherteks sehingga menjadi T.
Hasil dekripsi: $10,00 menjadi $ 10010,00

- Pengubah pesan tidak perlu mengetahui kunci, ia hanya perlu mengetahui posisi pesan yang diminati saja.
- Serangan semacam ini memanfaatkan karakteristik *cipher* aliran yang sudah disebutkan di atas, bahwa kesalahan 1-bit pada cipherteks hanya menghasilkan kesalahan 1-bit pada plainteks hasil dekripsi.

Aplikasi Cipher Aliran

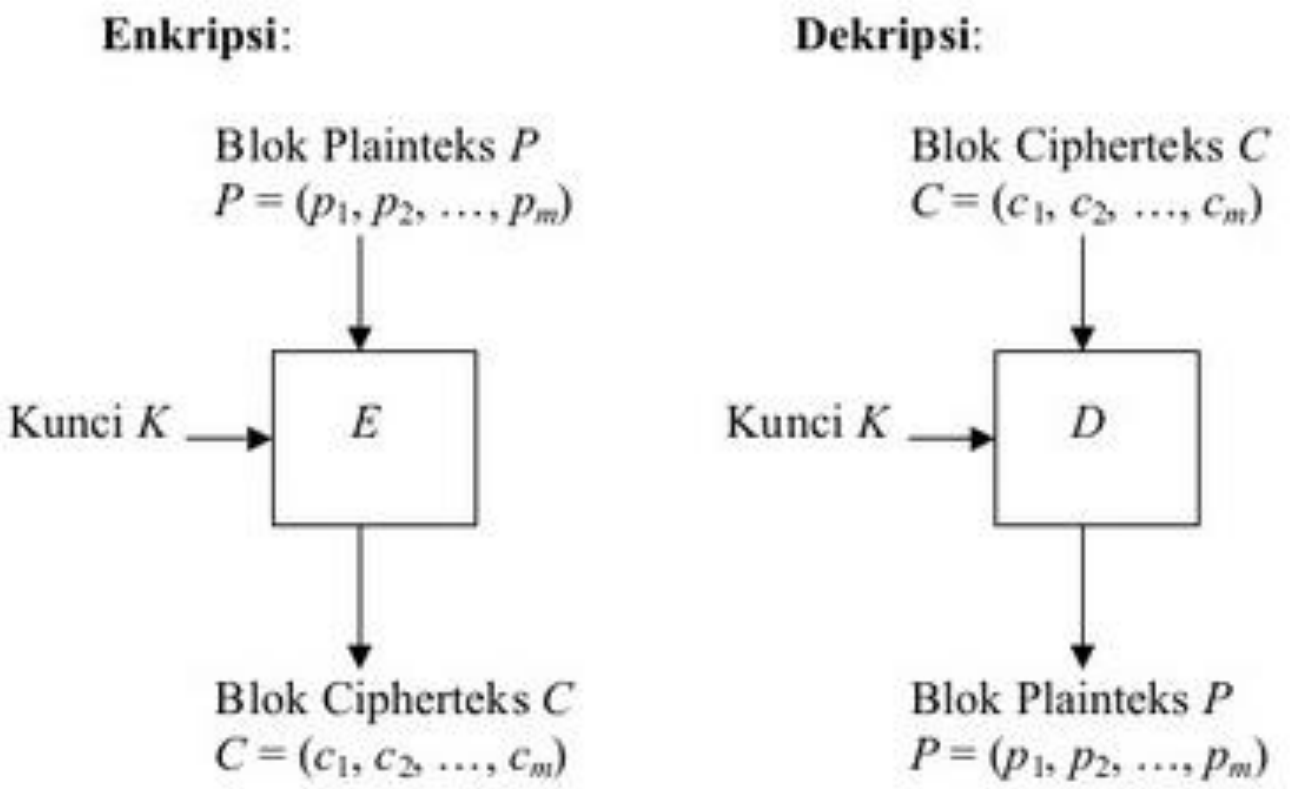
- *Cipher* aliran cocok untuk mengenkripsikan aliran data yang terus menerus melalui saluran komunikasi.
- Jika bit cipherteks yang diterima mengandung kesalahan, maka hal ini hanya menghasilkan satu bit kesalahan pada waktu dekripsi, karena tiap bit plainteks ditentukan hanya oleh satu bit cipherteks.

Contoh:

1. Mengenkripsikan data pada saluran yang menghubungkan antara dua buah komputer.
2. Mengenkripsikan suara pada jaringan telepon *mobile* GSM

2. Cipher Blok (*Block Cipher*)

- Bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama.
- Panjang kunci enkripsi = panjang blok
- Enkripsi dilakukan terhadap blok bit plainteks menggunakan bit-bit kunci
- Algoritma enkripsi menghasilkan blok cipherteks yang panjangnya sama dengan blok plainteks.



Skema enkripsi dan dekripsi pada cipher blok (Rinaldi Munir)

Mode Operasi Cipher Blok

- Mode operasi: berkaitan dengan cara blok dioperasikan
- Ada 5 mode operasi *cipher* blok:
  1. Electronic Code Book(ECB)
  2. Cipher Block Chaining(CBC)
  3. Cipher Feedback(CFB)
  4. *Output Feedback (OFB)*
  5. *Mode counter*

Electronic Code Book (ECB)

- Setiap blok plainteks *Pi* dienkripsi secara individual dan independen menjadi blok cipherteks *Ci*.
- Pada mode ECB, blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama.
- Contoh jika blok 1010 muncul dua kali maka selalu dienkripsi menjadi 0010.

Keuntungan Mode ECB

1. Tiap blok plainteks dienkripsi secara independen.
2. Kesalahan satu atau lebih bit pada blok cipherteks hanya mempengaruhi cipherteks yang bersangkutan pada waktu dekripsi.

Blok-blok cipherteks lainnya bila didekripsi tidak terpengaruh oleh kesalahan bit cipherteks tersebut.

Kelemahan ECB

1. Karena bagian plainteks sering berulang dan terdapat blok-blok plainteks yang sama, maka hasil enkripsinya menghasilkan blok cipherteks yang sama, sehingga mudah diserang secara statistik.
2. Pihak lawan dapat memanipulasi cipherteks untuk “membodohi” atau mengelabui penerima pesan.

Cipher Block Chaining(CBC)

- Tujuan: membuat ketergantungan antar blok.
- Setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.
- Hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current*.

Keuntungan Mode CBC

- Karena blok-blok plainteks yang sama tidak menghasilkan blok-blok cipherteks yang sama, maka kriptanalisis menjadi lebih sulit.
- Inilah alasan utama penggunaan mode *CBC* digunakan.

Kelemahan Mode CBC

1. Kesalahan satu bit pada sebuah blok plainteks akan merambat pada blok cipherteks yang berkoresponden dan semua blok cipherteks berikutnya.
2. Tetapi, hal ini berkebalikan pada proses dekripsi. Kesalahan satu bit pada blok cipherteks hanya mempengaruhi blok plainteks yang berkoresponden dan satu bit pada blok plainteks berikutnya (pada posisi bit yang berkoresponden pula).

Cipher-Feedback (CFB)

- Mengatasi kelemahan pada mode *CBC* jika diterapkan pada komunikasi data (ukuran blok yang belum lengkap)
- Data dienkripsikan dalam unit yang lebih kecil daripada ukuran blok.
- Unit yang dienkripsikan dapat berupa bit per bit (jadi seperti *cipher*aliran), 2 bit, 3-bit, dan seterusnya.
- Bila unit yang dienkripsikan satu karakter setiap kalinya, maka mode *CFB*-nya disebut *CFB* 8-bit.

- *CFB n*-bit mengenkripsi plainteks sebanyak *n*-bit setiap kalinya, n ≤ *m* (*m* = ukuran blok).
- Dengan kata lain, *CFB* mengenkripsikan *cipher* blok seperti pada *cipher* aliran.
- Mode *CFB* membutuhkan sebuah antrian (*queue*) yang berukuran sama dengan ukuran blok masukan.

Output-Feedback (OFB)

- Mode *OFB* mirip dengan mode *CFB*, kecuali *n*-bit dari hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan diantrian.
- Dekripsi dilakukan sebagai kebalikan dari proses enkripsi.

- Kesalahan1-bit pada blok plainteks hanya mempengaruhi blok cipherteks yang berkoresponden saja
- Begitu pula pada proses dekripsi, kesalahan1-bit pada blok cipherteks hanya mempengaruhi blok plainteks yang bersangkutan saja.

- Karakteristik kesalahan semacam ini cocok untuk transmisi analog yang di-digitisasi, seperti suara atau video, yang dalam hal ini kesalahan 1-bit dapat ditolerir, tetapi penjalaran kesalahan tidak dibolehkan.

Daftar Pustaka

- http://news.purcode.net/2018/12/macam-macam-kriptografi-modern.html
- https://www.academia.edu/22371107/Algoritma_Kriptografi_Modern
- Rinaldi Munir, Algoritma Kriptografi Modern, 2018
- http://dinus.ac.id/repository/docs/ajar/Kriptografi_-_Week7_-_Sream_Cipher.pdf
- https://www.slideshare.net/triyulianto182/13algoritma-kriptografi-modern-bagian-2
- https://www.slideshare.net/KuliahKita/kriptografi-prinsip-perancangan-cipher-blok
- http://dinus.ac.id/repository/docs/ajar/Sessi_05.pdf

PERTEMUAN 05

ALGORITMA KUNCI PUBLIK

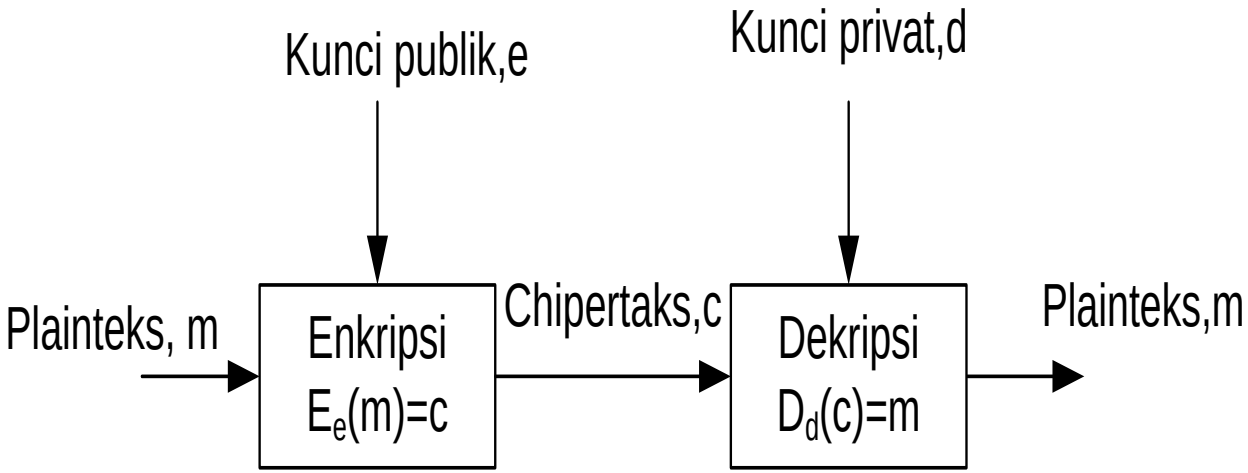
Sub Pembahasan

- ✓ **Konsep kriptografi Kunci Publik**
- ✓ **Perbandingan Kriptografi Kunci Simetri dengan Kriptografi Kunci Publik**
- ✓ **Aplikasi Kriptografi Kunci Publik**
- ✓ **RSA**
- ✓ **ElGamal**
- ✓ **Algoritma Pertukaran Kunci Diffie-Hellman**
- ✓ **Algoritma Knapsack**

- Kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi, dan satu kunci untuk deskripsi
- Kunci untuk enkripsi disebut dengan kunci publik, disimbolkan dengan ***e***
- Kunci untuk dekripsi disebut dengan kunci privat, disimbolkan dengan ***d***
- Karena kunci enkripsi tidak sama dengan kunci deskripsi, maka sering disebut sistem kriptografi asimetri (Kunci publik)

Konsep Kriptografi Kunci Publik

- Konsep kriptografi kunci publik sederhana akan tetapi mempunyai konsekuensi pengunaan yang hebat.
- Misalkan E adalah kunci enkripsi, dan D adalah kunci deskripsi. E dan D adalah pasangan kunci untuk enkripsi dan deskripsi.



Sumber: V. Lusiana

Skema kriptografi kunci publik

- Konsep diatas digunakan untuk mengamankan pertukaran dari dua entitas yang saling berkomunikasi.
- Sistem kriptografi kunci publik cocok untuk kelompok pengguna dijaringan komputer (LAN, WAN)
- Sistem kunci publik tidak memerlukan pengiriman kunci privat melalui saluran komunikasi khusus
- Meskipun kunci publik di umumkan ke setiap orang didalam kelompok, namun perlu dilindungi agar otentikasinya terjamin. Misal tidak diubah oleh orang lain

Perbandingan Kriptografi Kunci Simetri dengan Kriptografi Kunci Publik (Asimetri)

- Kriptografi kunci simetri maupun asimetri mempunyai kelebihan dan kekurangan masing-masing

Kelebihan Kriptografi Kunci Simetri

- ✓ Algoritma dirancang sehingga proses enkripsi dan deskripsi membutuhkan waktu yang singkat
- ✓ Ukuran kunci relatif pendek
- ✓ Dapat digunakan untuk membangkitkan bilangan acak
- ✓ Dapat disusun untuk menghasilkan cipher yang lebih kuat
- ✓ Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima

Kelemahan kriptografi kunci simetri

- Harus dikirim melalui saluran yang aman, kedua pihak yang berkomunikasi harus menjaga kerahasiaan kunci
- Kunci harus sering diubah pada setiap komunikasi

Kelebihan Kriptografi Kunci Publik (Asimetri)

- ✓ Hanya kunci privat yang perlu dijaga kerahasiaannya.
- ✓ Pasangan kunci publik dan privat tidak perlu diubah bahkan dalam periode waktu yang panjang.
- ✓ Dapat digunakan untuk mengamankan pengiriman kunci simetri
- ✓ Beberapa algoritma dapat digunakan untuk pengiriman tanda tangan digital pada pesan.

Kelemahan kriptografi kunci Asimetri

- Enkripsi dan deskripsi data umumnya lebih lambat
- Ukuran cipherteks lebih besar daripada plainteks.
- Ukuran kunci lebih besar dari kunsi simetri
- Karena kunci diketahui secara luas, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.

Kelemahan kriptografi kunci Asimetri

- Tidak ada algoritma kunci publik yang terbukti aman. Kebanyakan algoritma mendasarkan pada sulitnya memecahkan persoalan aritmetik yang menjadi dasar pembangkit kunci.

Aplikasi Kriptografi Kunci Publik

- Aplikasi kriptografi kunci publik dibagi menjadi tiga kategori:
  1. Enkripsi/Deskripsi
  2. Digital Signature
  3. Pertukaran Kunci (Key Exchange)
- Beberapa algoritma cocok digunakan untuk ketiga macam kategori aplikasi(contoh: RSA)
- Beberapa hanya ditujukan untuk aplikasi spesifik (contoh: DSA)

RSA

- ✓Sandi RSA merupakan algoritma kriptografi kunci publik asimetri.
- ✓Ditemukan pertama tahun 1977 oleh Ron Rivest, Adi Shamir dan Len Adleman.
- ✓Nama RSA diambil dari nama tiga penemunya.

- ✓ Kunci enkripsi dan deskripsi menggunakan bilangan bulat.
- ✓ Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum, sehingga disebut kunci publik
- ✓ Sedangkan kunci deskripsi bersifat rahasia.
- ✓ Untuk menemukan kunci deskripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor primanya.
- ✓ Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya

- ✓ Skema RSA sendiri mengadopsi dari skema block cipher.
- ✓ Dimana sebelum dilakukan enkripsi, plainteks yang ada dibagi – bagi menjadi blok – blok dengan panjang yang sama.
- ✓ Plainteks dan cipherteksnya berupa integer(bilangan bulat) antara 1 hingga n.
- ✓ N berukuran biasanya sebesar 1024 bit, dan panjang bloknya sendiri berukuran lebih kecil atau sama dengan log(n) +1 dengan basis 2

Algoritma RSA

1. Menentukan dua bilangan prima
2. Menghitung nilai modulus
3. Menghitung nilai totient
4. Menentukan nilai ***e***
5. Mencari nilai ***d***
6. Mendapatkan nilai ***n,e, dan d*** sehingga pasangan kunci telah terbentuk.

ELGamaL

- Merupakan salah satu algoritma kriptografi kunci publik yang dibuat oleh Taher ElGamal pada tahun 1984.
- Algoritma ini pada umumnya digunakan untuk digital signature, tetapi kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan deskripsi.
- Kekuatan algoritma ini terletak pada sulitnya menghitung logaritma diskrit.
- Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, enkripsi, dan deskripsi

1. Proses Pembentukan Kunci

- Algoritma ElGamal memerlukan sepasang kunci yang dibangkitkan dengan memilih sebuah bilangan prima ***p*** dan dua buah bilangan random ***g*** dan ***x***. Nilai ***g*** dan ***x*** lebih kecil dari ***p*** yang memenuhi persamaan :

$$y = g^x \bmod p$$

- Dari persamaan tersebut ***y***, ***g*** dan ***p*** merupakan kunci publik dan ***x*** adalah kunci rahasia

2. Proses Enkripsi

- Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (ciphertext).
- Pada proses ini digunakan kunci publik (***p, g, y*****).**

3. Proses Deskripsi

- Proses dekripsi merupakan proses mengubah pesan rahasia (ciphertext) menjadi pesan asli (plaintext).
- Pada proses ini digunakan kunci pribadi (***x, p***).

Algoritma Knapsack

- Knapsack dapat diartikan sebagai karung atau kantung.
- Karung digunakan untuk memuat sesuatu.
- Dan tentunya tidak semua objek dapat ditampung di dalam karung. Karung tersebut hanya dapat menyimpan beberapa objek dengan total ukurannya (weight) lebih kecil atau sama dengan ukuran kapasitas karung.
- Setiap objek itupun tidak harus kita masukkan seluruhnya. Tetapi bisa juga sebagian saja.

Knapsack Problem:

- ✓Diberikan bobot knapsack adalah M.
- ✓ Diketahui *n* buah objek yang masing-masing bobotnya adalah w*1*, w*2*, ..., w*n*.
- ✓Tentukan nilai b sedemikian sehingga M = b*1*w*1* + b*2*w*2*+ ... + b*n*w*n*.
- ✓Yang dalam hal ini, b*i* bernilai 0 atau 1. Jika b*i*= 1, berarti objek *i* dimasukkan ke dalam knapsack, sebaliknya jika b*i* = 0, objek *i* tidak dimasukkan

- Ide dasar dari algoritma kriptografi knapsack adalah mengkodekan pesan sebagai rangkaian solusi dari dari persoalan knapsack. Setiap bobot widi dalam persoalan knapsack merupakan kunci privat, sedangkan bit-bit plainteks menyatakan b*i*.

- Misalkan n = 6.

  w1 = 1 w4 = 11

  w2 = 5 w5 = 14

  w3 = 6 w6 = 20.

- Plainteks: 111001010110000000011000
- Plainteks dibagi menjadi blok yang panjangnya n, kemudian setiap bit di dalam blok dikalikan dengan w*i* yang berkorepsonden sesuai dengan persamaan (1)

Blok plainteks ke-1: 111001

Knapsack : 1, 5, 6, 11, 14, 20

Kriptogram: $(1 \times 1) + (1 \times 5) + (1 \times 6) + (1 \times 20)$

$= 32$

Blok plainteks ke-2: 010110

Knapsack : 1, 5, 6, 11, 14, 20

Kriptogram: $(1 \times 5) + (1 \times 11) + (1 \times 14) = 30$

Blok plainteks ke-3: 000000

Knapsack : 1, 5, 6, 11, 14, 20

Kriptogram : 0

Blok plainteks ke-4: 011000

Knapsack : 1, 5, 6, 11, 14, 20

Kriptogram : $(1 \times 5) + (1 \times 6) = 11$

Jadi, cipherteks yang dihasilkan: 32 30 0 11

Enkripsi

- ✓ Enkripsi dilakukan dengan cara yang sama seperti algoritma knapsack sebelumnya.
- ✓ Mula-mula plainteks dipecah menjadi blok bit yang panjangnya sama dengan kardinalitas barisan kunci publik.
- ✓ Kalikan setiap bit di dalam blok dengan elemen yang berkoresponden di dalam kunci publik

Contoh enkripsi

- ✓Plainteks: 011000110101101110
- ✓N=6.
- ✓Kunci publik: 62, 93, 81, 88, 102, 37
- ✓Plainteks dibagi menjadi blok yang panjangnya 6, kemudian setiap bit di dalam blok dikalikan dengan elemen yang berkorepsonden di dalam kunci publik.

Blok plainteks ke-1 : 011000
Kunci publik : 62, 93, 81, 88, 102, 37
Kriptogram : $(1 \times 93) + (1 \times 81) = 174$

Blok plainteks ke-2 : 110101
Kunci publik : 62, 93, 81, 88, 102, 37
Kriptogram : $(1 \times 62) + (1 \times 93) + (1 \times 88) + (1 \times 37) = 280$

Blok plainteks ke-3 : 101110
Kunci publik : 62, 93, 81, 88, 102, 37
Kriptogram : $(1 \times 62) + (1 \times 81) + (1 \times 88) + (1 \times 102) = 333$

Jadi, cipherteks yang dihasilkan : 174, 280, 333

Sumber: Rinaldi Munir

Dekripsi

- ✓ Dekripsi dilakukan dengan menggunakan kunci privat.
- ✓ Mula-mula penerima pesan menghitung n–1 , yaitu balikan ***n*** modulo ***m***, sedemikian sehingga $n \cdot n^{-1} \equiv 1 \pmod{m}$.
- ✓ Kalikan setiap kriptogram dengan n–1 mod m, lalu nyatakan hasil kalinya sebagai penjumlahan elemen-elemen kunci privat untuk memperoleh plainteks dengan menggunakan algoritma pencarian solusi superincreasing knapsack.

Daftar Pustaka

- https://www.unisbank.ac.id/ojs/index.php/fti2/article/view/288
- Veronica Lusiana, Wiwien Hadikurniawati, Kriptografi Kunci Publik, 2010, DINAMIKA INFORMATIKA – Vol II No 1.
- https://docplayer.info/37588712-Sistem-kriptografi-kunci-publik.html
- https://docplayer.info/45911948-Implementasi-kriptografi-kunci-publik-dengan-algoritma-rsa-crt-pada-aplikasi-instant-messaging.html
- https://media.neliti.com/media/publications/144706-ID-implementasi-algoritma-kriptografi-rsa-u.pdf

- https://media.neliti.com/media/publications/174360-ID-pengamanan-dokumen-menggunakan-metode-rs.pdf

PERTEMUAN 06

TANDA TANGAN DIGITAL
&
PROTOKOL KRIPTOGRAFI

Sub Pembahasan

- ✓ **Tandatangan Digital**
  - ✓Konsep tanda tangan digital
  - ✓Penandatangan dengan Cara Mengenkripsi Pesan
  - ✓Tandatangan dengan menggunakan Fungsi Hash
  - ✓Digital Standard Algorithm (DSA)
- ✓ **Protokol Kriptografi**
  - ✓ Protokol komunikasi dengan sistem kriptografi simetri
  - ✓ Protokol komunikasi dengan sistem kriptografi kunci publik
  - ✓ Protokol untuk tanda tangan digital
  - ✓ Protokol untuk tanda tangan digital dengan enkripsi
  - ✓ Pertukaran kunci
  - ✓ Otentikasi

- Aspek keamanan yang disediakan oleh kriptografi:
  1. Kerahasiaan pesan (*confidentiality/secrecy*)
  2. Otentikasi (*authentication*).
  3. Keaslian pesan (*data integrity*).
  4. Anti-penyangkalan (*nonrepudiation*).
- Aspek 1 diselesaikan dengan enkripsi/dekripsi
- Aspek 2 s/d 4 diselesaikan dengan tanda-tangan digital (*digital signature*).

Konsep Tanda Tangan Digital

- Sejak zaman dahulu, tanda-tangan sudah digunakan untuk otentikasi dokumen cetak.
- Tanda-tangan mempunyai karakteristik sebagai berikut:

  - Tanda-tangan adalah bukti yang otentik.

  - Tanda tangan tidak dapat dilupakan.

  - Tanda-tangan tidak dapat dipindah untuk digunakan ulang.

  - Dokumen yang telah ditandatangani tidak dapat diubah.

  -Tanda-tangan tidak dapat disangkal(*repudiation*).

- Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data digital (pesan, dokumen elektronik).
- Tanda-tangan untuk data digital dinamakan **tanda-tangan digital**.
- Tanda-tangan digital bukanlah tulisan tanda-tangan yang di-digitisasi (di-*scan*).

- Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci.
- Tanda-tangan pada dokumen cetak selalu sama, apa pun isi dokumennya.
- Tanda-tangan digital selalu berbeda-beda antara satu isi dokumen dengan dokumen lain.

- Contoh:

Kepada Yth.
Bapak Dekan
Di Tempat

Dengan hormat.
Bersama surat ini saya ingin mengabarkan bahwa nilai skripsi mahasiswa yang bernama Faisal Saleh dengan NIM 13902021 adalah 86,5 atau dalam nilai indeks A. Sidang skripsi sudah dilakukan pada Hari Rabu Tanggal 26 Juli 2023.

Atas perhatian Bapak saya ucapkan terima kasih.

Bandung, 31 Juli 2023

Dosen Pembimbing Skripsi

Ir. Ahmad Agus

-----BEGIN PGP SIGNATURE-----

iQA/AwUAQnibsbPbxejK4Bb3EQJXvQCg8zN6UL0xnwBTPR5
FfWNt4uxh3AEAn2NC/G2VTUrLpcSyo2l/S/D/+rUl=pZeh

-----END PGP SIGNATURE-----

Tanda-tangan digital

Dua cara menandatangani pesan:

1. Enkripsi pesan
2. Menggunakan kombinasi fungsi *hash* (*hash function*) dan kriptografi kunci-publik

Penandatangan dengan Cara Mengenkripsi Pesan

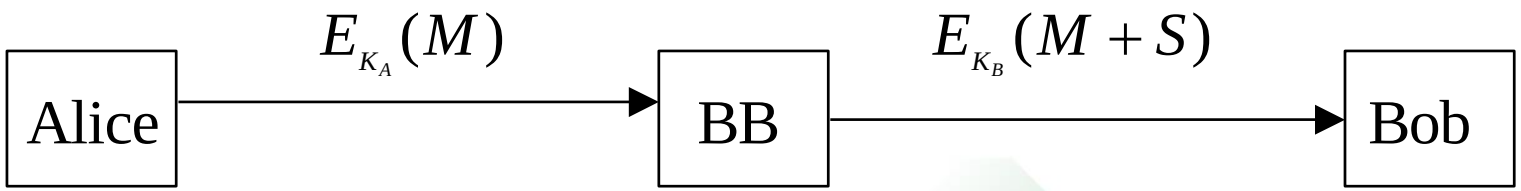
a. Menggunakan kriptografi simetri

Pesan yang dienkripsi dengan algoritma simetri sudah memberikan solusi untuk otentikasi pengirim dan keaslian pesan, karena kunci simetri hanya diketahui oleh pengirim dan penerima.

Tetapi cara ini tidak menyediakan mekanisme untuk anti-penyangkalan.

- Agar dapat mengatasi masalah penyangkalan, maka diperlukan pihak ketiga yang dipercaya oleh pengirim/penerima. Pihak ketiga ini disebut **penengah (arbitrase).**
- Misalkan BB (*Big Brothers*) adalah pihak ketiga (arbitrase) yang dipercaya oleh Alice dan Bob.
- BB memberikan kunci rahasia K_A kepada Alice dan kunci rahasia K_B kepada Bob.
- Hanya Alice dan BB yang mengetahui K_A, begitu juga hanya Bob dan BB yang mengetahui K_B.

- Jika Alice bekirim pesan *P* kepada Bob, maka langkah-langkahnya adalah sebagai berikut:
  1. Alice mengenkripsi pesan *M* untuk Bob dengan K_A, lalu mengirim cipherteksnya ke BB.
  2. BB melihat bahwa pesan dari Alice, lalu mendekripsi pesan dari Alice dengan K_A.
  3. BB membuat pernyataan *S* bahwa ia menerima pesan dari Alice, lalu menambahkan pernyataan tersebut pada plainteks dari Alice.
  4. BB mengenkripsi bundel pesan ($M + S$) dengan K_B, lalu mengirimkannya kepada Bob.
  5. Bob mendekripsi bundel pesan dengan K_B. Ia dapat membaca pesan dari Alice (*M*) dan pernyataan (*S*) dari BB bahwa Alice yang mengirim pesan tersebut.



- Jika Alice menyangkal telah mengirim pesan tersebut, maka pernyataan dari BB pada pesan yang diterima oleh Bob digunakan untuk menolak penyangkalan Alice.

- Bagaimana BB tahu bahwa pesan tersebut dari Alice dan bukan dari Charlie? Karena hanya BB dan Alice yang mengetahui kunci rahasia, maka hanya Alice yang dapat mengenkripsi pesan dengan kunci terebut.

b. Menggunakan kriptografi kunci-publik

Enkripsi biasa (hanya untuk *secrecy*):

- Pesan dienkripsi dengan kunci publik penerima.
- Pesan didekripsi dengan kunci privat penerima.

Cara ini tidak memberikan sarana otentikasi karena kunci publik diketahui oleh banyak orang

Enkripsi sebagai tanda-tangan:

- Pesan dienkripsi dengan kunci privat pengirim.
- Pesan didekripsi dengan kunci publik pengirim.

Dengan cara ini, maka kerahasiaan pesan dan otentikasi keduanya dicapai sekaligus. Ide ini ditemukan oleh Diffie dan Hellman.

- Proses menandatantangani pesan (oleh pengirim):

  $S = E_{SK}(M)$

- Proses membuktikan otentikasi pesan (oleh penerima):

  $M = D_{PK}(S)$

Keterangan:

SK = *secret key* = kunci privat pengirim

PK = *public key* = kunci publik pengirim

E = fungsi enkripsi *D* = fungsi dekripsi

M = pesan semula

S = *signature* = hasil enkripsi pesan

- Dengan algoritma kunci-publik, penandatanganan pesan tidak membutuhkan lagi pihak penengah (arbitrase).

- Beberapa agoritma kunci-publik dapat digunakan untuk menandatangani pesan dengan cara mengenkripsinya, asalkan algoritma tersebut memenuhi sifat:

$$D_{SK}(E_{PK}(M)) = M \text{ dan } D_{PK}(E_{SK}(M)) = M ,$$

Keterangan:

PK = kunci publik

SK = kunci privat (*secret key*).

E = fungsi enkripsi

D = fungsi dekripsi

M = pesan

- Misalkan *M* adalah pesan yang akan dikirim. Pesan *M* ditandatangani menjadi pesan terenkripsi *S* dengan menggunakan kunci privat (*SK*) si pengirim,

$$S = E_{SK}(M)$$

yang dalam hal ini, *E* adalah fungsi enkripsi dari algoritma kunci-publik.

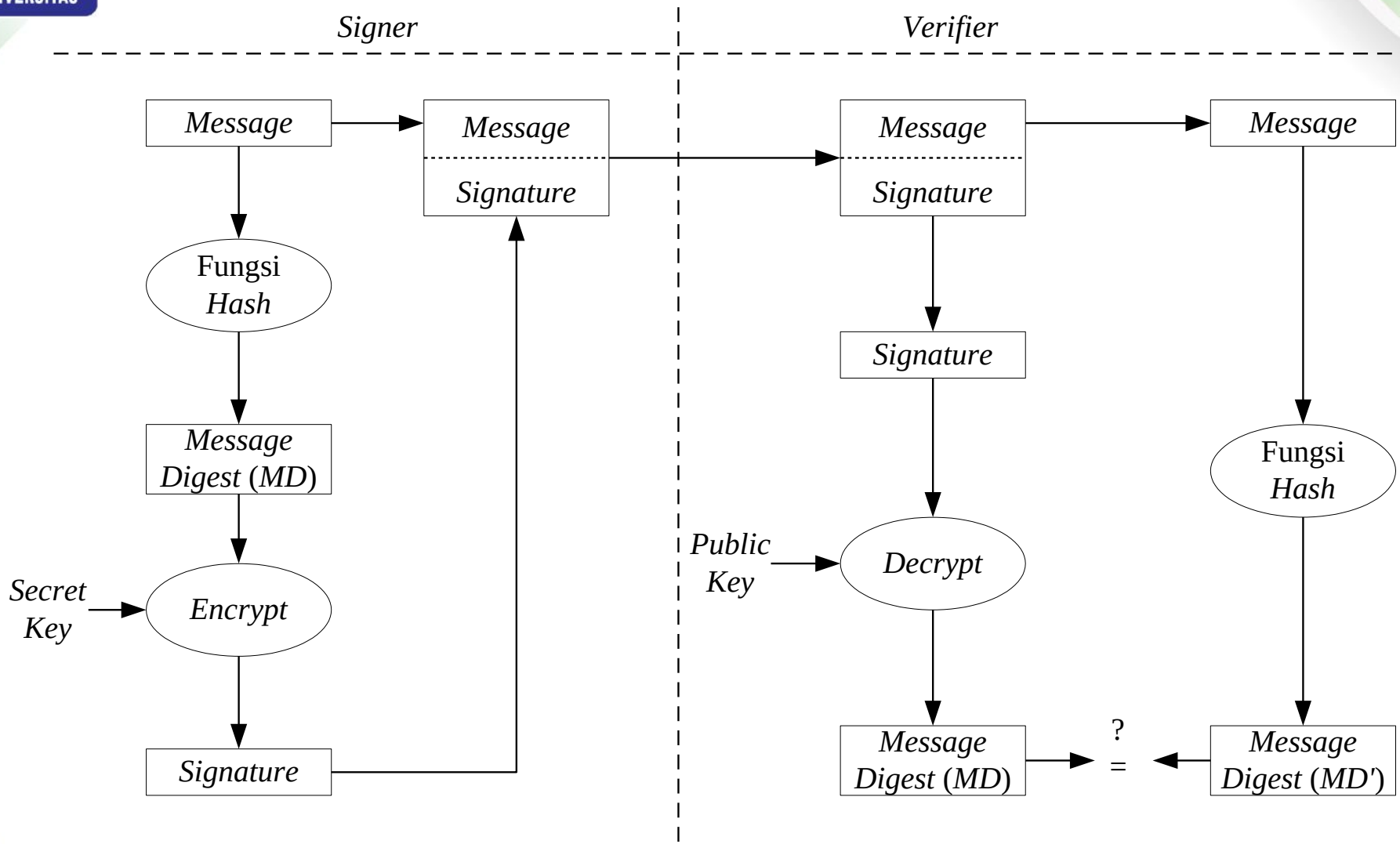
- Selanjutnya, *S* dikirim melalui saluran komunikasi.

Penandatangan dengan Menggunakan Kriptografi kunci-publik dan Fungsi *Hash*

- Penandanganan pesan dengan cara mengenkripsinya selalu memberikan dua fungsi berbeda: kerahasiaan pesan dan otentikasi pesan.

- Pada beberapa kasus, seringkali otentikasi yang diperlukan, tetapi kerahasiaan pesan tidak. Maksudnya, pesan tidak perlu dienkripsikan, sebab yang dibutuhkan hanya keotentikan pesan saja.

- Algoritma kunci-publik dan fungsi hash dapat digunakan untuk kasus seperti ini.



Keotentikan ini dijelaskan sebagai berikut:

a. Apabila pesan M yang dikirim sudah berubah, maka *MD'* yang dihasilkan dari fungsi *hash* berbeda dengan *MD* semula. Ini berarti pesan sudah tidak asli lagi.
b. Apabila pesan M tidak berasal dari orang yang sebenarnya, maka *MD* yang dihasilkan berbeda dengan *MD'* yang dihasilkan pada proses verifikasi (hal ini karena kunci publik yang digunakan oleh penerima pesan tidak berkoresponden dengan kunci privat pengirim)
c. Bila *MD* = *MD'*,ini berarti pesan yang diterima adalah pesan yang asli (*message authentication*) dan orang yang mengirim adalah orang yang sebenarnya (*user authentication*)

- Dua algoritma *signature* yang digunakan secara luas adalah *RSA (Ron Rivest, Adi Shamir and Leonard Adleman)* dan *ElGamal*.
- Pada *RSA*, algoritma enkripsi dan dekripsi identik, sehingga proses *signature* dan verifikasi juga identik.
- Selain *RSA*, terdapat algoritma yang dikhususkan untuk tanda-tangan digital, yaitu *Digital Signature Algorithm* (DSA), yang merupakan bakuan (*standard*) untuk *Digital Dignature Standard* (DSS).
- Pada *DSA*, algoritma *signature* dan verifikasi berbeda

Tanda-tangan dengan algoritma RSA

- **Langkah-langkah pemberian tanda-tangan**

1. Pengirim menghitung nilai *hash* dari pesan *M* yang akan dikirim, misalkan nilai *hash* dari M adalah *h*.
2. Pengirim mengenkripsi *h* dengan kunci privatnya menggunakan persamaan enkripsi *RSA*:

$$S = h^{SK} \bmod n$$

   yang dalam hal ini *SK* adalah kunci privat pengirim dan n adalah modulus ($n = pq$, p dan q adalah dua buah bilangan prima).
3. Pengirim mentransmisikan $M + S$ ke penerima

Langkah-langkah verifikasi tanda-tangan

1. Penerima menghitung nilai *hash* dari pesan *M* yang akan dikirim, misalkan nilai *hash* dari *M* adalah *h*'.
2. Penerima melakukan dekripsi terhadap tanda-tangan *S* dengan kunci publik si pengirim menggunakan persamaan dekripsi *RSA*:

   $h = S^{PK} \bmod n$

   yang dalam hal ini *PK* adalah kunci privat pengirim dan *n* adalah modulus (*n* = *pq*, *p* dan *q* adalah dua buah bilangan prima).
3. Penerima membandingkan *h* dengan *h*'. Jika *h* = *h*' maka tanda-tangan digital adalah otentik. Jika tidak sama, maka tanda-tangan tidak otentik sehingga pesan dianggap tidak asli lagi atau pengirimnya

Digital Standard Algorithm (DSA)

- Digital Signature Algorithm (DSA) merupakan algoritma kriptografi otentikasi pesan yang menggunakan teknologi kunci publik dan Secure Hash Algorithm (SHA-1) dalam operasinya.
- Secara umum DSA dapat dideskripsikan sebagai algoritma kriptografi yang memproses pesan dalam sekumpulan bit (block)/ satuan waktu tertentu dengan menggunakan sepasang kunci publik dan kunci privat bagi proses pembentukan dan verifikasi tanda tangan digital.

Protokol Kriptografi

- Protokol adalah aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan.
- Protokol kriptografi adalah protokol yang menggunakan kriptografi.
- Orang yang berpartisipasi dalam protokol kriptografi memerlukan protokol tersebut misalnya untuk:
  - ✓ Berbagi komponen rahasia untuk menghitung sebuah nilai
  - ✓ Membangkitkan rangkaian bilangan acak,
  - ✓ Meyakinkan identitas orang lainnya (otentikasi)

Protokol Kriptografi

- Protokol kriptografi dibangun dengan melibatkan beberapa algoritma kriptografi.
- Sebagian besar protokol kriptografi dirancang untuk dipakai oleh kelompok yang terdiri dari 2 orang pemakai, tetapi ada juga beberapa protokol yang dirancang untuk dipakai oleh kelompok yang terdiri dari lebih dari dua orang pemakai (misalnya pada aplikasi *teleconferencing*)

Protokol Kriptografi

Untuk mendemonstrasikan protokol kriptografi, kita menggunakan nama-nama pemain sebagai berikut:

- ✓ Alice: orang pertama (dalam semua protokol)
- ✓ Bob: orang kedua (dalam semua protokol)
- ✓ Carol: orang ketiga dalam protokol tiga- atau empatorang
- ✓ Dave: orang keempat dalam protokol empat-orang
- ✓ Eve: penyadap (*eavesdropper*)
- ✓ Trent: juru penengah (*arbitrator*) yang dipercaya

Protokol Komunikasi dengan sistem kriptografi simetri

Protokol 1:

1) Alice dan Bob menyepakati algoritma kriptografi simetri yang akan digunakan.
2) Alice dan Bob menyepakati kunci yang akan digunakan.
3) Alice menulis pesan plainteks dan mengenkripsinya dengan kunci menjadi cipherteks.
4) Alice mengirim pesan cipherteks kepada Bob.
5) Bob mendekripsi pesan cipherteks dengan kunci yang sama dan membaca plainteksnya.

Protokol Komunikasi dengan sistem kriptografi simetri

Eve mendengar semua percakapan antara Alice dan Bob pada protokol ini.

- ✓ Jika Eve menyadap transmisi pesan pada langkah (4), ia harus mencoba mengkriptanalisis cipherteks untuk memperoleh plainteks tanpa mengetahui kunci.
- ✓ Jika ia mendengar pembicaraan pada langkah (1) dan (2), maka ia mengetahui algoritma dan kunci yang digunakan, sehingga ia dapat mendekripsi cipherteks dengan kunci tsb.

Protokol Komunikasi dengan sistem kriptografi simetri

- Protokol kriptografi di atas tidak bagus karena kunci harus tetap rahasia sebelum, sepanjang, dan setelah protokol.
- Langkah (1) dapat dilakukan dalam mode publik, namun
- langkah (2) harus dilakukan dalam mode rahasia. Sistem kriptografi kunci-publik dapat memecahkan masalah distribusi kunci ini.

- https://id.wikipedia.org/wiki/Protokol_kriptografi
- http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Protokol%20Kriptografi.pdf
- Heri Wibowo, Niken Dwi Cahyani, Vera Suryani. Implementasi Digital Signature Algorithm (DSA) Dalam Keamanan SMS Pada Mobile Device. 2010.
- Kaspar Situmorang. Analisis Keamanan dan Kinerja Algoritma Digital Signature Algorithm (DSA) Pada Proses Pembentukan dan Verifikasi Tanda Tangan Digital.
- Rinaldi Munir. Protokol Kriptografi

TUGAS PERTEMUAN 06

- Dikumpulkan pada pertemuan 07
- Buat makalah dengan tema Protokol Kriptografi

PERTEMUAN 07

REVIEW MATERI
&
QUIZ

PERTEMUAN 09

KRIPTOGRAFI DALAM KEHIDUPAN SEHARI-HARI

SUB PEMBAHASAN

- ✓ Kartu Cerdas (Smart Card)
- ✓ Transaksi Lewat Anjungan Tunai Mandiri (ATM)
- ✓ Pay TV
- ✓ Komunikasi dengan Telepon Seluler
- ✓ E-commerce di Internet dan SSL

- Penggunaan kriptografi saat ini sudah menjadi hal yang sering ditemui dalam kehidupan kita sehari–hari.
- Contohnya transaksi di ATM, transaksi dengan kartu kredit, mengakses internet, percakapan dengan menggunakan telepon genggam.
- Kriptografi sangat penting untuk keamanan informasi, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan menggunakan komputer, maka orang tidak bisa memisahkannya dengan kriptografi

Kartu Cerdas

- ✓ Kartu cerdas yang mirip kartu kredit dapat melayani banyak fungsi, mulai dari otentikasi sampai penyimpanan data.
- ✓ Kartu cerdas yang paling populer adalah memory card dan microprocessor card.
- ✓ Memory card mirip dengan floppy disk, sedangkan microprocessor card mirip dengan komputer kecil dengan sistem operasi, sekuriti, dan penyimpanan data

Kartu Cerdas

- ✓ Kartu cerdas mempunyai beberapa jenis antarmuka (interface) yang berbeda.
- ✓ Jenis antarmuka yang umum adalah contact interface, yang dalam hal ini kartu cerdas dimasukkan ke dalam alat pembaca (card reader) dan secara fisik terjadi kontak fisik antara alat dan kartu

Kartu Cerdas

- ✓ Penggunaan kartu cerdas dikombinasikan dengan PIN (Personal Identification Number).
- ✓ Jadi, ada dua level yang harus dari penggunaan kartu cerdas, yaitu memiliki kartu cerdas itu sendiri dan mengetahui PIN yang mengakses informasi yang disimpan di dalam kartu.

Kartu Cerdas

- ✓ Banyak peralatan mobile yang menggunakan kartu cerdas untuk otentikasi. Namun kartu cerdas masih tidak menjamin keamanan secara total.
- ✓ Jika peralatan mobile hilang atau dicuri, sertifikat digital dan kunci privat di dalam kartu cerdas (yang terdapat di dalam peralatan tersebut) berpotensi diakses oleh pencuri untuk mengakses informasi rahasia.

Kartu Cerdas

- ✓ Telpon seluler dengan teknologi GSM memiliki kartu cerdas yang terintegrasi di dalam handphone.
- ✓ Pemilik handphone memiliki opsi untuk men-set PIN untuk proteksi tambahan, sehingga jika handphone hilang atau dicuri, handphone tidak dapat digunakan tanpa mengetahui PIN tersebut.
- ✓ Dengan menggunakan kartu cerdas, pengguna dapat mengakses informasi dari berbagai peralatan dengan kartu cerdas yang sama.

ATM

- ✓ Anjungan Tunai Mandiri atau Automatic Teller Machine(ATM) digunakan nasabah bank untuk melakukan transaski perbankan.
- ✓ Utamanya, kegunaan ATM adalah untuk menarik uang secara tunai (cash withdrawal), namun saat ini ATM juga digunakan untuk transfer uang (pemindahbukuan), mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya.
- ✓ Transaksi lewat ATM memerlukan kartu magnetik (disebut juga kartu ATM) yang terbuat dari plastik dan kode PIN(Personal Information Number) yang berasosiasi dengan kartu tersebut

ATM

- ✓ PIN terdiri dari angka yang harus dijaga kerahasiannya oleh pemilik kartu ATM, sebab orang lain yang mengetahui PIN dapat menggunakan kartu ATM yang dicuri atau hilang untuk melakukan penarikan uang.
- ✓ PIN digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM.
- ✓ Proses verifikasi dilakukan di komputer pusat (host) bank, oleh karena itu harus ada komunikasi dua arah antara ATM dan komputer host.
- ✓ Selama transmisi dari ATM ke komputer host, PIN harus dilindungi dari penyadapan oleh orang yang tidak berhak

ATM

- ✓ Bentuk perlindungan yang dilakukan selama transmisi adalah dengan mengenkripsikan PIN. Di sisi bank, PIN yang disimpan di dalam basisdata juga dienkripsi.
- ✓ Algoritma enkripsi yang digunakan adalah DES dengan mode ECB. Karena DES bekerja dengan mengenkripsikan blok 64-bit, maka PIN yang hanya terdiri dari 32 bit harus ditambah dengan padding bits sehingga panjangnya menjadi 64 bit.
- ✓ Padding bits yang ditambahkan berbeda-beda untuk setiap PIN, bergantung pada informasi tambahan pada setiap kartu ATM-nya

PAY TV

- ✓ PayTV adalah siaran TV yang hanya dapat dinikmati oleh pelanggan yang membayar saja, sedangkan pemilik TV yang tidak berlangganan tidak dapat menikmati siarannya.
- ✓ Siaran PayTV dipancarkan secara broadcast, namun hanya sejumlah pesawat TV yang berhasil menangkap siaran tersebut yang dapat ‘mengerti’ isinya.
- ✓ Pada sistem PayTV, sinyal broadcast dienkripsi dengan kunci yang unik. Orang-orang yang berlangganan Pay TV pada dasarnya membayar untuk mengetahui kunci tersebut.

PAY TV

- ✓ Bagaimana mengetahui bahwa kunci tersebut dimiliki oleh pelanggan yang sah, dan bukan orang yang mengetahui kunci tersebut dari pelanggan lainnya?
- ✓ Solusi yang umum adalah setiap pelanggan diberikan kartu cerdas (smart card) yang mengandung kunci privat (private key) yang unik dalam konteks algoritma kriptografi kunci-publik.

PAY TV

- ✓ Kartu cerdas dimasukkan ke dalam card reader yang dipasang pada pesawat TV.
- ✓ Selanjutnya, pelanggan Pay TV dikirimi kunci simetri yang digunakan untuk mengenkripsi siaran.
- ✓ Kunci simetri ini dikirim dalam bentuk terenkripsi dengan menggunakan kunci publik pelanggan.
- ✓ Smart card kemudian mendekripsi kunci simetri ini dengan kunci privat pelanggan.
- ✓ Selanjutnya, kunci simetri digunakan untuk mendekripsi siaran TV.

KOMUNIKASI TELP SELULAR

- ✓ Penggunaan telepon seluler (ponsel) yang bersifat mobile memungkinkan orang berkomunikasi dari tempat mana saja.
- ✓ Telepon seluler bersifat nirkabel (wireless), sehingga pesan yang dikirim dari ponsel ditransmisikan melalui gelombang mikro (microwave) atau radio sampai ia mencapai base station (BST) terdekat, selanjutnya ditransfer ke ponsel penerim.
- ✓ GSM merupakan teknologi telepon seluler yang paling banyak digunakan di seluruh dunia.

KOMUNIKASI TELP SELULAR

- ✓ Untuk membuat komunikasi lewat ponsel aman, maka pesan dienkripsi selama transmisi dari ponsel ke BST terdekat. Metode enkripsi yang digunakan adalah metode cipher aliran (stream cipher)
- ✓ Pada GSM diperlukan dua kebutuhan keamanan yaitu:
  1. Otentikasi penelpon (user authentication), yang merupakan kebutuhan bagi sistem.
  2. Kerahasiaan (confidentiality) pesan (data atau suara), yang merupakan kebutuhan bagi pelanggan.

KOMUNIKASI TELP SELULAR

Dua kebutuhan ini dipenuhi dengan penggunaan kartu cerdas (smart card) personal yang disebut kartu SIM(Subscriber Identity Modulecard). Kartu SIM berisi:

1. Identitas pelanggan/pengguna operator seluler berupa IMSI (international mobile subscriber identity) yang unik nilainya.
2. Kunci otentikasi rahasia sepanjang 128-bit yang diketahui hanya oleh operator.
3. Pin (jika di-set oleh pengguna)
4. Program enkripsi.

KOMUNIKASI TELP SELULAR

Secara keseluruhan, sistem keamanan GSM terdiri atas dalam 3 komponen, yaitu:

1. Kartu SIM
2. Handset (pesawat telepon seluler)
3. Jaringan GSM

Setiap jaringan dioperasikan oleh operatornya masing-masing (Excelcomindo, Telkomsel, Satelindo). Komputer operator (host) memiliki basisdata yang berisi identitas (IMSI) dan kunci otentikasi rahasia semua pelanggan/pengguna GSM.’

E-Commerce di Internet

- ✓ Sekarang banyak orang berbelanja melalui *web* di internet.
- ✓ Pembayaran barang bisa dilakukan dengan menggunakan kartu kredit atau e-money yang berarti bahwa pembeli harus mengirimkan kode PIN melalui internet.
- ✓ *Browsing web* secara aman adalah fitur paling penting pada *e-commerce*.
- ✓ *Secure Socket Layer* (SSL) adalah protokol yang digunakan untuk *browsing web* secara aman.
- ✓ Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara *website* dan *web brwoser* (misalnya *Netscape*, *Interner Explorer*, dsb).

E-Commerce di Internet

- ✓ SSL adalah contoh protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*.
- ✓ *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*.
- ✓ Fungsi paling dasar yang digunakan SSL adalah membentuk saluran untuk mengirimkan data terenkripsi, seperti data kartu kredit, dari *browser* ke *website* yang dituju

Daftar Pustaka

- Nandang Iriadi. Analisis Keamanan E-mail Menggunakan Pretty Good Privacy. 2011. https://ejournal.bsi.ac.id/ejurnal/index.php/paradigma/article/view/3422.
- Alamsyah. Implementasi Keamanan E-mail Dengan Menggunakan Pgptray. 2011. Majalah Ilmiah Mektek.

PERTEMUAN
10 - 15

PRESENTASI PROJECT

Project Kelompok

- Project kriptografi berupa makalah dan program.
- Presentasi project pertemuan 10-15