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 8 diadakan UTS
- 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 UAS)

1. Membentuk kelompok. Satu kelompok 5 mahasiswa atau disesuaikan dengan jumlah mhs keseluruhan.
2. Project kriptografi berupa makalah dan program.
3. Hasil program di burning dalam CD dan dilampirkan di belakang makalah.
4. Presentasi project pertemuam 10-14

Outline makalah kriptografi

LEMBAR JUDUL
KATA PENGANTAR
DAFTAR ISI

BAB I PENDAHULUAN

1.1. Latar Belakang Masalah
1.2. Perumusan Masalah
1.3. Maksud dan Tujuan
1.4. Metode Penelitian
1.5. Ruang Lingkup

BAB II LANDASAN TEORI

BAB III PEMBAHASAN

3.1. Analisa Kebutuhan
3.2. Perancangan Objek
3.3. Tampilan Hasil
3.4. Cara Kerja Aplikasi

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan
5.2. Saran

DAFTAR PUSTAKA
DAFTAR RIWAYAT HIDUP
LAMPIRAN

Penilaian akhir

Absen	: 20 %
Tugas	: 25 %
UTS	: 25 %
UAS/Project	: 30 %

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

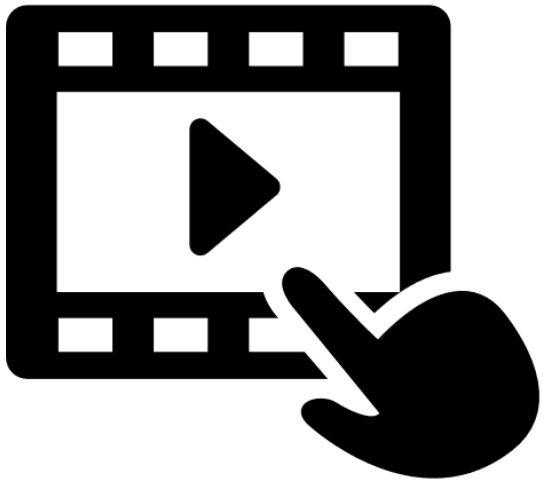
Pesan

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

2. Gambar→

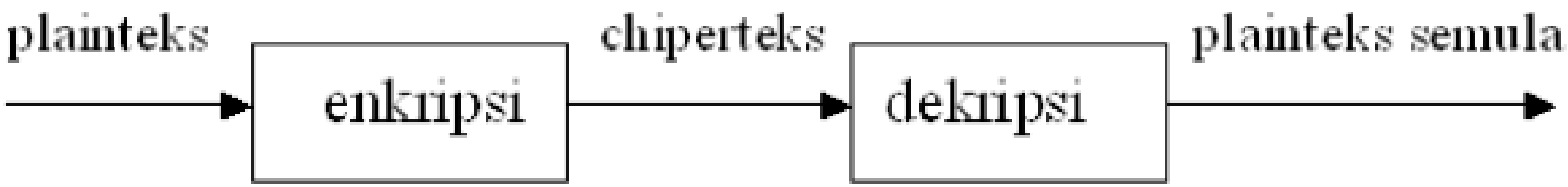
Pesan

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)

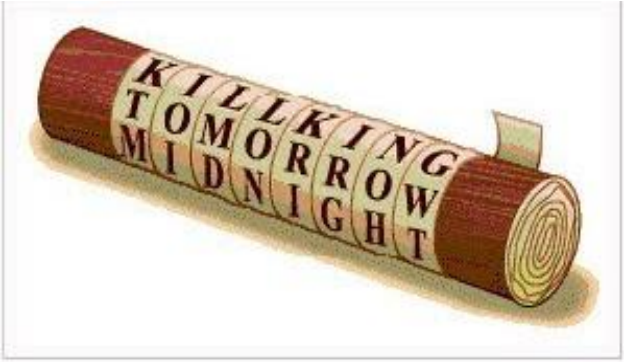
Pada zaman Romawi kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang dengan mengganti susunan alfabet dari:

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

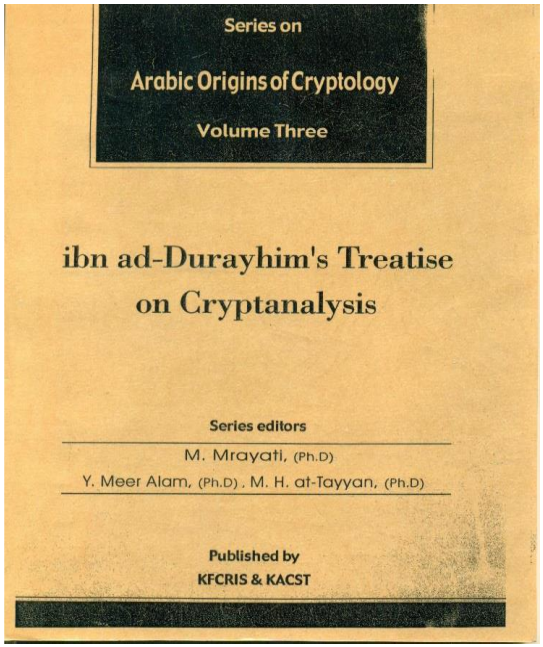
- Awal tahun 400 SM bangsa Spartan di Yunani memanfaatkan kriptografi di bidang militer dengan menggunakan alat yang disebut *scytale*, yakni pita panjang berbahan daun papyrus yang dibaca dengan cara digulungkan ke sebatang silinder



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

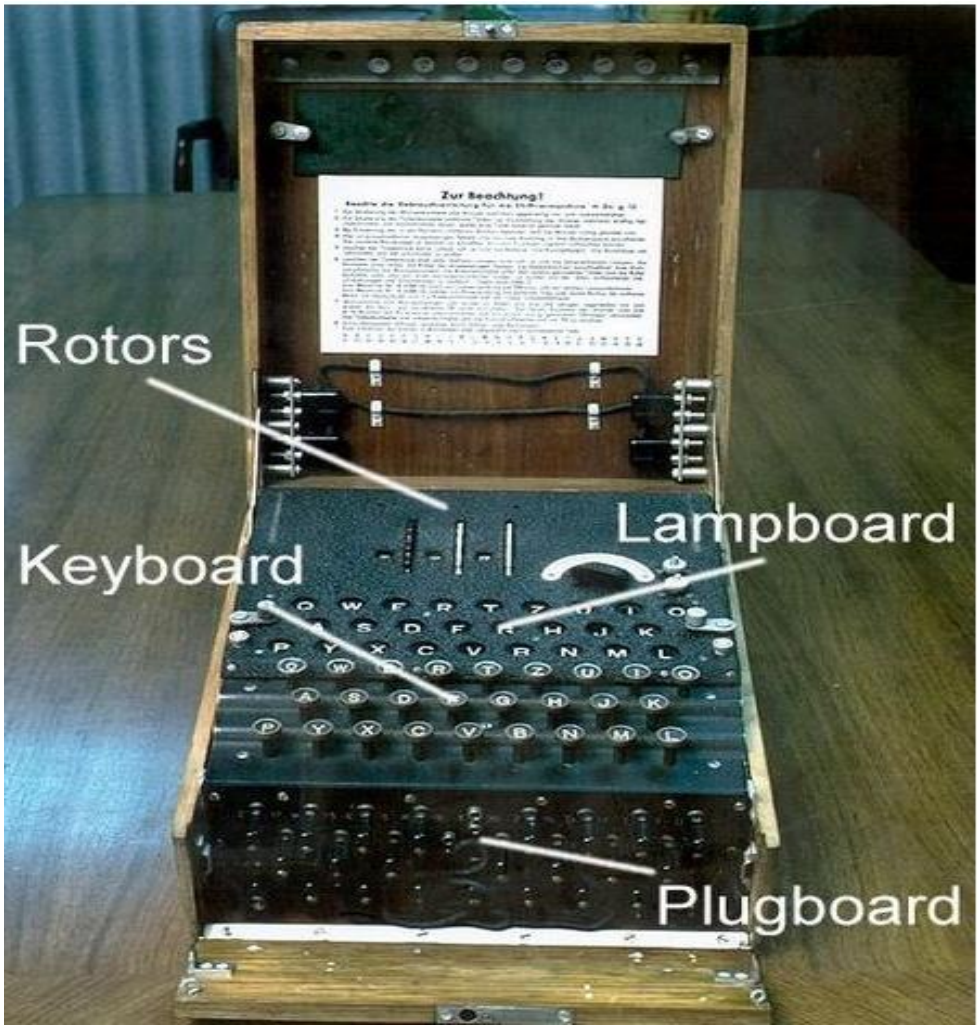
- Seri pertama menyajikan manuskrip kuno tentang kriptanalisis yang ditulis oleh Al-Kindi
- Seri kedua tentang risalah Ibn Adlan yang berisi manual kriptanalisi yang ditulis abad ke 13
- Seri ketiga adalah risalah Ibn Ad-Durayhim



- 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

