



**ITelkom
Surabaya**
Solution for The Nation

INTRODUCTION TO INFORMATION TECHNOLOGY

PROGRAM STUDI S1 TEKNOLOGI INFORMASI
FAKULTAS TEKNOLOGI INFORMASI DAN INDUSTRI
INSTITUT TEKNOLOGI TELKOM SURABAYA

-
- ▶ INFORMATION AND DATABASES
 - ▶ RELATIONAL DATABASE AND DATAWAREHOUSE
 - ▶ DATA MINING
 - ▶ INFORMATION ASSURANCE AND SECURITY
 - ▶ RISK MANAGEMENT
 - ▶ Information assets and vulnerabilities
 - ▶ IT Threats, Goals, and Solutions
 - ▶ Policies and Actions
 - ▶ IT DISASTER RECOVERY PLANNING
 - ▶ RAID LEVELS
 - ▶ Cryptography



INFORMATION

- ▶ Informasi bukanlah akhir dari sebuah information processing, urutan sebuah informasi adalah
 - ▶ DIKW (Data – Information – Knowledge - Wisdom)
- ▶ Kita dapat memproses data mengorganisasi, memanipulasi, mengurutkan, memfilter, dan/atau melakukan perhitungan didalamnya
 - ▶ Data merupakan sebuah input yang belum diproses atau data mentah (akumulasi, temuan, input, atau persepsi yang tidak terorganisir)
 - ▶ Informasi, Knowledge, dan Wisdom secara kolektif terdiri dari kekayaan intelektual



DATABASES

- ▶ Bentuk utama dari penyimpanan saat ini adalah kumpulan data yang terorganisir
- ▶ Menggunakan database management system (DBMS) untuk membuat database, mengakses data pada database, memanipulasi data pada database dan melihat data melalui berbagai filter
- ▶ Bentuk umum dari database adalah relational database



RELATIONAL DATABASE

- ▶ Relations database merupakan kumpulan dari rekaman, berkaitan dengan personal seperti catatan siswa, catatan pelanggan, catatan laporan insiden dan setiap rekaman pada relation share harus memiliki struktur yang sama
- ▶ Relation terlihat seperti sebuah table setiap baris pada relation adalah rekaman dan setiap kolomnya adalah bidang datanya (fields)
- ▶ Fields memiliki tipe (string, number, date, Boolean, dll)
- ▶ Apabila memiliki satu atau lebih relational database maka yang perlu dilakukan antara lain Query, Insert, Update/Modify, Delete, dan Set Operations



TWO RELATIONS

Student ID	First Name	Last Name	Major	Minor	GPA
11151631	George	Duke	MUS	PHY	3.676
10857134	Mike	Keneally	MUS	CHE	2.131
19756311	Ian	Underwood	MUS	HIS	3.801
18566131	Ruth	Underwood	MUS	MAT	3.516
18371513	Frank	Zappa	MUS		2.571

Student ID	Address	City	State	Zip	Phone
10857134	8511 N. Pine St	Erlanger	KY	41011	(859) 555-1234
11151631	315 Sycamore Dr	Cincinnati	OH	45215	(513) 555-2341
18371513	32 East 21st Apt C	Columbus	OH	43212	(614) 555-5511
18566131	191 Canyon Lane	Los Angeles	CA	91315	(413) 555-1111
19756311	32 East 21st Apt C	Columbus	OH	43212	(614) 555-5511



UNIQUE IDENTIFIERS

- ▶ Untuk mengkombinasi data dari beberapa relation, kita membutuhkan beberapa informasi yang sama pada relation tersebut
 - ▶ Misalnya, bagian pada informasi terdapat persamaan relation Student ID



DATA WAREHOUSE

- ▶ Organisasi mengumpulkan data (puluhan hingga ribuan databases) yang dikenal sebagai data warehouse
 - ▶ Jumlah total dari data didapatkan dari atau tentang organisasi
 - ▶ Data proses (informasi), bisnis proses, dan
- ▶ Untuk membangun warehouse, organisasi menggunakan proses ETL
 - ▶ Extract data – data berasal dari variasi source
 - ▶ Transform data – perbedaan source memungkinkan tidak “sync up”
 - ▶ Load data – menjadi storage facility
- ▶ Bagaimana belajar dari data warehouse?
 - ▶ Variasi proses dari organisasi namun termasuk database management system operations, analysis tools, statistical algorithm



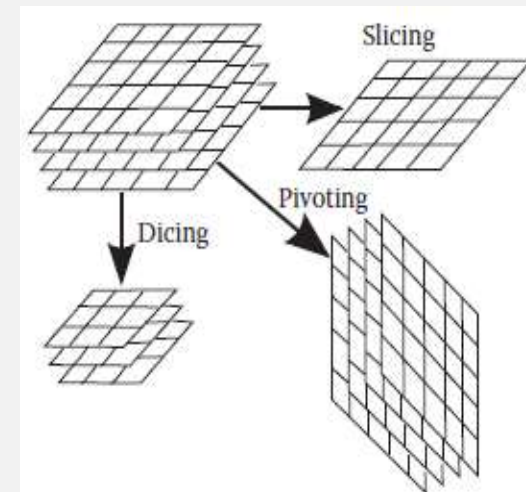
DATA WAREHOUSE SOURCES

- Enterprise resource planning systems
- Supply chain management systems
- Marketing and public relations reports
- Sales records
- Purchasing and inventory records
- Direct input from customers (e.g., input from a web form or a survey)
- Human relations records
- Budget planning
- Ongoing project reports
- General accounting data



OLAP

- ▶ Online Analytical Processing – membuat himpunan data yang bermakna
 - ▶ Slicing – mengelompokkan data multidimensi ke satu dimensi
 - ▶ Dicing – melalui pembatasan dan proyeksi
 - ▶ Drilling up/down – menggeser tampilan ke atas (kurang detail) atau ke bawah (lebih detail)
 - ▶ Pivoting – mengubah prespektive dari data



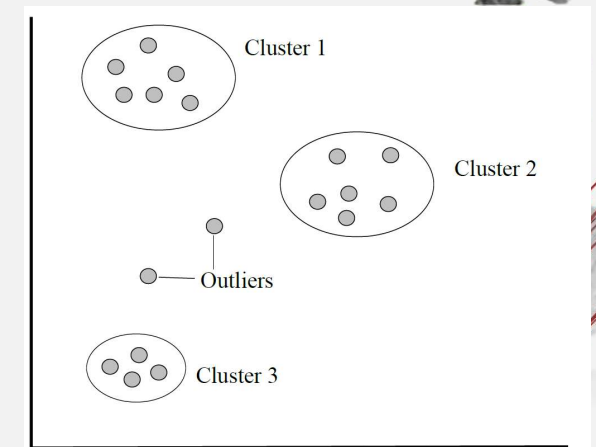
DATA MINING

- ▶ Merupakan cabang dari AI
 - ▶ Algoritma statistic diaplikasikan untuk mengelompokkan data
 - ▶ Dicoba untuk menemukan sesuatu yang menarik/bermanfaat
- ▶ Berputar disekitar *nearest neighbors*
 - ▶ Diberikan beberapa datum yang nilainya adalah $(X1, X2, X3, X4, \dots, Xn)$ dapat dicari dari nearest neighbor(s)
 - ▶ Jarak perhitungan menjadi Euclidean distance formula
 - ▶ $\sqrt{(X1 - Y1)^2 + (X2 - Y2)^2 + (X3 - Y3)^2}$
 - ▶ Dapatkah kita hitung $(X1 - Y1)$ jika data bukan angka?
 - ▶ Bagaimana jika datum ini untuk menghitung jenis kelamis, kebangsaan, etnis, dll ?
- ▶ Variasi adalah *K-nearest neighbors*
 - ▶ Pilih K-fields (mungkin diacak) bukan n fields
 - ▶ 10 bidang memungkinkan menghasilkan 1024 kombinasi berbeda

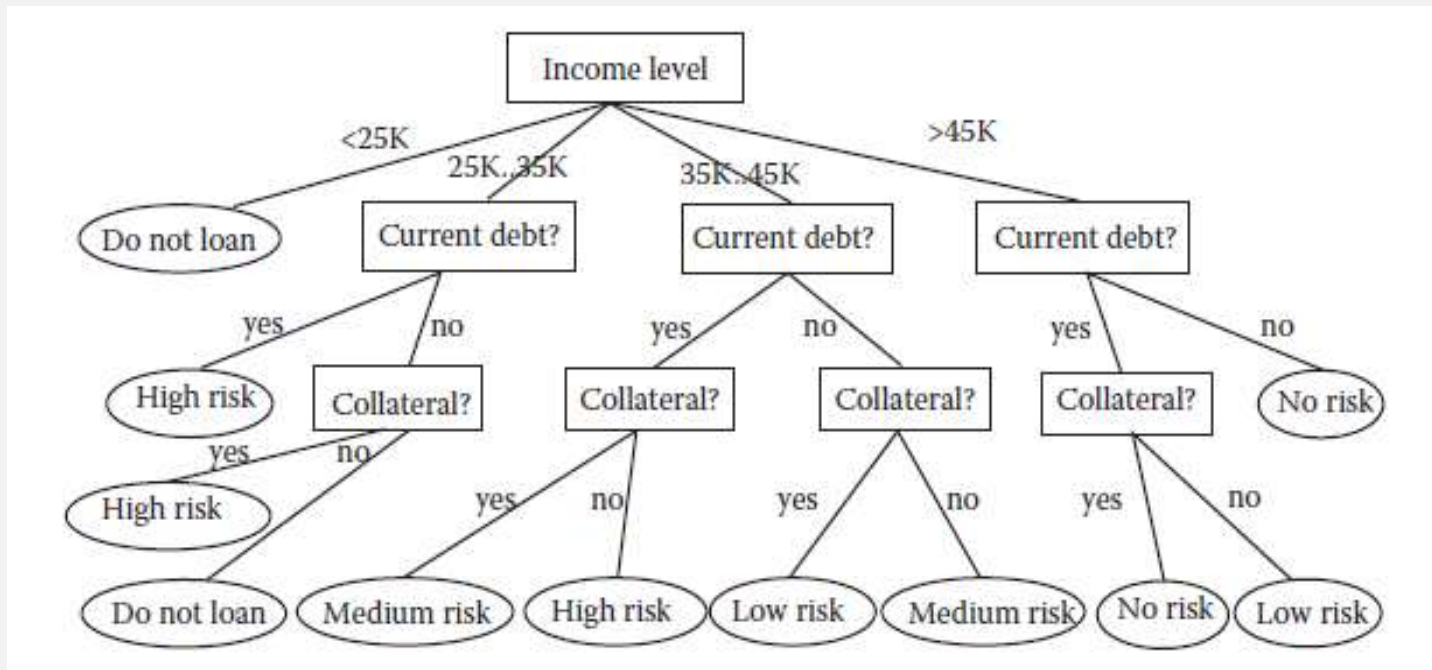


CLUSTERING

- ▶ Groupkan data bersama dengan yang terdekat
 - ▶ Dimulai dengan memilih data sebagai “center” dari cluster
 - ▶ Untuk memberikan rekaman, Rx, mencari diantara center yang terdekat
 - ▶ Mengidentifikasi cluster (kelompok data dari jarak terdekat) dan menandai mereka berdasarkan kategori
- ▶ Cluster memungkinkan memberi informasi data
 - ▶ Pada data medis, mungkin satu kluster dapat berasosiasi dengan pasien yang menderita diabetes tipe 2 sehingga dapat mengidentifikasi fitur yang memberi tahu factor apa yang dapat dijadikan klasifikasi diabetes



DECISION TREES



ADVANTAGES/DISADVANTAGES OF DATA MINING

- ▶ Data tersedia
- ▶ Penambangan berpotensi memberi kita informasi baru
 - ▶ Sering diterapkan dalam bisnis untuk membantu pengambilan keputusan
 - ▶ Telah digunakan dalam penelitian medis/bioinformatika
 - ▶ Diterapkan di komunitas intelijen
- ▶ Perhitungan
 - ▶ Dengan n data, mungkin harus mencoba kombinasi 2^n untuk mendapatkan hasil
 - ▶ Jika $n = 10$, $2^n = 1024$
 - ▶ Jika $n = 20$, 2^n lebih dari 1 juta
 - ▶ Jika $n = 30$, 2^n lebih dari 1 milyar
 - ▶ Ketika n meningkat, 2^n meningkat jauh lebih cepat



ADVANTAGES/DISADVANTAGES OF DATA MINING

- ▶ Tidak diketahui apakah akan mendapatkan sesuatu yang berarti dalam penambangan data
- ▶ Data yang ditambang mungkin atau tidak benar, misalnya aturan tentang a dan b bekerja dengan baik tetapi mungkin tidak



INFORMATION ASSURANCE AND SECURITY

- ▶ Memastikan informasi benar dan aman
- ▶ IAS melarang tiga tujuan :
 - ▶ Confidentiality – memastikan data aman
 - ▶ Integrity – memastikan data benar
 - ▶ Availability – memastikan data dapat diakses saat dibutuhkan
- ▶ Sebagaimana yang diterapkan pada tiga komponen TI: komunikasi, hardware, software



RISK MANAGEMENT

- ▶ IAS berkaitan dengan perlindungan IT (baik perangkat keras fisik dan informasi/data)
 - ▶ Untuk melakukan perlindungan ini, organisasi akan menjalani analisis resiko strategis menggunakan manajemen resiko
 - ▶ Mengidentifikasi tujuan organisasi
 - ▶ Mengidentifikasi asset informasi organisasi
 - ▶ Menyebutkan kerentanan asset tersebut
 - ▶ Mengidentifikasi ancaman yang mengeksploitasi kerentanan tersebut
 - ▶ Menemukan solusinya
 - ▶ Memprioritaskan solusi berdasarkan pada tujuan awal



INFORMATION ASSETS AND VULNERABILITIES

- ▶ Aset Fisik
- ▶ Hak Milik Intelektual
- ▶ Informasi
- ▶ Aset diprioritaskan oleh kegunaan atau kegunaannya dalam organisasi
- ▶ Organisasi dapat menerapkan klasifikasi keamanan untuk asset
- ▶ Kerentanan akan bervariasi dari asset ke asset meskipun ada beberapa kerentanan di beberapa kategori
 - ▶ Setiap hardware komputer memiliki kerentanan terhadap kebakaran dan kerusakan air
 - ▶ Sebagian besar komputer rentan terhadap serangan berbasis jaringan



THREATS AND GOALS

- ▶ Bagaimana kerentanan masing-masing asset dapat dieksploitasi?
 - ▶ Seseorang dapat dieksploitasi oleh social engineering
 - ▶ Server mungkin memiliki ancaman oleh penolakan serangan layanan
 - ▶ Setiap komputer mungkin terancam dengan akses tidak sah (pembobolan) dengan mengeksploitasi beberapa kelemahan sistem operasi
- ▶ Dengan asset, kerentanan, dan ancaman ditetapkan, kembali ke tujuan kami
 - ▶ Memprioritaskan tujuan sehingga bias memprioritaskan asset dan ancaman
 - ▶ Jika menghargai lebih karyawan lebih dari informasi, dapat dipastikan bahwa ancaman terhadap karyawan ditangani sebelum kami menangani ancaman perangkat keras



POLICIES AND ACTIONS

- ▶ Menurunkan mekanisme untuk menangani ancaman
- ▶ Buat kebijakan dan item yang dapat ditindaklanjuti
 - ▶ Kebijakan: Batasan akses pengguna, kata sandi yang kuat, pelatihan menentang rekaya social
 - ▶ Tindakan: perangkat lunak deteksi instruksi, bangunan tahan api dengan sprinkler atau sistem busa, menjaga keamanan data di luar lokasi, dll
- ▶ Salah satu ancaman adalah bencana (kecelakaan alami, buatan manusia) jadi kita harus mendefinisikan kebijakan yang menentukan tindakan pencegahan dan cara untuk pulih dari bencana



IT DISASTER RECOVERY PLANNING

▶ Persiapan

- ▶ Backup regular dan tepat waktu diadakan di luar lokasi
- ▶ Redundansi penyimpanan data
- ▶ Memiliki peralatan cadangan
- ▶ Pelindung lonjakan arus, catu daya yang tidak terputus, gunakan penghambat busa untuk kebakaran, bukan alat penyiram
- ▶ Pemantauan peraltan dan personil logging yang mengakses data sensitive
- ▶ Kata sandi yang kuat

▶ Pemulihan

- ▶ Mengembalikan data, membawa kembali peralatan, mengganti peralatan yang rusak
- ▶ Memiliki situs lain yang dapat menangani pemrosesan selama keadaan darurat



IT THREATS AND SOLUTIONS

- ▶ Humans:
 - ▶ Social engineering, phishing scams, insider attacks education, good morale, auditing access, providing restrictive access rights
- ▶ Computer systems:
 - ▶ Protocol attacks, software exploits, malware – sistem yang dikonfigurasi dan diamankan dengan benar, mendidik pengguna, kata sandi yang kuat, dan/atau bentuk otentikasi biometric
 - ▶ Denial of service attacks, intruksi – firewall, konfigurasi lain untuk menguji pesan dan aktifitas yang mencurigakan, memeriksa file log
 - ▶ Kerusakan penyimpanan, intersepsi pesan – enkripsi, tanda tangan digital, redundansi



DIGITAL SIGNATURES AND CERTIFICATES



TWO SAMPLE CERTIFICATES



Certificate Viewer: "*.nku.edu"

General Details

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN)	*.nku.edu
Organization (O)	Northern Kentucky University
Organizational Unit (OU)	Department of Computer Science
Serial Number	00:D2:64:9B:80:C8:D4:80:4E

Issued By

Common Name (CN)	*.nku.edu
Organization (O)	Northern Kentucky University
Organizational Unit (OU)	Department of Computer Science

Validity

Issued On	Sat 3/3/2012
Expires On	Mon 3/3/2014

Fingerprints

SHA1 Fingerprint	92:FB:C4:D3:11:F5:59:6D:D6:E1:78:D5:6B:39:15:5D:9A:C6:68:E6
MD5 Fingerprint	83:51:AE:30:18:AA:67:22:3E:81:F1:EE:8D:87:1B:15

Close

Certificate Viewer: "Builtin Object Token: Visa eCommerce Root"

General Details

This certificate has been verified for the following uses:

SSL Certificate Authority

Issued To

Common Name (CN)	Visa eCommerce Root
Organization (O)	VISA
Organizational Unit (OU)	Visa International Service Association
Serial Number	13:86:35:4D:1D:3F:06:F2:C1:F9:65:05:D5:90:1C:62

Issued By

Common Name (CN)	Visa eCommerce Root
Organization (O)	VISA
Organizational Unit (OU)	Visa International Service Association

Validity

Issued On	Tue 6/25/2002
Expires On	Thu 6/23/2022

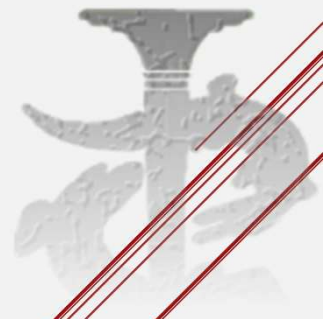
Fingerprints

SHA1 Fingerprint	70:17:9B:86:8C:00:A4:FA:60:91:52:22:3F:9F:3E:32:BD:E0:05:62
MD5 Fingerprint	FC:11:B8:D8:08:93:30:00:6D:23:F9:7E:EB:52:1E:02

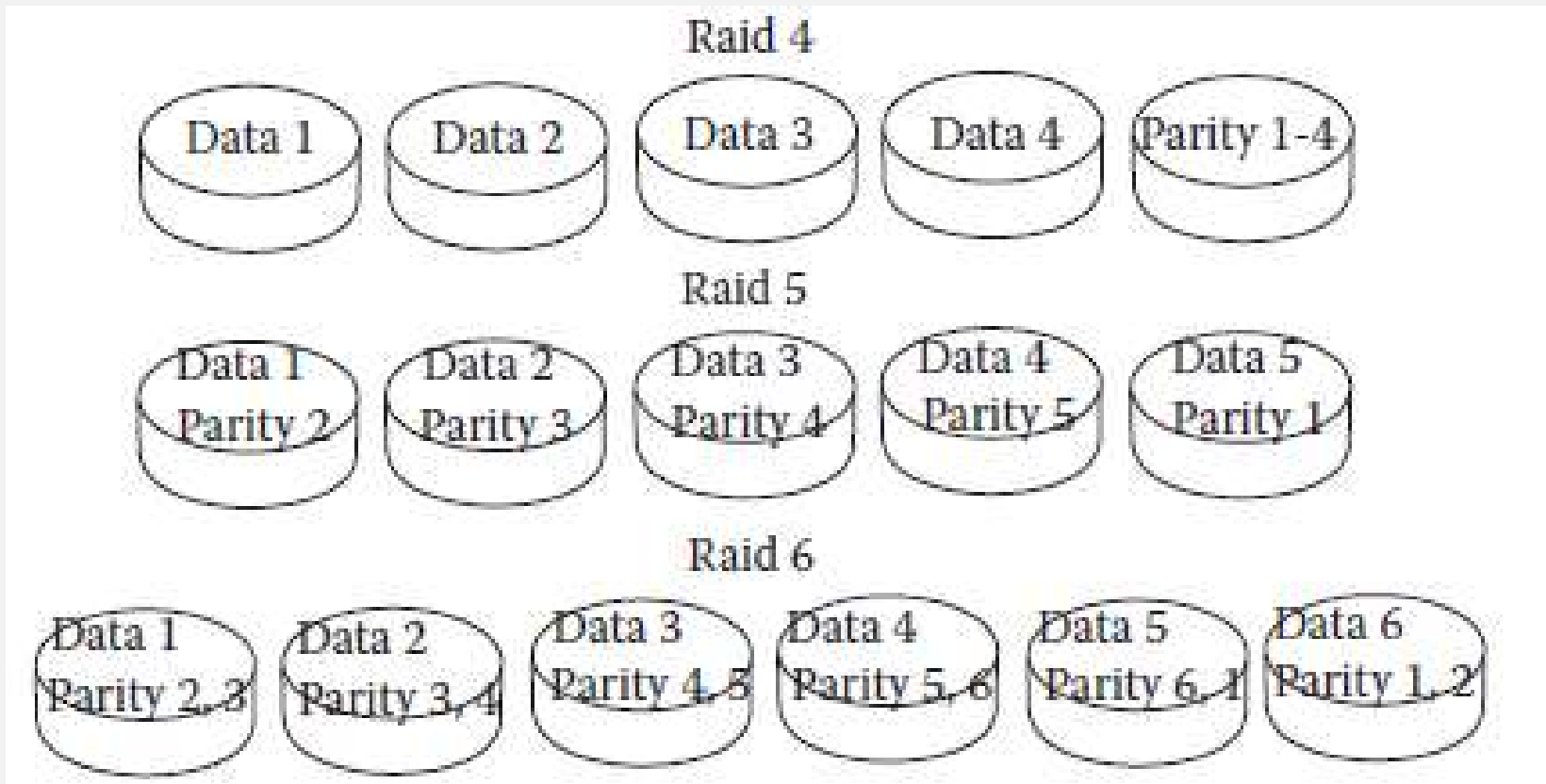
Close

RAID LEVELS

- ▶ RAID 0 – no redundancy, hanya mendistribusikan file
- ▶ RAID 1 – mirror, setengah dari driver merupakan cadangan
- ▶ RAID 2 – redundancy melalui kode Hamming
- ▶ RAID 3 – redundancy melalui parity bits
- ▶ RAID 4 – redundancy (parity) disimpan pada single drive
- ▶ RAID 5 – redundancy split across surfaces
- ▶ RAID 6 – sama seperti 5 namun duplikasi parity data untuk redundancy lebih



RAID 4-6

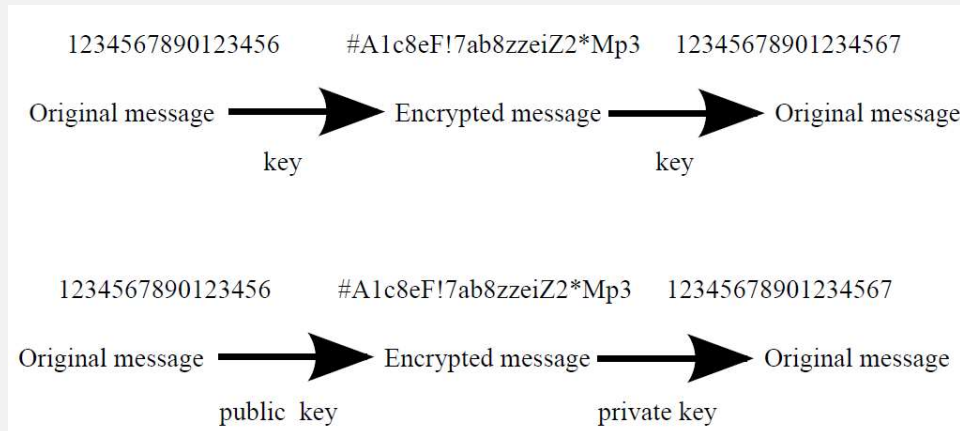


CRYPTOGRAPHY

- ▶ Menempatkan pesan dengan dikode menggunakan kunci untuk encrypt dan decrypt pesan
- ▶ Saat ini, kriptografi didasarkan pada manipulasi matematis dari pesan
 - ▶ Penyimpanan pesan pada ASCII untuk setiap 1 bit pada pesan, ditambah angka, menyimpan atau mengirimkan pesan dengan jumlahnya
 - ▶ Pesan "Hello"
 - ▶ 01001000 01100101 01101100 01101100 01101111
 - ▶ Menggunakan kunci dari 13 bit, kelompok pesan menjadi 13 bit
 - ▶ 0100100001100 1010110110001 1011000110111 1
 - ▶ Menggunakan jumlah 13 integer
 - ▶ Jika 13 bits menggunakan 1, tambahkan angka integer yang sesuai
 - ▶ 0100100001100 → 2 + 19 + 743 + 1501 = 2265
 - ▶ Menyimpan atau mengirim 2265



PUBLIC VS PRIVATE KEY ENCRYPTION



- ▶ Symmetric (public) key encryption – one key used for both encrypting and decrypting
- ▶ Asymmetric (private) key encryption – one key used for encrypting (public key) and another for decrypting (private key)



USING A FOR DECRYPTING KEY

- ▶ Urutan numerik dari 13 angka integer semakin aditif
 - ▶ Untuk setiap nomor tunggal dalam urutan, ini lebih besar dari jumlah sebelumnya
 - ▶ Mudah untuk mengkonversi dari 2265 kembali ke angka yang jumlahnya 2265
 - ▶ Largest number ≤ 2265 ? 1501. $2265 - 1501 = 764$
 - ▶ Largest number ≤ 764 ? 743. $764 - 743 = 21$
 - ▶ Largest number ≤ 21 ? 19. $21 - 19 = 2$
 - ▶ Largest number ≤ 2 ? 2. $2 - 2 = 0$.
 - ▶ So $2265 = 2 + 21 + 764 + 1501 = 0100100001100$



-
- ▶ BUAT ARTIKEL TENTANG PEKERJAAN YANG INGIN KALIAN LAKUKAN PADA SAAT LULUS DIBIDANG TEKNOLOGI INFORMASI DAN JELASKAN MATERI APA SAJA YANG AKAN KALIAN KUASAI UNTUK MENDAPATKAN PEKERJAAN TERSEBUT SEHINGGA BISA MEMOTIVASI.....

