Nama : Andri Firman Saputra

NIM : 201011402125

Kelas : 07TPLP016

Tugas : UTS – Keamanan Komputer

---

1. Data Sensitif
2. Konsep CIA adalah singkatan dari Confidentiality (Kerahasiaan), Integrity (Integritas), dan Availability (Ketersediaan). Konsep ini merupakan prinsip dasar dalam keamanan informasi dan sistem komputer yang digunakan untuk melindungi data dan sistem dari berbagai ancaman dan risiko. Berikut adalah penjelasan lebih lanjut tentang masing-masing aspek dalam konsep CIA:
   - Kerahasiaan (Confidentiality): Kerahasiaan adalah prinsip yang berkaitan dengan menjaga informasi agar tidak dapat diakses atau diungkapkan oleh pihak yang tidak memiliki hak akses. Ini berarti bahwa hanya orang yang memiliki izin atau otorisasi yang tepat dapat melihat atau menggunakan data tersebut. Teknik yang sering digunakan untuk menjaga kerahasiaan termasuk enkripsi data, pengelolaan akses yang ketat, dan kebijakan keamanan yang kuat.
   - Integritas (Integrity): Integritas berkaitan dengan memastikan bahwa data tetap utuh, tidak terubah, dan tidak dimanipulasi oleh pihak yang tidak sah. Prinsip ini menekankan bahwa data harus tetap konsisten dan akurat sepanjang siklus hidupnya. Untuk mencapai integritas data, sering digunakan teknik seperti penandaan tanda waktu (timestamping), penggunaan checksums, dan tindakan pencegahan terhadap modifikasi data yang tidak sah.
   - Ketersediaan (Availability): Ketersediaan berarti bahwa sistem dan data harus tersedia untuk digunakan oleh pengguna yang sah ketika dibutuhkan. Ini mencakup upaya untuk mencegah gangguan, pemadaman sistem, atau serangan yang dapat menghambat akses ke sistem atau data. Untuk mencapai ketersediaan, perencanaan kontinuitas bisnis, pemulihan bencana, dan redundansi sistem sering digunakan untuk memastikan bahwa data dan layanan tetap tersedia meskipun terjadi gangguan.
3. Keamanan fisik dan keamanan siber dalam sebuah data center sangat erat terkait, karena keduanya bekerja bersama untuk melindungi aset berharga, termasuk infrastruktur fisik dan data, dari berbagai ancaman dan risiko. Keamanan fisik membantu mencegah akses fisik yang tidak sah ke fasilitas data center dan melindungi perangkat keras, sementara keamanan siber menjaga data dan sistem dari serangan perangkat lunak jahat dan aktivitas siber yang

mencurigakan. Dalam kerja sama yang harmonis, keduanya membentuk lapisan perlindungan yang kuat yang memastikan keamanan, integritas, dan ketersediaan data di data center, yang sangat penting dalam menjaga operasi yang lancar dan melindungi informasi sensitif.

4. Menurut saya, CIA dalam konteks keamanan informasi merujuk pada tiga aspek utama: Confidentiality (Kerahasiaan), Integrity (Integritas), dan Availability (Ketersediaan). Setiap aspek ini dapat terganggu dari sebuah jaringan komputer, dan berikut adalah penjelasan lebih lanjut:
    - Kerahasiaan (Confidentiality):

      Alasan: Kerahasiaan adalah aspek yang berkaitan dengan melindungi informasi dari akses oleh pihak yang tidak berhak. Jika sebuah jaringan komputer terganggu, informasi sensitif dapat bocor ke tangan pihak yang tidak berhak. Hal ini dapat terjadi melalui serangan seperti peretasan (hacking), pencurian data, atau kebocoran informasi yang disebabkan oleh kesalahan konfigurasi atau ketidakamanan jaringan.
    - Integritas (Integrity):

      Alasan: Integritas berfokus pada menjaga bahwa data tetap utuh dan tidak dimanipulasi oleh pihak yang tidak berhak. Ketika jaringan terganggu, data dapat rusak atau dimodifikasi tanpa sepengetahuan atau izin pemiliknya. Serangan seperti serangan perusakan data atau serangan man-in-the-middle dapat mengancam integritas data.
    - Ketersediaan (Availability):

      Alasan: Ketersediaan berarti bahwa sistem atau layanan harus tersedia ketika dibutuhkan. Serangan yang dapat mengganggu ketersediaan meliputi serangan Denial of Service (DoS) atau Distributed Denial of Service (DDoS). Ketika jaringan terganggu, sistem atau layanan yang penting dapat menjadi tidak tersedia, yang dapat menyebabkan gangguan operasional yang serius.

    Selain ketiga aspek utama ini, ada juga tiga aspek tambahan dalam model CIA yang dapat terpengaruh oleh gangguan jaringan:

    - Authenticity (Autentikasi):

      Alasan: Autentikasi adalah tentang memastikan bahwa pihak-pihak yang berinteraksi dengan jaringan adalah yang mereka klaim. Serangan seperti serangan

phishing atau spoofing dapat mengancam autentikasi dengan memungkinkan pihak yang tidak sah untuk berpura-pura sebagai entitas yang sah.

- Non-Repudiation (Tidak Dapat Dibantah):
  Alasan: Tidak dapat dibantah berkaitan dengan memastikan bahwa pihak yang terlibat dalam komunikasi tidak dapat membantah atau menyangkal transaksi atau pesan yang mereka kirim atau terima. Serangan yang melibatkan pemalsuan tanda tangan digital atau mengabaikan catatan audit dapat mengancam aspek ini.
- Accountability (Akuntabilitas):
  Alasan: Akuntabilitas melibatkan pelacakan aktivitas dan tindakan yang dilakukan dalam jaringan, sehingga dapat mengidentifikasi siapa yang bertanggung jawab jika terjadi insiden keamanan. Jika jaringan terganggu, pelacakan dan akuntabilitas dapat menjadi sulit atau bahkan tidak mungkin.

Penting untuk memiliki strategi keamanan yang holistik dan berlapis untuk melindungi aspek-aspek ini dari gangguan jaringan. Ini melibatkan penggunaan teknologi keamanan, kebijakan keamanan, pelatihan pegawai, dan pemantauan aktif untuk mendeteksi dan merespons ancaman keamanan yang mungkin terjadi.

5. Untuk menyusun rangkaian karakter dengan menggunakan kode Huffman, langkah-langkah berikut dapat diikuti:
   - Menghitung Frekuensi Kemunculan Setiap Karakter: Pertama-tama, kita perlu menghitung berapa kali setiap karakter muncul dalam data yang diberikan. Dalam kasus Anda, data yang diberikan adalah "BDCEEDCBAADDEABACBEBBCA," jadi kita perlu menghitung berapa kali munculnya setiap karakter:
     A: 6 kali
     B: 7 kali
     C: 6 kali
     D: 3 kali
     E: 5 kali
   - Membuat Daftar Simpul Pohon Huffman: Selanjutnya, kita akan membuat daftar simpul pohon Huffman. Simpul ini akan mencakup setiap karakter bersama dengan frekuensinya. Kemudian, daftar ini akan diurutkan berdasarkan frekuensi, dengan karakter yang memiliki frekuensi terendah di bagian atas.

Karakter	Frekuensi
D	3
A	6
C	6
E	5
B	7

- Membangun Pohon Huffman:

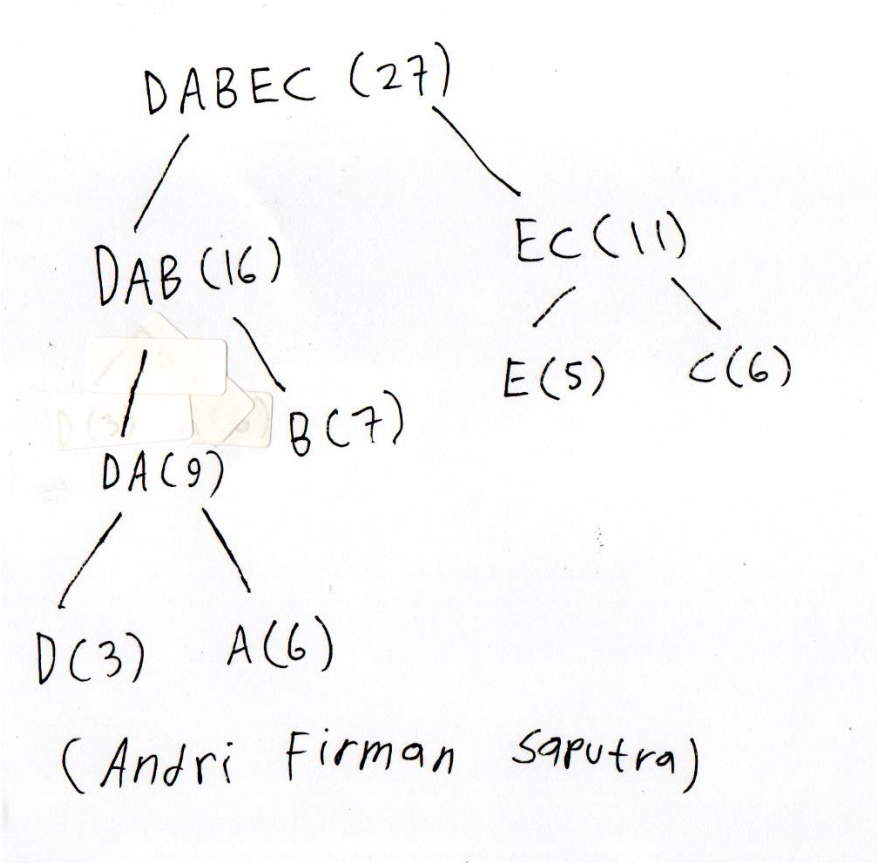
  Pohon Huffman dibangun dengan menggabungkan dua simpul dengan frekuensi terendah pada setiap langkahnya. Pohon ini akan terus berkembang hingga hanya ada satu simpul tersisa, yang merupakan akar pohon Huffman.

  Langkah 1: Gabungkan D (3) dan A (6) menjadi DA (9)

  Langkah 2: Gabungkan E (5) dan C (6) menjadi EC (11)

  Langkah 3: Gabungkan DA (9) dan B (7) menjadi DAB (16)

  Langkah 4: Gabungkan DAB (16) dan EC (11) menjadi DABEC (27)



- Mengkodekan Karakter
  - A: 01
  - B: 00
  - C: 11
  - D: 10
  - E: 11
- Mengkodekan Data Asli

  Sekarang, kita bisa mengkodekan data asli menggunakan kode Huffman yang telah dibuat. Data asli Anda "BDCEEDCBAADDEABACBEBBCA" akan menjadi:

00 10 11 11 11 10 11 01 00 10 00 11 10 00 00 11 11 01 10 00 11 00 00 00 00 11 10 01

UNIVERSITAS PAMULANG
KARTU UJIAN TENGAH SEMESTER GANJIL 2023/2024
NOMOR UJIAN : 651020129049

FAKULTAS / PRODI : ILMU KOMPUTER / TEKNIK INFORMATIKA S1

NAMA MAHASISWA : ANDRI FIRMAN SAPUTRA

NIM : 201011402125

SHIFT : REGULER A

No	Hari/ Tanggal	Waktu	Ruang	Kelas	Mata Kuliah	Paraf
1	Senin, 23 Okt 2023	07.10 - 08.50	V.754	07TPLP016	MANAJEMEN PROYEK INFORMATIKA	1
2	Senin, 23 Okt 2023	08.50 - 10.30	V.754	07TPLP016	TEKNIK RISET OPERASIONAL	2
3	Senin, 23 Okt 2023	10.30 - 12.10	V.754	07TPLP016	KEAMANAN KOMPUTER	3
4	Senin, 23 Okt 2023	13.00 - 14.40	V.754	07TPLP016	METODE NUMERIK	4
5	Selasa, 24 Okt 2023	13.00 - 14.40	V.754	07TPLP016	SISTEM PENUNJANG KEPUTUSAN	5
6	Rabu, 25 Okt 2023	07.10 - 08.50	V.754	07TPLP016	KEWIRAUSAHAAN	6
7	Rabu, 25 Okt 2023	13.00 - 14.40	V.754	07TPLP016	TESTING DAN QA PERANGKAT LUNAK	7
8	Jumat, 27 Okt 2023	10.30 - 12.10	V.754	07TPLP016	E-COMMERCE	8

Peraturan dan Tata Tertib Peserta Ujian

1. Peserta ujian harus berpakaian rapi, sopan dan memakai jaket Almamater
2. Peserta ujian sudah berada di ruangan sepuluh menit sebelum ujian dimulai
3. Peserta ujian yang terlambat diperkenankan mengikuti ujian setelah mendapat ijin, tanpa perpanjangan waktu
4. Peserta ujian hanya diperkenankan membawa alat-alat yang ditentukan oleh panitia ujian
5. Peserta ujian dilarang membantu teman, mencontoh dari teman dan tindakan-tindakan lainnya yang mengganggu peserta ujian lain
6. Peserta ujian yang melanggar tata tertib ujian dikenakan sanksi akademik

Tangerang Selatan, 23 Oktober 2023
Ketua Panitia Ujian

UBAID AL FARUQ, S.Pd., M. Pd
NIDN. 0418028702