Kelompok Unyil Kucrit:

- Yan Andhinaya Ardika (103052300062)
- Bennedict Brian Joel P (103052300066)
- Rafi Arkan Fachreza A (103052300074)
- Arkhan Falih Fahrie P (103052330051)

1. Jelaskan yang dimaksud dengan:
   a. Confidentiality
      Jawab: Properti bahwa informasi tidak tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak berwenang. Data confidentiality menjamin informasi pribadi atau rahasia tidak tersedia untuk pihak tidak sah. Privacy menjamin bahwa individu memiliki kontrol atas informasi yang dikumpulkan atau disimpan tentang dirinya serta kepada siapa informasi itu boleh diungkapkan.

   b. Integrity
      Jawab: Menjaga dan menjamin keakuratan dan kelengkapan informasi selama siklus hidupnya. Informasi tidak boleh dimodifikasi dengan cara yang tidak sah atau tidak terdeteksi.

   c. Availability
      Jawab: Menjamin bahwa sistem bekerja dengan baik dan layanan tidak ditolak untuk pengguna yang berwenang. Tujuannya untuk menghindari downtime atau gangguan layanan yang menghambat akses informasi yang sah.

   d. Authenticity
      Jawab: Properti bahwa sesuatu itu asli, dapat diverifikasi, dan dapat dipercaya. Artinya, memastikan bahwa pengguna memang benar-benar siapa yang mereka klaim dan bahwa setiap input berasal dari sumber yang terpercaya. Tujuannya untuk Mencegah pemalsuan identitas atau manipulasi asal data.

2. Jelaskan perbedaan antara RBAC, MAC dan DAC!
   Jawab:

Aspek	RBAC	MAC	DAC
Kontrol Akses oleh	Peran pengguna (jabatan/tugas)	Sistem (administrator + label)	Pemilik data
Fleksibilitas	Sedang–tinggi (tergantung kebijakan)	Rendah (ketat)	Tinggi
Cocok untuk	Organisasi, perusahaan, sistem besar	Sistem militer, keamanan tinggi	Sistem umum, personal
Contoh	Hak akses HR, Finance, IT, dan lainnya	Data classified menurut label	File sharing manual

3. Hashing
   a. Jelaskan apa yang dimaksud dengan Hasing!

Hashing adalah proses menggunakan fungsi hash untuk mengubah data berukuran sembarang menjadi nilai berukuran tetap (biasanya string angka atau heksadesimal), disebut sebagai hash value atau digest.

b. Sebutkan cara kerja hashing!
   - Input: Data masukan (contoh: teks, file, password) diberikan ke fungsi hash.
   - Proses: Fungsi hash menghitung nilai berdasarkan algoritma tertentu dan menghasilkan string tetap.
   - Output:
     Hasilnya adalah hash value unik (dalam idealnya), misalnya:
     "Hello" → 8b1a9953c4611296a827abf8c47804d7 (menggunakan MD5)

c. Sebutkan 3 contoh cryptographic hasing!
   MD5, SHA-1, SHA-2, SHA-3

4. Enkripsi-symmetric:
   a. Jelaskan apa yang dimaksud dengan Eknripsi!
      Enkripsi (Encryption) adalah proses mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma tertentu, agar data tersebut tidak bisa dipahami oleh pihak yang tidak berwenang.

   b. Jelaskan yang dimaksud dengan symmetric encryption!
      Symmetric encryption (enkripsi simetris) adalah metode enkripsi di mana kunci yang sama digunakan untuk enkripsi (mengubah plaintext menjadi ciphertext) dan dekripsi (mengubah ciphertext kembali menjadi plaintext).

   c. Sebutkan 3 contoh symmetric encryption!
      AES, Blowfish, 3DES

5. Enkripsi- asymmetric:
   a. Jelaskan perbedaan antara public key dan private key!
      Public Key adalah kunci yang dibagikan secara terbuka, digunakan untuk enkripsi.
      Private Key adalah kunci yang dibagikan secara rahasia, digunakan untuk dekripsi.

   b. Jelaskan yang dimaksud dengan asymmetric encryption!
      Asymmetric encryption (enkripsi asimetris) adalah metode kriptografi yang menggunakan dua kunci berbeda namun saling berpasangan: Public key: digunakan untuk mengenkripsi data. Private key: digunakan untuk mendekripsi data.

   c. Sebutkan 3 contoh asymmetric encryption!
      RSA, DSA, Diffie Helman Key Exchange