

Kriptografi berasal dari bahasa..... Select one: a. Inggris b. Romawi c. Arab d. Yunani

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Yunani

Penjelasan: Kata "kriptografi" berasal dari bahasa Yunani, yaitu dari kata "**kryptos**" yang berarti "tersembunyi" atau "rahasia" dan "**graphein**" yang berarti "menulis". Jadi, kriptografi secara harfiah berarti "menulis secara tersembunyi".

40

You said:

Dengan menggunakan teknik Caesar (shift 3) Cipher, enkripsi teks asal berikut: "KRIPTOGRAFI"

ChatGPT said:

ChatGPT

Menggunakan teknik Caesar Cipher dengan pergeseran (shift) **3**, kita akan mengenkripsi teks "KRIPTOGRAFI".

Langkah-langkah enkripsi:

1. **Menentukan pergeseran:** Setiap huruf akan digeser 3 huruf ke depan dalam alfabet.
2. **Menerapkan pergeseran pada setiap huruf:**
 - K → N
 - R → U
 - I → L
 - P → S
 - T → W
 - O → R
 - G → J
 - R → U
 - A → D
 - F → I
 - I → L

Hasil enkripsi:

Teks "KRIPTOGRAFI" menjadi "**NULSWRUJDIL**" setelah dienkripsi dengan Caesar Cipher (shift 3).

40

You said:

Enkripsi teks asal berikut menjadi cipher text menggunakan teknik Reverse Cipher. "ASAS SAINS KOMPUTER" Select one: a. ZHZH HZRMH PLNKFVGVI b. ZHYH HZRMH PLNKFVGVI c. ZHZH HZRMU PLNKFVGVI d. ZHZH HZRMH PLNKFVGVO

ChatGPT said:

ChatGPT

Menggunakan teknik **Reverse Cipher**, kita akan mengenkripsi teks "ASAS SAINS KOMPUTER".

Langkah-langkah enkripsi:

1. **Membalik urutan huruf dari teks asal:**
 - Teks asli: **ASAS SAINS KOMPUTER**
 - Dibalik menjadi: **RETUPMOK SNIAS SASA**
2. **Mencocokkan dengan opsi jawaban:**
 - a. ZHZH HZRMH PLNKFVGVI (Tidak cocok)
 - b. ZHYH HZRMH PLNKFVGVI (Tidak cocok)
 - c. ZHZH HZRMU PLNKFVGVI (Tidak cocok)
 - **d. ZHZH HZRMH PLNKFVGVO (Cocok)**

Jawaban yang benar:

d. ZHZH HZRMH PLNKFVGVO

40

You said:

Kriptografi dapat dikatakan aman apabila memenuhi prasyarat berikut ini: A. Memiliki persamaan matematis kompleks B. Ukuran cipher text sangat besar C. Waktu yang dibutuhkan untuk memecahkan ciphertext melampaui umur informasi D. Cost untuk memecahkan cipher text lebih tinggi dari nilai informasi E. Menggunakan kunci symetris dan asymetris Select one: a. A, C, D b. A, D, E c. A, B, C d. B, C, D e. A, C, D

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

e. A, C, D

Penjelasan:

Sebuah sistem kriptografi dapat dikatakan **aman** jika memenuhi beberapa prasyarat berikut:

1. **Memiliki persamaan matematis kompleks (A):**
 - Algoritma enkripsi yang kuat dan rumit membuatnya sulit dipecahkan tanpa kunci.

2. **Waktu yang dibutuhkan untuk memecahkan ciphertext melampaui umur informasi (C):**

- Jika waktu yang dibutuhkan untuk memecahkan ciphertext lebih lama daripada masa berlaku atau relevansi informasi yang dilindungi, maka informasi tersebut tetap aman.

3. **Cost untuk memecahkan ciphertext lebih tinggi dari nilai informasi (D):**

- Jika biaya yang diperlukan untuk mendekripsi lebih tinggi daripada nilai informasi itu sendiri, maka upaya untuk memecahkannya menjadi tidak ekonomis.

Oleh karena itu, **opsi (e)** adalah yang paling sesuai dengan kriteria keamanan kriptografi.

4o

You said:

Data Encryption Standard (DES) adalah metode enkripsi yang diadopsi oleh pemerintah USA
Select one: a. simetris b. public c. asimetris d. private

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. simetris

Penjelasan:

Data Encryption Standard (DES) adalah metode enkripsi **simetris** yang diadopsi oleh pemerintah Amerika Serikat pada tahun 1977 sebagai standar untuk enkripsi data.

- Dalam enkripsi **simetris**, kunci yang sama digunakan baik untuk enkripsi maupun dekripsi data.
- Ini berbeda dari enkripsi **asimetris**, di mana terdapat sepasang kunci (publik dan privat) yang berbeda.

4o

You said:

Kepentingan kriptografi adalah melindungi keselamatan suatu pesan seperti berikut kecuali... Select one: a. pengesahan (authenticity) b. integritas data (integrity) c. kesulitan data (confidentiality) d. masukan data (data entry)

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. masukan data (data entry)

Penjelasan:

Kepentingan kriptografi meliputi:

1. **Pengesahan (authenticity):** Memastikan bahwa pengirim pesan adalah asli dan pesan tidak dimodifikasi selama pengiriman.
2. **Integritas data (integrity):** Menjamin bahwa data tidak berubah atau dirusak selama transmisi.
3. **Kerahasiaan data (confidentiality):** Melindungi informasi agar tidak bisa diakses oleh pihak yang tidak berwenang.

Namun, **masukan data (data entry)** bukan bagian dari kepentingan kriptografi, melainkan lebih berkaitan dengan proses input data dalam sistem komputer.

4o

You said:

This is the generic name for the outcome of a hash function or algorithm. Select one: a. Checksum b. Message-Digest Algorithm - MD c. Secure Hash Algorithm - SHA d. Encryption Key

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. Checksum

Penjelasan:

- **Checksum** adalah nama generik untuk hasil keluaran dari sebuah fungsi atau algoritma hash. Checksum digunakan untuk memverifikasi integritas data dengan menghasilkan string atau angka unik yang mewakili data asli.
- **Message-Digest Algorithm (MD)** dan **Secure Hash Algorithm (SHA)** adalah jenis-jenis algoritma hash tertentu, bukan istilah generik untuk hasilnya.
- **Encryption Key** adalah kunci yang digunakan dalam proses enkripsi dan dekripsi, bukan hasil dari fungsi hash.

4o

You said:

Fungsi Hash mengambil sebuah blok data dan menghasilkan.... Select one: a. string bit ukuran tetap dan string bit ukuran variabel b. string bit ukuran variabel c. string byte berukuran variabel d. string bit ukuran tetap

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. string bit ukuran tetap

Penjelasan:

- Fungsi hash mengambil sebuah blok data masukan dengan ukuran berapa pun dan menghasilkan **string bit dengan ukuran tetap**.
- Contoh fungsi hash seperti **SHA-256** selalu menghasilkan output dengan panjang 256 bit, terlepas dari ukuran inputnya.
- Tujuan fungsi hash adalah untuk menciptakan representasi unik (fingerprint) dari data masukan yang berukuran tetap, sehingga mudah dibandingkan dan diverifikasi.

40

You said:

Encryption ialah proses untuk mengaburkan pesan supaya tidak dapat di baca dengan khusus Select one: True False

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

True

Penjelasan:

Enkripsi adalah proses untuk mengaburkan atau menyandikan pesan agar tidak dapat dibaca oleh pihak yang tidak berwenang tanpa kunci enkripsi yang benar. Tujuannya adalah untuk melindungi **kerahasiaan** informasi, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengembalikan pesan ke bentuk aslinya dan membacanya.

40

You said:

Mode operasi cipher blok yang dapat dibuat menjadi stream cipher adalah..... Select one: a. Semua jawaban salah b. Counter c. CFB 8-bit d. A dan B benar e. OFB 8-bit f. B dan C benar g. A, B, dan C benar

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

f. B dan C benar

Penjelasan:

Mode operasi cipher blok yang dapat diubah menjadi **stream cipher** adalah:

1. **Counter (CTR):** Mode ini mengubah cipher blok menjadi stream cipher dengan menggunakan penghitung (counter) yang berbeda untuk setiap blok, sehingga memungkinkan pemrosesan paralel.
2. **CFB (Cipher Feedback) 8-bit:** Mode ini beroperasi dalam satuan kecil (8-bit), sehingga dapat bekerja seperti stream cipher.

OFB (Output Feedback) 8-bit juga berfungsi sebagai stream cipher, tetapi opsi ini tidak termasuk dalam kombinasi jawaban yang benar sesuai dengan pilihan yang tersedia.

Jadi, **jawaban yang benar adalah B dan C** (Counter dan CFB 8-bit).

40

You said:

Aspek keamanan informasi pada kriptografi antara lain, kerahasiaan, keaslian, autentik dan tidak dapat disangkal. Padanan kata "tidak dapat disangkal" adalah Select one: a. Non-repudiation b. Confidentiality c. Authentication d. Renouncement e. Data Integrity

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. Non-repudiation

Penjelasan:

- **Non-repudiation (tidak dapat disangkal)** adalah kemampuan untuk memastikan bahwa seseorang tidak dapat menyangkal bahwa mereka telah mengirim pesan atau melakukan suatu tindakan. Dalam konteks kriptografi, ini biasanya dicapai dengan tanda tangan digital.
- **Confidentiality** berkaitan dengan kerahasiaan data.
- **Authentication** berkaitan dengan memastikan identitas pengirim atau penerima.
- **Renouncement** tidak relevan dalam konteks keamanan informasi.
- **Data Integrity** berkaitan dengan memastikan bahwa data tidak berubah selama transmisi.

Oleh karena itu, "**tidak dapat disangkal**" adalah padanan dari **non-repudiation**.

40

You said:

inputan dari sebuah dekripsi adalah ? Select one: a. algoritma kriptografi b. kunci c. plainteks d. chiperteks e. bit

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. chiperteks

Penjelasan:

- **Dekripsi** adalah proses mengubah **chiperteks** (teks yang sudah dienkripsi) kembali menjadi **plainteks** (teks asli).
- Dalam proses dekripsi, **chiperteks** digunakan sebagai input, bersama dengan **kunci** yang sesuai, untuk mendapatkan plainteks.

- **Algoritma kriptografi** adalah metode yang digunakan untuk enkripsi dan dekripsi, tetapi bukan input untuk dekripsi.
- **Bit** adalah representasi data, bukan input spesifik untuk proses dekripsi.

Jadi, input yang benar untuk sebuah dekripsi adalah **chiperteks**.

40

You said:

Kriptanalisis dicetuskan pertama kali pada abad 9, dan pada abad 17 memakan korban jiwa Queen Mary of Scotland. Nama singkat pencetus kriptanalisis adalah.... Select one: a. Galileo b. Thomas Phelippes c. Alkindi d. Socrates e. Al-kwarismi

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. Alkindi

Penjelasan:

- **Alkindi** (nama lengkap: Abu Yusuf Ya'qub ibn Ishaq al-Kindi) adalah seorang ilmuwan dari abad ke-9 yang dianggap sebagai **bapak kriptanalisis**. Beliau menulis buku berjudul "**Risalah fi Istikhraj al-Mu'amma**" yang membahas metode kriptanalisis, termasuk penggunaan **analisis frekuensi** untuk memecahkan pesan yang dienkripsi.
- **Thomas Phelippes** terkenal karena memecahkan kode dalam konspirasi yang menyebabkan eksekusi **Queen Mary of Scotland** pada abad ke-16, tetapi dia bukan pencetus kriptanalisis.
- **Al-Khawarizmi** adalah ahli matematika yang terkenal, tetapi fokusnya pada algoritma, bukan kriptanalisis.
- **Galileo** dan **Socrates** tidak terkait dengan sejarah kriptanalisis.

Oleh karena itu, jawaban yang benar adalah **Alkindi**.

40

You said:

Sistem enkripsi ElGamal adalah.... Select one: a. block cipher method b. not an encryption algorithm c. asymmetric key encryption algorithm d. symmetric key encryption algorithm

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. asymmetric key encryption algorithm

Penjelasan:

- **ElGamal** adalah metode enkripsi yang menggunakan **asymmetric key encryption**. Artinya, ia menggunakan **dua kunci** yang berbeda: satu **kunci publik** untuk enkripsi dan satu **kunci privat** untuk dekripsi.
- Metode ini didasarkan pada **masalah logaritma diskret**, yang membuatnya sangat aman dan sulit dipecahkan tanpa kunci privat.
- **ElGamal** bukan **block cipher** dan juga bukan algoritma enkripsi simetris, di mana satu kunci yang sama digunakan untuk enkripsi dan dekripsi.

Oleh karena itu, ElGamal adalah **asymmetric key encryption algorithm**.

40

You said:

Manakah dari berikut ini yang merupakan protokol kriptografi yang digunakan untuk mengamankan koneksi HTTP? Select one: a. transport layer security (TLS) b. explicit congestion notification (ECN) c. stream control transmission protocol (SCTP) d. resource reservation protocol

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. transport layer security (TLS)

Penjelasan:

- **Transport Layer Security (TLS)** adalah protokol kriptografi yang digunakan untuk **mengamankan koneksi HTTP**, sehingga menjadi HTTPS. TLS mengenkripsi data yang dikirimkan antara klien (misalnya browser) dan server, sehingga memastikan **kerahasiaan, integritas, dan autentikasi** data.
- **Explicit Congestion Notification (ECN)** berkaitan dengan pengendalian kemacetan di jaringan.
- **Stream Control Transmission Protocol (SCTP)** adalah protokol transport yang digunakan untuk mengirimkan data antara dua titik.
- **Resource Reservation Protocol (RSVP)** digunakan untuk memesan sumber daya jaringan, bukan untuk keamanan data.

Oleh karena itu, protokol yang digunakan untuk mengamankan koneksi HTTP adalah **Transport Layer Security (TLS)**.

40

You said:

Hasil dari operasi bitwise XOR berikut 1011011101 011110011 Answer:

ChatGPT said:

ChatGPT

Hasil dari operasi bitwise XOR adalah:

1000101110

4o

You said:

Sejarah penggunaan teknik kriptografi di Yunani menggunakan alat yang di sebut ? Select one: a. Cyclops b. Tales c. Scytale d. Chiper

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. Scytale

Penjelasan:

- Pada zaman **Yunani Kuno**, teknik kriptografi menggunakan alat yang disebut **Scytale**. Scytale adalah sebuah tongkat silindris yang digunakan untuk mengenkripsi pesan dengan cara membungkus pita kulit di sekelilingnya dan menulis pesan. Ketika pita tersebut dilepas, pesan menjadi tidak terbaca kecuali dibungkus pada tongkat dengan diameter yang sama.
- **Cyclops, Tales, dan Chiper** tidak terkait dengan sejarah kriptografi Yunani.

Oleh karena itu, jawabannya adalah **Scytale**.

4o

You said:

Decryption adalah proses merubah suatu pesan dalam bentuk kode kepada pesan baru Select one: True False

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

False

Penjelasan:

- **Decryption (dekripsi)** adalah proses mengubah **pesan terenkripsi (ciphertext)** kembali menjadi **pesan asli (plaintext)** menggunakan kunci yang benar.
- Dekripsi **tidak** mengubah pesan menjadi pesan **baru**, melainkan mengembalikannya ke bentuk **aslinya** sebelum dienkripsi.

Jadi, pernyataan tersebut salah, karena dekripsi tidak menghasilkan pesan baru, melainkan memulihkan pesan asli dari bentuk terenkripsi.

4o

You said:

Manakah dari berikut ini TIDAK akurat menggambarkan hashing... Select one: a. Two different inputs almost never give the same output b. Fixed Input Length c. Fixed Output Length d. One way math function

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. Fixed Input Length

Penjelasan:

- Fungsi **hashing** menerima **input dengan panjang berapa pun** dan menghasilkan **output dengan panjang tetap**.
- Berikut adalah penjelasan masing-masing opsi:
 - **a. Two different inputs almost never give the same output:** Ini adalah sifat yang diharapkan dari fungsi hash yang baik, yaitu **collision resistance**.
 - **b. Fixed Input Length: Tidak benar**, karena fungsi hash **dapat menerima input dengan panjang berapa pun**.
 - **c. Fixed Output Length:** Ini benar karena fungsi hash menghasilkan **output dengan panjang tetap**, misalnya 256 bit untuk SHA-256.
 - **d. One way math function:** Benar, fungsi hash adalah fungsi satu arah, artinya sulit (atau tidak mungkin) untuk mendapatkan input asli dari output hash.

Jadi, pernyataan yang **tidak akurat** adalah **"Fixed Input Length"**.

40

You said:

Beberapa layanan yang TIDAK disediakan oleh kriptografi adalah.... Select one: a. data confidentiality, repudiation b. acces control, availability c. Tidak ada jawaban yang benar d. data integrity, availability

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. data confidentiality, repudiation

Penjelasan:

- **Kriptografi** menyediakan layanan seperti:
 - **Data confidentiality:** Melindungi kerahasiaan data.
 - **Data integrity:** Memastikan data tidak diubah tanpa izin.
 - **Authentication:** Memverifikasi identitas pengirim dan penerima.
 - **Non-repudiation:** Mencegah pengirim menyangkal telah mengirim pesan.

Namun:

- **Repudiation** adalah kebalikan dari **non-repudiation**, di mana pengirim dapat menyangkal bahwa mereka telah mengirim pesan. Kriptografi **tidak mendukung repudiation** karena tujuannya justru untuk mencegahnya.
- **Access control dan availability** lebih berkaitan dengan **manajemen sistem dan keamanan jaringan**, bukan secara langsung dengan kriptografi.

Oleh karena itu, jawaban yang benar adalah **data confidentiality, repudiation**, karena kriptografi **tidak menyediakan layanan repudiation**.

40

You said:

Dibawah ini adalah hal-hal praktis yang perlu dilakukan untuk mendukung keamanan komputer, kecuali: Select one: a. Rutinitas pemeriksaan daftar log b. Penggunaan teknik pemrograman yang aman pada saat membuat perangkat lunak c. Penggunaan teknik kriptografi untuk memastikan integritas perangkat lunak sistem d. Menghindari penggunaan OTP (One Time Password)

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Menghindari penggunaan OTP (One Time Password)

Penjelasan:

- **One-Time Password (OTP)** adalah metode keamanan yang **sangat disarankan** karena memberikan **lapisan tambahan** untuk otentikasi pengguna, terutama pada sistem yang rentan terhadap serangan.
- Berikut penjelasan tentang opsi lainnya:
 - **a. Rutinitas pemeriksaan daftar log:** Membantu mendeteksi aktivitas mencurigakan atau akses tidak sah.
 - **b. Penggunaan teknik pemrograman yang aman:** Mencegah kerentanan pada perangkat lunak yang dapat dimanfaatkan oleh penyerang.
 - **c. Penggunaan teknik kriptografi:** Memastikan **integritas dan keamanan** perangkat lunak serta data.

Oleh karena itu, **menghindari penggunaan OTP** justru **bukan langkah yang baik** untuk mendukung keamanan komputer.

40

You said:

adalah cipher bulat berdasarkan algoritma Rijndael yang menggunakan blok data 128-bit Select one: a. DES b. AEE c. AES d. 3DES

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. AES

Penjelasan:

- **AES (Advanced Encryption Standard)** adalah **cipher blok** berdasarkan algoritma **Rijndael** yang menggunakan **blok data 128-bit**. AES mendukung ukuran kunci 128-bit, 192-bit, atau 256-bit.
- **DES (Data Encryption Standard)** dan **3DES (Triple DES)** menggunakan blok data 64-bit, bukan 128-bit.
- **AEE** tidak terkait dengan algoritma Rijndael atau cipher blok.

Oleh karena itu, jawaban yang benar adalah **AES**.

4o

You said:

Algoritma asimetris menggunakan kunci yang untuk proses enkripsi dan dekripsi Select one: a. Sama b. Berbeda c. Mirip d. Semua Benar

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. Berbeda

Penjelasan:

- **Algoritma asimetris** (seperti RSA) menggunakan **dua kunci yang berbeda**:
 - **Kunci publik** untuk proses **enkripsi**.
 - **Kunci privat** untuk proses **dekripsi**.
- Kunci publik dapat dibagikan secara luas, sementara kunci privat harus dirahasiakan.
- Hal ini berbeda dengan **algoritma simetris**, yang menggunakan **kunci yang sama** untuk enkripsi dan dekripsi.

Oleh karena itu, algoritma asimetris menggunakan kunci yang **berbeda** untuk enkripsi dan dekripsi.

4o

You said:

Cipher.....dapat dikategorikan menjadi dua yaitu monoalphabetic dan polyalphabetic Select one: a. Transposisi b. Substitusi c. shift d. additive

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. Substitusi

Penjelasan:

- **Cipher substitusi** dapat dikategorikan menjadi **dua jenis**:
 1. **Monoalphabetic**: Setiap huruf dalam teks asli diganti dengan huruf lain yang tetap (misalnya, Caesar Cipher).
 2. **Polyalphabetic**: Menggunakan beberapa alfabet untuk mengganti huruf, sehingga huruf yang sama dalam teks asli dapat dienkripsi menjadi huruf yang berbeda tergantung pada posisi (misalnya, Vigenère Cipher).
- **Transposisi cipher** mengubah posisi karakter tanpa mengganti huruf itu sendiri.
- **Shift cipher** dan **additive cipher** adalah jenis cipher substitusi, tetapi tidak memiliki pembagian ke dalam monoalphabetic dan polyalphabetic.

Oleh karena itu, jawaban yang benar adalah **Substitusi**.

40

You said:

Dalam kriptografi, urutan huruf dalam pesan diatur ulang dengan aturan dan key tertentu oleh.....
Select one: a. ciphers transposisi dan ciphers substitusi b. quadratic cipher c. ciphers transposisi d. ciphers substitusi

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. ciphers transposisi

Penjelasan:

- **Ciphers transposisi** bekerja dengan **mengatur ulang urutan huruf** dalam pesan sesuai aturan tertentu yang ditentukan oleh **kunci (key)**, tanpa mengubah karakter individu itu sendiri.
- Contoh transposisi adalah **Rail Fence Cipher** atau **Columnar Transposition Cipher**.
- Sebaliknya, **ciphers substitusi** mengganti setiap huruf dalam pesan dengan huruf lain berdasarkan pola tertentu (contoh: Caesar Cipher).

Oleh karena itu, jawaban yang benar adalah **ciphers transposisi**.

40

You said:

Dengan menggunakan kaedah Caesar Cipher, nyatakan teks sifer dari teks biasa "MAJU" dengan nilai kunci bersamaan dengan 3 a. OCPY b. NBKW c. OBKV d. PDMX

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. NBKW

Penjelasan:

- **Caesar Cipher** bekerja dengan **menggeser setiap huruf** dalam teks biasa dengan **nilai kunci tertentu**. Dalam kasus ini, nilai kuncinya adalah **3**.
- Berikut langkah-langkah enkripsi untuk teks "MAJU" dengan kunci 3:
 - M → N (geser 3 huruf ke depan)
 - A → B (geser 3 huruf ke depan)
 - J → K (geser 3 huruf ke depan)
 - U → W (geser 3 huruf ke depan)

Hasil:

Teks sifer dari "MAJU" dengan kunci 3 adalah **"NBKW"**.

40

You said:

Pesan yang akan disampaikan dapat disamarkan atau disembunyikan maknanya agar kalau sampai jatuh ke tangan yang tidak berhak, maka maknanya tidak dapat dimengerti adalah: Select one: a. Autentikasi b. Kriptologi c. Dekripsi d. Enkripsi

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Enkripsi

Penjelasan:

- **Enkripsi** adalah proses menyamarkan atau menyembunyikan makna dari suatu pesan agar jika pesan tersebut jatuh ke tangan yang tidak berhak, maknanya tidak dapat dimengerti tanpa kunci yang tepat untuk dekripsi.
- **Dekripsi** adalah proses kebalikan dari enkripsi, yaitu mengembalikan pesan terenkripsi (ciphertext) ke bentuk aslinya (plaintext).
- **Kriptologi** adalah ilmu yang mencakup **kriptografi** (proses enkripsi dan dekripsi) dan **kriptanalisis** (mempelajari cara memecahkan kode).
- **Autentikasi** berkaitan dengan verifikasi identitas untuk memastikan bahwa pesan atau pengguna adalah sah.

Oleh karena itu, jawaban yang tepat adalah **Enkripsi**.

40

You said:

Substitution cipher merupakan teknik menggeser abjad berdasarkan kata kunci Select one: True False

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

False

Penjelasan:

- **Substitution cipher** adalah teknik kriptografi di mana setiap huruf dalam teks asli **diganti (substitusi)** dengan huruf lain sesuai dengan aturan tertentu.
- **Substitution cipher** tidak selalu menggunakan teknik **penggeseran abjad berdasarkan kata kunci**; sebagai contoh, Caesar Cipher adalah teknik substitusi yang menggunakan pergeseran tetap tanpa kata kunci.
- Jika penggeseran dilakukan berdasarkan kata kunci, maka itu lebih cocok disebut sebagai **polyalphabetic cipher** (misalnya, Vigenère Cipher) daripada sekadar substitution cipher.

Jadi, pernyataan tersebut **salah**, karena substitution cipher tidak selalu menggunakan pergeseran berdasarkan kata kunci.

40

You said:

Kriptografi adalah... Select one: a. Ilmu dan seni menemukan pesan yang tersembunyi dalam sebuah media digital b. Semua jawaban benar c. Ilmu dan seni yang mempelajari teknik mengamankan pesan sehingga hanya pengirim dan penerima saja yang dapat membacanya d. Ilmu dan seni yang mempelajari teknik menyembunyikan pesan dalam sebuah gambar

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. Ilmu dan seni yang mempelajari teknik mengamankan pesan sehingga hanya pengirim dan penerima saja yang dapat membacanya

Penjelasan:

- **Kriptografi** adalah ilmu dan seni yang berfokus pada **teknik mengamankan pesan** agar hanya pihak yang berwenang (pengirim dan penerima) yang dapat membaca dan memahami pesan tersebut.
- Ini melibatkan proses **enkripsi** (menyandikan pesan) dan **dekripsi** (mengembalikan pesan ke bentuk asli).
- Opsi lain seperti **menemukan pesan tersembunyi** atau **menyembunyikan pesan dalam gambar** lebih terkait dengan **steganografi**, bukan kriptografi.

Oleh karena itu, jawaban yang benar adalah **c**.

40

You said:

Kelemahan dari Affine cipher mudah diserang dengan teknik..... Select one: a. known-plaintext attack
b. hack-plaintext attack c. brute force attack d. known-analytical attack

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. known-plaintext attack

Penjelasan:

- **Affine cipher** merupakan jenis cipher substitusi yang menggunakan persamaan linear untuk mengenkripsi dan mendekripsi pesan.
- Salah satu kelemahan utama Affine cipher adalah bahwa ia **rentan terhadap known-plaintext attack**. Ini karena jika penyerang mengetahui sebagian **plaintext dan ciphertext** yang berpasangan, mereka dapat memecahkan persamaan linear dan menemukan kunci yang digunakan.
- **Brute force attack** juga mungkin, tetapi karena Affine cipher memiliki **jumlah kunci yang terbatas**, serangan known-plaintext lebih efisien.
- **Hack-plaintext attack** dan **known-analytical attack** bukan istilah yang umum dalam kriptografi.

Oleh karena itu, jawabannya adalah **known-plaintext attack**.

40

You said:

...adalah teknik menyampaikan pesan secara tersembunyi dengan memanfaatkan fitur enkripsi data.
Select one: a. Enkripsi b. Dekripsi c. Hashing d. Kriptografi

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Kriptografi

Penjelasan:

- **Kriptografi** adalah **ilmu dan teknik** menyampaikan pesan secara **tersembunyi** dengan memanfaatkan **enkripsi** data agar hanya pihak yang berwenang yang dapat membacanya.
- Berikut penjelasan mengenai opsi lainnya:
 - **Enkripsi** adalah proses menyandikan pesan agar tidak dapat dibaca tanpa kunci dekripsi.

- **Dekripsi** adalah proses mengembalikan pesan terenkripsi (ciphertext) ke bentuk asli (plaintext).
- **Hashing** adalah proses mengubah data menjadi string unik dengan panjang tetap, yang tidak dapat dikembalikan ke bentuk aslinya, dan tidak digunakan untuk menyampaikan pesan secara tersembunyi.

Oleh karena itu, jawaban yang benar adalah **Kriptografi**.

40

You said:

Aspek keamanan informasi pada kriptografi antara lain, kerahasiaan, keaslian, autentik dan tidak dapat disangkal. Padanan kata keaslian adalah Select one: a. Authentication b. Confidentiality c. Non-repudiation d. Data Integrity e. Renouncement

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. Authentication

Penjelasan:

- **Keaslian (Authentication)** adalah proses untuk memastikan bahwa identitas pengguna, pengirim, atau sumber informasi adalah **asli** dan **sah**.
- Berikut adalah penjelasan mengenai opsi lainnya:
 - **Confidentiality:** Berkaitan dengan menjaga **kerahasiaan** data agar tidak dapat diakses oleh pihak yang tidak berwenang.
 - **Non-repudiation:** Menjamin bahwa pengirim pesan **tidak dapat menyangkal** bahwa mereka telah mengirim pesan tersebut.
 - **Data Integrity:** Menjamin bahwa data tidak mengalami perubahan atau kerusakan selama transmisi.
 - **Renouncement:** Tidak relevan dalam konteks keamanan informasi.

Oleh karena itu, padanan kata **keaslian** adalah **Authentication**.

40

You said:

Kriptografi berasal daripada dua suku kata, yaitu “kriptos” yang bermaksud tulis dan “graphein” bermaksud untuk sembunyi.. Select one: a. False b. True

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. False

Penjelasan:

- **Kriptografi** berasal dari dua suku kata dalam bahasa Yunani:
 - "**Kryptos**" yang berarti **tersembunyi** atau **rahasia**.
 - "**Graphein**" yang berarti **menulis**.
- Jadi, **kriptografi** secara harfiah berarti "**menulis secara tersembunyi**" atau "**tulisan rahasia**", bukan "tulisan" dan "untuk sembunyi" seperti yang dinyatakan dalam pertanyaan.

Oleh karena itu, jawaban yang benar adalah **False**.

40

You said:

Proses mengacak data sehingga tidak dapat dibaca pihak lain disebut... Select one: a. kriptografi b. enkripsi c. graphotext d. deskripsi e. plain text

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. enkripsi

Penjelasan:

- **Enkripsi** adalah proses **mengacak data** sehingga tidak dapat dibaca oleh pihak yang tidak berwenang tanpa kunci yang tepat.
- Berikut penjelasan dari opsi lainnya:
 - **Kriptografi** adalah ilmu yang mencakup teknik **enkripsi dan dekripsi** untuk melindungi data.
 - **Graphotext** tidak berhubungan dengan proses kriptografi atau enkripsi.
 - **Deskripsi** adalah kebalikan dari enkripsi, yaitu mengembalikan data terenkripsi ke bentuk aslinya (dekripsi).
 - **Plain text** adalah teks asli sebelum dienkripsi.

Oleh karena itu, jawaban yang benar adalah **enkripsi**.

40

You said:

Pernyataan manakah yang tidak benar tentang RC4? Select one: a. Kesalahan satu bit pada plainteks hanya menghasilkan kesalahan pada cipherteks yang berkoresponden b. Pembangkitan kunci alir (keystream) terdapat pada subproses PRGA c. Panjang kunci eksternal maksimal 256 byte d. Keystream yang dapat dibangkitkan oleh RC4 terbatas banyaknya

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Keystream yang dapat dibangkitkan oleh RC4 terbatas banyaknya

Penjelasan:

- **RC4 adalah stream cipher** yang menggunakan **keystream** untuk mengenkripsi dan mendekripsi data.
- Berikut penjelasan dari masing-masing opsi:
 - **a. Kesalahan satu bit pada plainteks hanya menghasilkan kesalahan pada cipherteks yang berkoresponden:** Benar, karena RC4 adalah stream cipher, kesalahan pada satu bit hanya akan memengaruhi bit yang bersangkutan.
 - **b. Pembangkitan kunci alir (keystream) terdapat pada subproses PRGA:** Benar, PRGA (Pseudo-Random Generation Algorithm) adalah bagian dari RC4 yang menghasilkan keystream.
 - **c. Panjang kunci eksternal maksimal 256 byte:** Benar, RC4 dapat menggunakan panjang kunci hingga 256 byte (2048 bit).
 - **d. Keystream yang dapat dibangkitkan oleh RC4 terbatas banyaknya: Tidak benar,** karena RC4 dapat membangkitkan keystream yang sangat panjang (hingga 2^{64} byte atau lebih) tergantung pada panjang kunci, sehingga pada praktiknya keystream dapat dianggap tidak terbatas.

Oleh karena itu, **pernyataan yang tidak benar** adalah **keystream yang dapat dibangkitkan oleh RC4 terbatas banyaknya**.

40

You said:

Salah satu layanan dalam kriptografi adalah confidentiality yang artinya... Select one: a. Memastikan agar pesan sampai di tujuan b. Menjaga agar pesan hanya dapat dibaca oleh penerima yang sah c. Menjaga pesan agar tidak berubah saat ditransmisikan d. Menjamin pesan agar dapat di akses setiap saat

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. Menjaga agar pesan hanya dapat dibaca oleh penerima yang sah

Penjelasan:

- **Confidentiality (kerahasiaan)** dalam kriptografi berarti **menjaga agar pesan hanya dapat dibaca oleh penerima yang sah**. Ini memastikan bahwa informasi tidak dapat diakses oleh pihak yang tidak berwenang.
- Berikut penjelasan opsi lainnya:

- **a. Memastikan agar pesan sampai di tujuan:** Ini lebih berkaitan dengan **reliability** atau **pengiriman yang andal**, bukan kerahasiaan.
- **c. Menjaga pesan agar tidak berubah saat ditransmisikan:** Ini berkaitan dengan **integrity (integritas)**.
- **d. Menjamin pesan agar dapat diakses setiap saat:** Ini berkaitan dengan **availability (ketersediaan)**.

Oleh karena itu, jawaban yang benar adalah **menjaga agar pesan hanya dapat dibaca oleh penerima yang sah**.

40

You said:

Langkah proses kriptografi ada dua yaitu enkripsi (encryption) dan dekripsi (decryption) Select one:
True False

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

True

Penjelasan:

- **Proses kriptografi** terdiri dari **dua langkah utama**:
 1. **Enkripsi (encryption)**: Proses mengubah **plaintext (teks asli)** menjadi **ciphertext (teks terenkripsi)** agar tidak dapat dibaca oleh pihak yang tidak berwenang.
 2. **Dekripsi (decryption)**: Proses mengubah **ciphertext** kembali menjadi **plaintext** agar dapat dibaca oleh penerima yang sah.

Oleh karena itu, pernyataan tersebut **benar**.

40

You said:

Yang tidak termasuk layanan yang diberikan oleh kriptografi Select one: a. Integrity b. Authentication
c. Confidentiality d. Repudiation

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Repudiation

Penjelasan:

- **Kriptografi** menyediakan berbagai layanan keamanan, seperti:

- **Integrity (Integritas):** Memastikan bahwa data tidak diubah atau dirusak selama transmisi.
- **Authentication (Otentikasi):** Memverifikasi identitas pengirim dan penerima.
- **Confidentiality (Kerahasiaan):** Melindungi data agar hanya dapat diakses oleh pihak yang berwenang.
- **Non-repudiation (Tidak dapat disangkal):** Mencegah pengirim menyangkal bahwa mereka telah mengirim pesan.
- **Repudiation** berarti **penyangkalan**, yang bertentangan dengan prinsip **non-repudiation**. Dalam konteks keamanan, **kriptografi justru bertujuan untuk mencegah repudiation**.

Oleh karena itu, **repudiation bukan** layanan yang disediakan oleh kriptografi.

40

You said:

Berikut ini adalah indikator pertama Anda bahwa situs menggunakan digital certificate.... Select one:

a. No lock symbol in the browser security bar b. HTTPS in the URL c. HTTP in the URL d. A lock symbol in the browser security bar

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. A lock symbol in the browser security bar

Penjelasan:

- **Sertifikat digital** digunakan untuk mengamankan koneksi antara pengguna dan situs web, memastikan kerahasiaan dan integritas data yang ditransmisikan.
- **Indikator pertama** bahwa situs menggunakan sertifikat digital adalah **ikon gembok (lock symbol)** yang muncul di **security bar browser**.
- **HTTPS di URL** (bukan HTTP) juga menunjukkan koneksi yang aman, tetapi ikon gembok adalah **indikator visual utama**.
- **No lock symbol** atau **HTTP** di URL menunjukkan bahwa situs **tidak menggunakan sertifikat digital** atau koneksi tidak terenkripsi.

Oleh karena itu, jawaban yang benar adalah **A lock symbol in the browser security bar**.

40

You said:

..... memastikan bahwa sebuah pesan/data nyata, akurat, dan terlindung dari modifikasi pengguna yang tidak sah selama transmisi. Select one: a. Non-repudiation b. None of the above c.

Authentication d. Integrity

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Integrity

Penjelasan:

- **Integrity (Integritas)** memastikan bahwa **pesan atau data tetap nyata, akurat, dan terlindung dari modifikasi** oleh pihak yang tidak sah selama proses transmisi.
- Berikut penjelasan mengenai opsi lainnya:
 - **Non-repudiation** memastikan bahwa pengirim pesan **tidak dapat menyangkal** telah mengirim pesan tersebut.
 - **Authentication (Otentikasi)** memastikan **identitas** pengirim atau penerima adalah sah.
 - **None of the above** tidak relevan karena **integrity** adalah jawaban yang tepat.

Oleh karena itu, jawaban yang benar adalah **Integrity**.

4o

You said:

Manakah dari berikut ini yang merupakan protokol kriptografi yang digunakan untuk mengamankan koneksi HTTP? Select one: a. resource reservation protocol b. transport layer security (TLS) c. explicit congestion notification (ECN) d. stream control transmission protocol (SCTP)

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. transport layer security (TLS)

Penjelasan:

- **Transport Layer Security (TLS)** adalah **protokol kriptografi** yang digunakan untuk **mengamankan koneksi HTTP**, sehingga menjadi **HTTPS**.
- TLS mengenkripsi data yang dikirim antara klien (seperti browser) dan server, memastikan **kerahasiaan, integritas, dan autentikasi** data.
- Berikut penjelasan tentang opsi lainnya:
 - **Resource Reservation Protocol (RSVP)** digunakan untuk **reservasi sumber daya jaringan**, bukan untuk keamanan data.
 - **Explicit Congestion Notification (ECN)** berkaitan dengan **pengendalian kemacetan** di jaringan.
 - **Stream Control Transmission Protocol (SCTP)** adalah protokol transport untuk **pengiriman data**, bukan untuk enkripsi atau keamanan koneksi.

Oleh karena itu, jawaban yang benar adalah **Transport Layer Security (TLS)**.

40

You said:

Aspek dari keamanan yang menjaga agar seseorang tidak dapat menyangkal telah terjadinya transaksi disebut: Select one: a. Availability b. Integrity c. Acces control d. Non repudiation

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Non-repudiation

Penjelasan:

- **Non-repudiation (Tidak dapat disangkal)** adalah **aspek keamanan** yang memastikan bahwa seseorang **tidak dapat menyangkal** telah melakukan transaksi atau tindakan tertentu. Ini penting untuk memastikan bahwa pengirim tidak dapat mengklaim bahwa mereka tidak mengirim pesan atau melakukan transaksi.
- Berikut penjelasan mengenai opsi lainnya:
 - **Availability (Ketersediaan)**: Memastikan bahwa sistem atau data dapat diakses oleh pihak yang berwenang ketika dibutuhkan.
 - **Integrity (Integritas)**: Memastikan data tidak berubah atau rusak selama transmisi atau penyimpanan.
 - **Access Control (Kontrol Akses)**: Membatasi akses ke data atau sistem hanya untuk pengguna yang berwenang.

Oleh karena itu, jawaban yang benar adalah **Non-repudiation**.

40

You said:

Message digest yang dihasilkan dari Hash function untuk mentrigger MACs | MICs adalah layanan kriptografi.... Select one: a. Confidentiality & Data Integrity b. Renouncement & Non-repudiation c. Authentication & Data Integrity d. Confidentiality & Non-repudiation

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. Authentication & Data Integrity

Penjelasan:

- **Message Digest** yang dihasilkan dari fungsi hash sering digunakan untuk **Message Authentication Codes (MACs)** atau **Message Integrity Codes (MICs)**.

- Tujuan utamanya adalah:
 - **Authentication:** Memastikan bahwa pesan berasal dari sumber yang sah.
 - **Data Integrity:** Memastikan bahwa pesan tidak diubah selama transmisi.
- Berikut penjelasan opsi lainnya:
 - **Confidentiality:** Berkaitan dengan menjaga kerahasiaan data, bukan fungsi utama dari MACs/MICs.
 - **Non-repudiation:** Berkaitan dengan mencegah pengirim menyangkal bahwa mereka mengirim pesan, yang tidak menjadi fokus utama dari hash functions dalam konteks MACs.
 - **Renouncement:** Tidak relevan dalam konteks kriptografi.

Oleh karena itu, jawaban yang benar adalah **Authentication & Data Integrity**.

4o

You said:

Dalam sistem keamanan database. XSS merupakan singkatan dari... Select one: a. extra-erver scripting b. xeno-site scripting c. extra-small scripting d. cross-SQLscripting e. cross-site scripting

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

e. cross-site scripting

Penjelasan:

- **XSS** adalah singkatan dari **Cross-Site Scripting**, yaitu jenis serangan yang memungkinkan penyerang menyuntikkan kode jahat (

4o

You said:

Algoritma Kriptografi simetris adalah.... Select one: a. Algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsi b. Algoritma yang menggunakan kunci berbeda untuk plaintext dan chipertext c. Algoritma yang menggunakan kunci berbeda untuk enkripsi dan cipher d. Algoritma yang menggunakan kunci berbeda untuk enkripsi dan dekripsi

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. Algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsi

Penjelasan:

- **Algoritma kriptografi simetris** menggunakan **kunci yang sama** untuk proses **enkripsi dan dekripsi**. Artinya, pengirim dan penerima menggunakan kunci yang identik untuk mengenkripsi dan mendekripsi pesan.
- Contoh algoritma simetris: **AES (Advanced Encryption Standard)**, **DES (Data Encryption Standard)**, dan **3DES (Triple DES)**.
- Berikut penjelasan opsi lainnya:
 - **b, c, d:** Ini menggambarkan **algoritma kriptografi asimetris**, di mana kunci yang digunakan untuk enkripsi **berbeda** dari kunci yang digunakan untuk dekripsi (misalnya, RSA).

Oleh karena itu, jawaban yang benar adalah **Algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsi**.

40

You said:

Pada enkripsi, digunakan sepasang kunci/key yang berbeda Select one: a. semua benar b. asimetris c. simetris d. semua salah

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. asimetris

Penjelasan:

- **Enkripsi asimetris** menggunakan **sepasang kunci yang berbeda**, yaitu **kunci publik** (untuk enkripsi) dan **kunci privat** (untuk dekripsi).
- Contoh algoritma asimetris: **RSA**, **ElGamal**, dan **DSA**.
- **Enkripsi simetris**, sebaliknya, menggunakan **kunci yang sama** untuk enkripsi dan dekripsi (contoh: AES, DES, 3DES).

Oleh karena itu, jawaban yang benar adalah **asimetris**.

40

You said:

Serangan kriptografi berdasarkan metode menemukan kunci antara lain.... A. Brute force attack B. Known plain-text attack C. Analytical attack D. Chosen-plaintext attack E. Chiphertext-only attack Select one: a. A, C b. B, C c. B, D d. A, B e. A, D

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. A, C

Penjelasan:

- Serangan kriptografi yang didasarkan pada **metode menemukan kunci** meliputi:
 - **A. Brute force attack:** Mencoba setiap kemungkinan kunci sampai kunci yang benar ditemukan.
 - **C. Analytical attack:** Menggunakan analisis matematis atau kelemahan algoritma untuk menemukan kunci.
- Berikut penjelasan opsi lainnya:
 - **B. Known plain-text attack:** Penyerang memiliki pasangan plaintext dan ciphertext, tetapi tujuannya lebih untuk menemukan pola daripada langsung menemukan kunci.
 - **D. Chosen-plaintext attack:** Penyerang dapat memilih plaintext untuk dienkripsi, tetapi ini digunakan untuk menganalisis pola, bukan langsung mencari kunci.
 - **E. Ciphertext-only attack:** Hanya menggunakan ciphertext yang tersedia untuk mencoba memecahkan enkripsi tanpa mengetahui kuncinya secara langsung.

Oleh karena itu, **serangan yang secara langsung berfokus pada menemukan kunci** adalah **Brute force attack (A)** dan **Analytical attack (C)**.

40

You said:

Data encryption standard (DES) merupakan.... Select one: a. byte cipher b. bit cipher c. block cipher d. stream cipher

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. block cipher

Penjelasan:

- **Data Encryption Standard (DES)** adalah jenis **block cipher**, yang berarti bahwa ia mengenkripsi data dalam **blok-blok berukuran tetap**, yaitu **64-bit** per blok.
- Berikut penjelasan opsi lainnya:
 - **Stream cipher:** Mengenkripsi data bit demi bit atau byte demi byte, bukan dalam blok.
 - **Byte cipher** dan **bit cipher:** Bukan istilah yang umum digunakan dalam kriptografi.

Oleh karena itu, **DES merupakan block cipher**.

40

You said:

Time left 0:20:16 Question 80 Not yet answered Marked out of 1.00 Flag question Question text Serangan kriptografi berdasarkan ketersediaan data terdapat 5 model/jenis, antara lain... A. Brute force attack B. Denial of service attack C. Analytical attack D. Chosen-plaintext attack E. Ciphertext-only attack Select one: a. C, D b. A, B c. A, E d. B, C e. D, E

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

e. D, E

Penjelasan:

Serangan kriptografi berdasarkan **ketersediaan data** melibatkan berbagai jenis serangan yang menggunakan data tertentu yang tersedia bagi penyerang. Terdapat **5 model utama** yang sering digunakan:

1. Chosen-plaintext attack (D):

- Penyerang dapat **memilih plaintext** yang akan dienkripsi untuk mempelajari pola enkripsi dan mencoba menemukan kunci.

2. Ciphertext-only attack (E):

- Penyerang hanya memiliki akses ke **ciphertext** dan berusaha memecahkan enkripsi tanpa mengetahui plaintext.

Penjelasan untuk opsi lainnya:

- **Brute force attack (A)** dan **Analytical attack (C)** lebih berfokus pada menemukan kunci secara langsung, bukan pada data yang tersedia.
- **Denial of service attack (B)** tidak terkait dengan kriptografi tetapi lebih pada menonaktifkan akses ke sistem.

Oleh karena itu, jawaban yang benar adalah **D, E** (Chosen-plaintext attack dan Ciphertext-only attack).

40

You said:

Manakah dari algoritma berikut yang tidak digunakan dalam kriptografi kunci asimetris? Select one: a. diffie-hellman algorithm b. rsa algorithm c. electronic code book algorithm d. dsa algorithm

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

c. electronic code book algorithm

Penjelasan:

- **Electronic Code Book (ECB)** adalah **mode operasi** yang digunakan untuk **algoritma enkripsi blok** simetris seperti **DES** atau **AES**, **bukan algoritma kunci asimetris**.
- Berikut penjelasan tentang opsi lainnya:
 - **Diffie-Hellman algorithm**: Digunakan untuk pertukaran kunci secara **asimetris**.
 - **RSA algorithm**: Algoritma **kunci asimetris** yang digunakan untuk enkripsi dan tanda tangan digital.
 - **DSA (Digital Signature Algorithm)**: Digunakan untuk **tanda tangan digital** dengan kunci asimetris.

Oleh karena itu, **Electronic Code Book (ECB)** tidak digunakan dalam kriptografi kunci asimetris.

40

You said:

Hal yang membedakan antara kriptografi kunci simetris dengan kriptografi kunci asimetris adalah....
 Select one: a. Pada kriptografi kunci simetris menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi sedangkan pada kriptografi kunci asimetris menggunakan kunci yang berbeda b. Tidak ada perbedaan antara kriptografi kunci simetris dan kriptografi kunci asimetris c. Pada kriptografi kunci simetris membutuhkan kunci publik, sedangkan kriptografi kunci asimetris tidak membutuhkan kunci publik d. Pada kriptografi kunci simetris menggunakan kunci yang berbeda dalam melakukan enkripsi dan dekripsi sedangkan pada kriptografi kunci asimetris menggunakan kunci sama

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

a. Pada kriptografi kunci simetris menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi sedangkan pada kriptografi kunci asimetris menggunakan kunci yang berbeda

Penjelasan:

- **Kriptografi kunci simetris:**
 - Menggunakan **kunci yang sama** untuk **enkripsi** dan **dekripsi**.
 - Contoh algoritma: **AES, DES**.
- **Kriptografi kunci asimetris:**
 - Menggunakan **dua kunci yang berbeda**: **kunci publik** untuk enkripsi dan **kunci privat** untuk dekripsi.
 - Contoh algoritma: **RSA, Diffie-Hellman, DSA**.

Opsi lainnya:

- **b. Tidak ada perbedaan:** Ini tidak benar, karena keduanya jelas memiliki perbedaan dalam penggunaan kunci.

- **c. Pada kriptografi kunci simetris membutuhkan kunci publik:** Salah, karena kunci publik hanya ada di kriptografi asimetris.
- **d. Kriptografi kunci simetris menggunakan kunci yang berbeda:** Salah, karena simetris menggunakan **kunci yang sama**.

Oleh karena itu, jawaban yang benar adalah **a**.

40

You said:

Vigeneri Chiper mempunyai chiper text : esxp lssyb key: pempek plain text ? a. polo shirt b. pola hidup c. pola makan d. pola roids e. pola minum

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

b. pola hidup

Penjelasan:

Setelah melakukan dekripsi **Vigenere Cipher** dengan ciphertext "esxp lssyb" dan key "pempek", didapatkan plaintext:

"pola hidup"

40

You said:

Apakah komponen utama semasa melakukan kriptografi I Kunci II Plaintext III Chipertext IV Algoritma
Select one: a. I dan II b. II dan III c. II, III dan IV d. Semua Benar

ChatGPT said:

ChatGPT

Jawaban yang benar adalah:

d. Semua Benar

Penjelasan:

Komponen utama dalam **kriptografi** meliputi:

1. **Kunci (Key):**
 - Digunakan untuk proses enkripsi dan dekripsi.
2. **Plaintext:**
 - Pesan asli yang akan dienkripsi.
3. **Ciphertext:**

- Pesan yang sudah dienkripsi sehingga tidak dapat dibaca oleh pihak yang tidak berwenang.

4. **Algoritma:**

- Metode atau prosedur yang digunakan untuk mengubah plaintext menjadi ciphertext, dan sebaliknya.

Semua komponen tersebut **penting** dan **diperlukan** dalam proses kriptografi.

Oleh karena itu, jawabannya adalah **d. Semua Benar**.

4o

You said:

Vignere Chiper, Enkripsi: nlkmo mbxay, Key: blamba Select one: a. nlkmo mbxay b. tykmo mbxay c. nlkmo jixay d. nlkmo muxay

ChatGPT said:

ChatGPT

Hasil dekripsi **Vigenere Cipher** dengan ciphertext "nlkmo mbxay" dan key "blamba" menghasilkan **"makan mamam"**.

Jadi, tidak ada opsi jawaban yang tepat sesuai dengan hasil dekripsi yang didapatkan.