

2.1 Kriptografi dalam Keselamatan Data

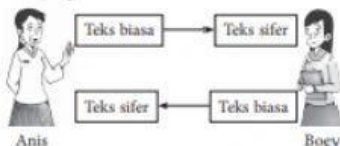
- _____ adalah sains dan seni menukarkan maklumat kepada bentuk yang selamat dan tidak mudah dicerobohi.
A Kriptografi
B Steganografi
C Kriptoanalisis
D Keselamatan siber
- Apakah item yang diperlukan untuk menyulit atau menyahsulit mesej rahsia?
A Kata laluan (*Password*)
B Kunci sifer (*Cipher key*)
C Sijil digital (*Digital certificate*)
D Tandatangan-e (*e-signature*)
- Apakah yang dimaksudkan dengan istilah sifer (*cipher*)?
A Mesej yang disulitkan.
B Keselamatan komputer.
C Algoritma untuk menukar teks biasa kepada teks sifer.
D Kajian kaedah-kaedah menyulit dan menyahsulit mesej rahsia.
- Chee Meng menerima mesej rahsia "ERAILGHAUAAZKABG" dalam peti suratnya. Beliau tahu bahawa mesej ini disulitkan dengan *Columnar Transposition*. Oleh itu, Chee Meng melukis jadual transposisi untuk menyahsulit mesej rahsia yang diterimanya.

Kunci sifer	?	?	?	?
	K	E	L	U
	A	R	G	A
	B	A	H	A
	G	I	A	Z

Antara yang berikut, yang manakah kunci sifer yang digunakan jika Chee Meng mendapati mesej asal ialah "KELUARGA BAHAGIA"?

- A CUBA C PETI
B NOTA D TEKS

- Apakah yang dimaksudkan fungsi integriti dalam perkhidmatan keselamatan data kriptografi?
A Pengesahan identiti pengirim dan penerima mesej.
B Perlindungan kerahsiaan mesej semasa dihantar kepada penerima.
C Kepastian isi kandungan mesej tidak diubah semasa dihantar kepada penerima.
D Kepastian pengirim dan penerima tidak boleh menafikan mereka adalah pihak yang menghantar dan menerima sesuatu mesej.
- Apakah nama bagi sistem sifer yang menyusun semula aksara-aksara dalam mesej biasa untuk menghasilkan teks sifer?
A *Reverse Cipher*
B *Encryption Cipher*
C *Substitution Cipher*
D *Transposition Cipher*
- Anis dan Boey saling bertukar mesej rahsia dengan menggunakan satu sistem sifer yang berdasarkan kunci asimetri.



Apakah yang diperlukan oleh Anis untuk menyahsulit mesej rahsia yang dihantar oleh Boey?

- A Kunci awam Boey.
B Kunci awamnya sendiri.
C Kunci persendirian Boey.
D Kunci persendirianya sendiri.

- Antara yang berikut, yang manakah teks *Pigpen cipher* setelah ditukarkan dari perkataan MALAYSIA?

- M A L A Y S I A
- A        
- B        
- C        
- D        

- Apakah nama bagi sistem sifer yang menggantikan setiap aksara dengan simbol grafik?

- A *Pigpen Cipher*
B *Caesar Cipher*
C *Reverse Cipher*
D *Transposition Cipher*

- Rina menggunakan *Rail Fence Cipher* untuk menyulitkan mesej "CARI DALAM PETI SEJUK". Rajah berikut menunjukkan "pagar" yang digunakan oleh Rina. Nyatakan teks sifer yang dihasilkan oleh Rina.

C						L								I						X
	A					A								T		S				K
		R				D								M		E				U
						I								P						J

- A CLIXKSTAAARDMEEUJPI
B CLIXAAATSKRDMEEUIPJ
C XILCKSTAAAUUEMDRJPI
D XKUJESITEPMALADIRAC

- Teliti situasi di bawah.

Ali ingin menyulitkan satu mesej yang mengandungi 36 aksara. Dia bercadang menggunakan *Columnar Transposition* dan perkataan "SULIT" sebagai kunci. Ali perlu melukis satu jadual untuk mengisi mesej asalnya.

Berdasarkan situasi ini, berapakah lajur dan baris perlu disediakan oleh Ali untuk diletakkan dalam jadual?

- A 5 lajur, 7 baris
B 5 lajur, 8 baris
C 6 lajur, 6 baris
D 6 lajur, 7 baris

- Apakah jenis *Reverse Cipher* yang telah digunakan untuk menyulitkan mesej berikut di bawah?

PENJARAKAN SOSIAL

(Teks biasa)

↓ penyulitan

KVMQZIZPZM HJHRZO

(Teks sifer)

- A Songsangan abjad
B Songsangan tulisan
C Songsangan perkataan
D Songsangan seluruh mesej