Nama : Mitra Hasibuan

Npm : 180840021

1. Apa yang dimaksud dengan:

* Cipher Substitusi adalah [cipher](http://itjambi.com/cipher/) dengan cara mensubstitusi huruf dengan huruf yang lain sesuai dengan yang ditetapkan.
* Kriptosistem adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya.
* **Cryptanalysis** adalah suatu ilmu dan seni membuka (breaking) ciphertext dan orang yang melakukannya disebut **cryptanalyst**.
* Simetri Kriptosistem adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.
* Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.
* Stegonografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.
* Plaintext adalah teks informasi yang merupakan masukan bagi suatu algoritme enkripsi dalam format ASCII.
* Kunci Public adalah kunci yang dapat disebarluaskan secara luas.

1. Jelaskan ancaman keamana apa saja yang mungkin terjadi pada komputer yang terkoneksi ke jaringan

* [Probe](https://id.wikipedia.org/w/index.php?title=Probe&action=edit&redlink=1) :Probe atau yang biasa disebut probing adalah usaha untuk mengakses sistem dan mendapatkan informasi tentang sistem
* [Scan](https://id.wikipedia.org/w/index.php?title=Scan&action=edit&redlink=1): Scan adalah probing dalam jumlah besar menggunakan suatu tool
* [Account compromise](https://id.wikipedia.org/w/index.php?title=Account_compromise&action=edit&redlink=1): Meliputi User compromize dan root compromize
* [Packet Snifer](https://id.wikipedia.org/w/index.php?title=Packet_Snifer&action=edit&redlink=1): Adalah sebuah program yang menangkap data dari paket yang lewat di jaringan. (username, password, dan informasi penting lainnya)
* [Hacking](https://id.wikipedia.org/w/index.php?title=Hacking&action=edit&redlink=1) : Hacking adalah tindakan memperoleh akses ke komputer atau jaringan komputer untuk mendapatkan atau mengubah informasi tanpa otorisasi yang sah
* [Denial-of-Service](https://id.wikipedia.org/w/index.php?title=Denial-of-Service&action=edit&redlink=1): Serangan Denial-of-service (DoS) mencegah pengguna yang sah dari penggunaan layanan ketika pelaku mendapatkan akses tanpa izin ke mesin atau data. Ini terjadi karena pelaku membanjiri jaringan dengan volume data yang besar atau sengaja menghabiskan sumber daya yang langka atau terbatas, seperti process control blocks atau koneksi jaringan yang tertunda. Atau mereka mengganggu komponen fisik jaringan atau memanipulasi data yang sedang dikirimkan, termasuk data terenkripsi.
* [Malicious code](https://id.wikipedia.org/wiki/Malicious_code) (Kode Berbahaya): Malicious code adalah program yang menyebabkan kerusakan sistem ketika dijalankan. Virus, worm dan Trojan horse merupakan jenis-jenis malicious code. - Virus komputer adalah sebuah program komputer atau kode program yang merusak sistem komputer dan data dengan mereplikasi dirinya sendiri melalui peng-copy-an ke program lain, boot sector komputer atau dokumen. - Worm adalah virus yang mereplikasi dirinya sendiri yang tidak mengubah file, tetapi ada di memory aktif, menggunakan bagian dari sistem operasi yang otomatis dan biasanya tidak terlihat bagi pengguna. Replikasi mereka yang tidak terkontrol memakan sumber daya sistem, melambatkan atau menghentikan proses lain. Biasanya hanya jika ini terjadi keberadaan worm diketahui. - Trojan horse adalah program yang sepertinya bermanfaat dan/atau tidak berbahaya tetapi sesungguhnya memiliki fungsi merusak seperti unloading hidden program atau command scripts yang membuat sistem rentan gangguan.
* [Social Engineering](https://id.wikipedia.org/w/index.php?title=Social_Engineering&action=edit&redlink=1) / Exploitation of Trust: Sekumpulan teknik untuk memanipulasi orang sehingga orang tersebut membocorkan informasi rahasia. Meskipun hal ini mirip dengan permainan kepercayaan atau penipuan sederhana, istilah ini mengacu kepada penipuan untuk mendapatkan informasi atau akses sistem komputer. Beberapa jebakan yang dapat dilakukan diantaranya dengan: - Memanfaatkan kepercayaan orang dalam bersosialisasi dengan komputer - Memanfaatkan kesalahan orang secara manusiawi misal: kesalahan ketik dll - Bisa dengan cara membuat tampilan Login yang mirip (teknik fake login)
* [Phishing](https://id.wikipedia.org/wiki/Phishing): Tindakan pemalsuan terhadap data atau identitas resmi.

1. Jelaskan perbedaan antara substitusi cipher dan transposisi cipher.

Teknik substitusi dan teknik transposisi adalah metode mendasar untuk mengkodifikasi pesan plaintext untuk mendapatkan ciphertext masing-masing. Dua metode ini adalah blok bangunan dasar dari teknik enkripsi dan juga dapat digunakan bersama, yang disebut **cipher produk** .

Perbedaan mendasar antara teknik substitusi dan teknik transposisi adalah bahwa teknik substitusi menggantikan huruf-huruf plaintext dari huruf, angka, dan simbol lainnya. Di sisi lain, teknik transposisi tidak menggantikan huruf, melainkan mengubah posisi simbol.

**Grafik perbandingan**

|  |  |  |
| --- | --- | --- |
| **Dasar untuk perbandingan** | **Teknik Substitusi** | **Teknik Transposisi** |
| Dasar | Mengganti karakter teks biasa dengan karakter, angka, dan simbol lainnya. | Mengatur ulang posisi karakter dari teks plaintext. |
| Formulir | Cipher substitusi monoalphabetic dan polyalphabetic. | Cipher transpositional keyless dan keyed. |
| Perubahan | Identitas karakter diubah sementara posisinya tetap tidak berubah. | Posisi karakter berubah terlepas dari identitasnya. |
| Kekurangan | Huruf dengan frekuensi rendah dapat membedakan plaintext. | Kunci yang dekat dengan kunci yang benar dapat mengungkapkan plaintext. |
| Contoh | Caesar Cipher | Reil Fence Cipher |

1. Jelaskan dengan contoh, serangan yang disebut dengan Man in the middle attack

Man in the Middle Attack (MiTM) adalah istilah teknik hacking ketika hacker memposisikan dirinya diantara dua perangkat yang saling berkomunikasi.

Contoh skenario cara kerja serangannya adalah salah satu pelanggan bank menerima email yang tampaknya berasal dari bank tersebut dan diminta untuk masuk ke akun pelanggan untuk mengisi informasi kontak, lalu pelanggan diarahkan untuk mengklik tautan di-email dan dibawa ke situs web bank tersebut. Sehingga pelanggan tidak ragu untuk memasukan kredensial login setelah mengklik tautan dalam email. Tetapi ketika pelanggan tersebut melakukannya, sebenarnya mereka tidak masuk ke rekening bank nya melainkan menyerahkan kredesial pelanggan tersebut kepada penyerang.

1. Mengapa rahasia perlu dijaga? Jelaskan dengan contoh
2. Jelaskan perbedaan antara kriptografi dan steganografi. Buat contohnya.

Kriptografi adalah ilmu yang berhubungan dengan teknik yang mempelajari matematika dalam aspek keamanan informasi seperti kerahasiaan data, integritas data, keabsahan data, dan autentikasi data.

Contohnya:

Data Asal = " RUMAH "  
Key = 7  
Data Acak ?

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

DAs = R U M A H

DAc = X A S G N

Steganografi adalah sebuah ilmu dan seni menulis atau menyembunyikan pesan tersembunyi dalam sebuah pesan sehingga hanya orang yang membuat dan menerima yang tahu pesan tersebut.

Contohnya: Pembuatan lagu pop yang melibatkan banyak pakar termasuk Steganografi, dalam pembuatan lagu tersebut si pembuat Steganografi akan menyisipkan Steganografi dalam file audio tersebut, sehingga orang lain tidak bisa menggunakannya dengan sembarangan.

1. Diketahui Plainteks : BERSYUKUR SEBAB ENGKAU SANGAT BERHARGA

Tentukan Cipherteksnya dengan menggunakan metode :

* 1. Caesar Cipher dengan kunci pergeseran C = P + (21)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Pergeseran sebanyak 21

21 22 23 24 25 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

BERSYUKUR SEBAB ENGKAU SANGAT BERHARGA

Ciphertext:

WZMNTPFPMNEWVWZIBFVPNVIBVOWZMCVMBV

b.Easier M Cipher dgn kunci : < MITRAHASIBUAN >

c.Vigenere Cipher dengan kunci : <MITRAHASIBUAN>

Pt: : BERSYUKUR SEBAB ENGKAU SANGAT BERHARGA

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Enkripsi:

Plaintext

B E R S Y U K U R S E B A B E N G K A U

1 4 17 18 24 20 10 20 17 18 4 1 0 1 4 13 6 10 0 20

S A N G A T B E R H A R G A

18 0 13 6 0 19 1 4 17 7 0 17 6 0

Kunci :

M I T R A M I T R A M I T R A M I T R A M I T R

12 8 19 17 0 12 8 19 17 0 12 8 19 17 0 12 8 19 17 0 12 8 19 17

A M I T R A M I T R

0 12 8 19 17 0 12 8 19 17

Ciphertext:

13 12 10 9 24 22 18 13 0 18 16 9 19 17 4 0 14 3 17 20 4 8 6 23 0 5 9 23 9 7 12 24 25 17

NMKJYWSNASQJTREAODRUEIGXAFJXJHMYZR

Dekripsi:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Ciphertext: NMKJYWSNASQJTREAODRUEIGXAFJXJHMYZR

13 12 10 9 24 6 18 13 8 18 16 9 19 18 4 25 14 3 17 20 4 8 6 23 0 5 9 23 9 7 12 24 25 17

Kunci : 12 8 19 17 0 12 8 19 17 0 12 8 19 17 0 12 8 19 17 0 12 8 19 17 0 12 8 19 17 0 12 8 19 17

Plaintext : 1 4 17 18 24 20 10 20 17 18 4 1 0 1 4 13 6 10 0 20 17 7 0 17 6 0

BERSYUKUR SEBAB ENGKAU SANGAT BERHARGA

d.Column Transposition Cipher dgn kunci : < MITRAHASIBUAN >