Nama : IIS NURJANAH

NIM :1310651078

Kelas : E

Tugas :UTS keamanan informasi

1.

No	Peneliti	Judul	Tool	Hasil
1	Reno Hamdani	Cyber Security for Elektronic Devices	komputer	semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan(*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari *physical attack* maupun *cyber attack*. *Cyber security* merupakan upaya untuk melindungi informasi dari adanya *cyber attack*, adapun elemen pokok *cyber security* adalah: Dokumen *security policy, ure, Perimeter Defense, Network Monitoring System, System Information and Event Management, Network Security Assessment, Human resource* dan*security awareness*
2	Ilham Irfan Fauzi	Cybercrime dan Internet Security	komputer	Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan keamanan bagi jaringan yang terkait ke Internet. Artinya jika operator jaringan tidak hati-hati dalam menset-up sistemnya, maka kemungkinan besar jaringan yang terkait ke Internet akan dengan mudah dimasuki orang yang tidak di undang dari luar. Adalah tugas dari operator jaringan yang

				bersangkutan, untuk menekan resiko tersebut seminimal mungkin.
3	DJOKO SUWITO	Sosialisasi Security Awareness Untuk Administrator Data	komputer	Keamanan administrator *(secutiry administrator)* perlu mendefinisikan peraturan untuk pengamanan administrator. Pada database yang besar dan terdapat beberapa macam database administrator, administrator keamanan harus menentukan kelompok *privilege administratif* untuk dimasukkan dalam beberapa persyaratan administratif. Persyaratan administratif tersebut kemudian dilakukan dan diberikan terhadap administrator tertentu. Atau, bila databasenya tidak terlalu besar dimana hanya ada sedikit administrator, akan lebih bijaksana bila dibuat satu persyaratan administratif, kemudian diberlakukan terhadap semua administrator data.

2.*VGlkYWsgc2VnYW1wYW5nIGl0dWxhaCBtYXMgYnJvLiBkZWNyeXB0IGluaTogDQo2ODc0NzQ3MDNhMmYyZjY0NmMyZTY0NzI2ZjcwNjI2Zjc4MmU2MzZmNmQyZjczMmYzMjM0NjkzMTZiNzEzNjc5NjM2ZjZmNjg3MTZhNmMyZjYzNzI3OTcwNzQ2ZjMxNDY2YzYxNjcyZTZkNzAzMw==*

langkah-langkah untuk menemukan "sesuatu" yang tersembunyi pada cipher

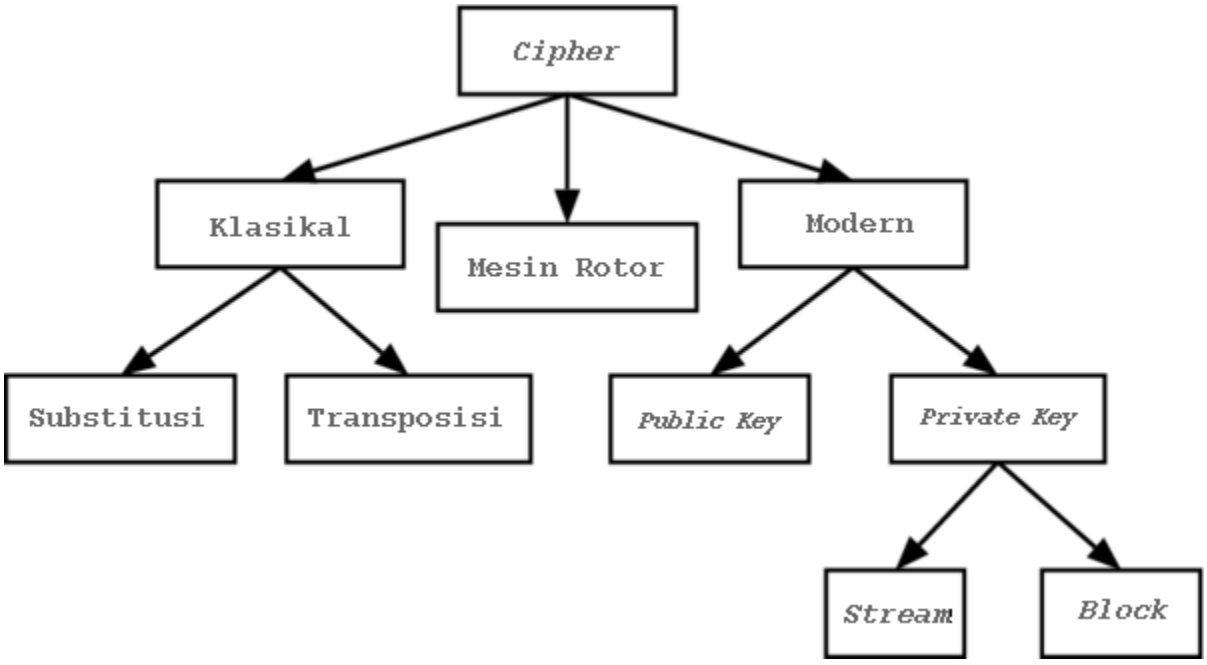
1. Sebuah cipher adalah sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi, serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah *encipherment*. Informasi yang asli disebut sebagai *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai *chiphertext*. Pesan *chipertext* berisi seluruh informasi dari pesan *plaintext*, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekasnisme yang tepat untuk melakukan dekripsi.*Cipher* pada biasanya memiliki parameter dari sebagian dari informasi utama, disebut sebagai kunci. Prosedur enkripsi sangat bervariasi tergantung pada kunci yang akan mengubah rincian dari operasi algoritma.

Tanpa menggunakan kunci, *chiper* tidak dapat digunakan untuk dienkirpsi ataupun didekripsi.

2. Pada penggunaan non teknis, sebuah *secret code* merupakan hal yang sama dengan *cipher*. Berdasar pada diskusi secara teknis, bagaimanapun juga, *code* dan *cipher* dijelaskan dengan dua konsep. *Code* bekerja pada tingkat pemahaman, yaitu, kata atau frasa diubah menjadi sesuatu yang lain. *Cipher*, dilain pihak, bekerja pada tingkat yang lebih rendah, yaitu, pada tingkat masing-masing huruf, sekelompok huruf, pada skema yang modern, pada tiap-tiap bit. Beberapa sistem menggunakan baik *code* dan *cipher* dalam sistem yang sama, menggunakan *superencipherment* untuk meningkatkan keamanan.

   Menurut sejarahnya, kriptografi dipisah menjadi dikotomi *code* dan *cipher*, dan penggunaan *code* memiliki terminologi sendiri, hal yang sama pun juga terjadi pada *cipher*: "*encoding*, *codetext*, *decoding*" dan lain sebagainya. Bagaimanapun juga, *code* memiliki berbagai macam cara untuk dikembalikan, termasuk kerapuhan terhadap kriptoanalisis dan kesulitan untuk mengatur daftar kode yang susah. Oleh karena itu, *code* tidak lagi digunakan pada kriptografi modern, dan *cipher* menjadi teknik yang lebih dominan.

3. Ada banyak sekali variasi pada tipe enkripsi yang berbeda. Algoritma yang digunakan pada awal sejarah kriptografi sudah sangat berbeda dengan metode modern, dan *cipher* modern dan diklasifikasikan berdasar pada bagaimana *cipher* tersebut beroperasi dan *cipher* tersebut menggunakan sebuah atau dua buah kunci.



Sejarah *Cipher* pena dan kertas pada waktu lampau sering disebut sebagai *cipher*

klasik. *Cipher* klasik termasuk juga *cipher* pengganti dan *cipher* transposisi. Pada awal abad 20, mesin-mesin yang lebih mutakhir digunakan untuk kepentingan enkripsi, mesin rotor, merupkan skema awal yang lebih kompleks.Metode enkripsi dibagi menjadi algoritma *symmetric key* dan algoritma *asymmetric key*. pada algoritma *symmetric key* (misalkan, DES dan AES), pengirim dan penerima harus memiliki kunci yang digunakan bersama dan dijaga kerahasiaanya. Pengirim menggunkan kunci ini untuk enkripsi dan penerima menggunakan kunci yang sama untuk dekripsi. Pada algoritma *asymmetric key* (misalkan, RSA), terdapat dua kunci terpisah, sebuah *public key* diterbitkan dan membolehkan siapapun pengirimnya untuk melakukan enkripsi, sedangkan sebuah *private key* dijaga kerahasiannya oleh penerima dan digunakan untuk melakukan dekripsi. Cipher *symmetric key* dapat dibedakan dalam dua tipe, tergantung pada bagaimana *cipher* tersebut bekerja pada blok simbol pada ukuran yang tetap (*block ciphers*), atau pada aliran simbol terus-menerus (*stream ciphers*).