# BAB II KRIPTOGRAFI

## Alasan dan Sejarah Kriptografi

- 3000 tahun SM bangsa Mesir menggunakan hieroglyphcs untuk menyembunyikan tulisan dari mereka yang tidak diharapkan.
- Sekitar 50 SM, Julius Caesar, kaisar Roma, menggunakan cipher substitusi untuk mengirim pesan ke Marcus Tullius Cicero.
    - Huruf-huruf apfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama.
    - Menggeser 3 posisi alphabet
- Pada abad ke-9, filsuf Arab al-Kindi menulis risalat (ditemukan kembali th 1987) yang diberi judul "A Manuscript on Deciphering Cryptographic Messages".
- Pada 1790, Thomas Jefferson mengembangkan alat enkripsi dengan menggunakan tumpukan yang terdiri dari 26 disk yang dapat diputar scr individual
- Mesin kriptografi mekanik yang disebut Hagelin Machine dibuat pada tahun 1920 oleh Boris Hagelin di Scockholm, Swedia. Di US, mesin Hagelin dikenal sebagai M-209.
- Militer Jerman menggunakan mesin cipher substitusi polialfabetik disebut Enigma sebagai sistem pengkodean utama selama PD II.
- awal tahun 70an Feistel menemukan DES, tahun 1977 DES (Data Encryption Standard) dipakai sebagai standar pemrosesan informasi federal US untuk mengenkripsi informasi yang unclassified. DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah
- 1976, Diffie dan Hellman mempublikasikan New Directions in Cryptography, memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru dan jenius untuk pertukaran kunci,
- Selama bertahun-tahun, kriptografi merupakan 'milik ekslusif' kalangan militer saja, sebelum akhirnya kaum akademis turut mengadakan riset tentang seni ini yang akhirnya menjadi cabang ilmu tersendiri, yang kemudian sangat mendorong penggunaan kriptografi ini secara meluas, yang tidak hanya dimanfaatkan di lingkungan militer dan diplomatik saja. Saat ini kriptografi diadopsi sebagai dasar sistem pengamanan data di setiap sistem komputasi, jaringan komputer dan terutama internet.

## Definisi Kriptografi (Pendahuluan Kriptografi)

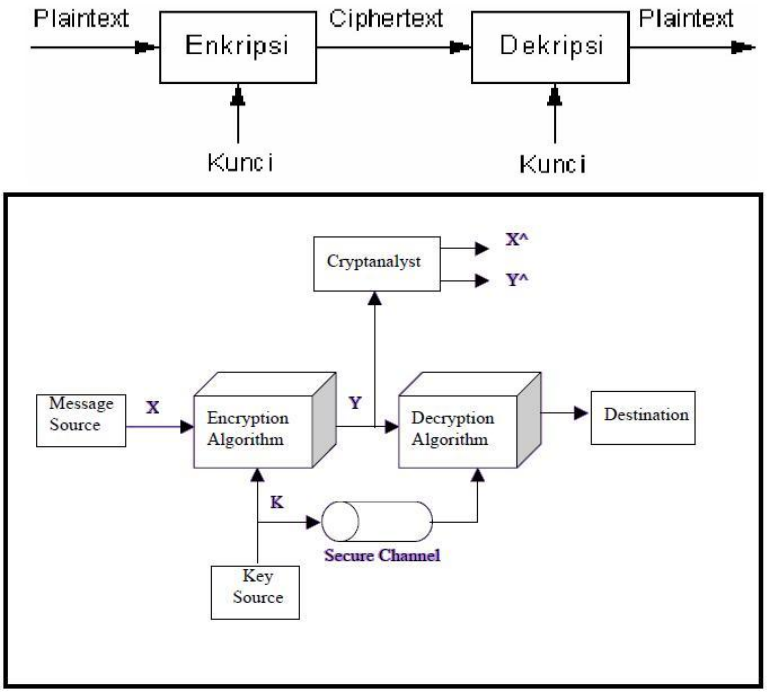
- Kriptografi berasal dari bahasa Yunani. Kata kriptografi dibagi menjadi dua, yaitu *kripto* (rahasia) dan *graphia* (tulisan)
- Menurut terminology kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.
  (*the art and science of keeping messages secure*) William Stallings
- Contoh : **Teks asli :** uang disimpan di balik buku X
  **Teks yang tersandikan :** j&kloP#d$gkh*7h^"tn%6^klp..t@
- Pesan dapat berupa: teks, gambar, audio, video.
- Perkembangan kriptografi sangat pesat. Para ahli kriptografi terus menerus menciptakan algoritma-algoritma kriptografi yang baru.

## Istilah-istilah yang Digunakan

- Kriptografi *(**Cryptography**)* adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh ***cryptographer***.
- *Sedangkan **cryptanalysis** adalah suatu ilmu dan seni membuka* (breaking) ciphertext dan orang yang melakukannya disebut ***cryptanalyst***.
- **Plaintext** (M) atau *cleartext* adalah pesan yang hendak dikirimkan (berisi data asli).
- **Ciphertext** (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- **Enkripsi** (fungsi E) (*encryption* atau *encipherment*) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- **Dekripsi** (fungsi D) (*decryption* atau *decipherment*) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.

- **Algoritma kriptografi** : Algoritma merupakan sekumpulan instruksi, sekumpulan fungsi matematis dan logika, yang disusun sedemikian rupa sehingga memiliki kekuatan kriptografis.
- **Kunci** adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi. (mengontrol algoritma yang dipakai)

Ilustrasi proses sederhananya :




Algoritma enkripsi harus benar-benar teruji sehingga tidak dimungkinkan untuk mendeskripsi sebuah pesan hanya dalam bentuk *chipertext*

## Notasi Matematis

- Misalkan:
  $C$ = chiperteks
  $P$ = plainteks dilambangkan
- Fungsi enkripsi $E$ memetakan $P$ ke $C$,
  $E(P) = C$
- Fungsi dekripsi $D$ memetakan $C$ ke $P$,
  $D(C) = P$
- Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka fungsi enkripsi dan deskripsi harus memenuhi sifat :
  $D(E(P)) = P$
- Dengan menggunakan kunci $K$, maka fungsi enkripsi dan dekripsi menjadi
  $E_K(P) = C$
  $D_K(C) = P$
  dan kedua fungsi ini memenuhi
  $D_K(E_K(P)) = P$
- Kekuatan algoritma kriptografi diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan data chiperteks menjadi plainteksnya. Kerja ini dapat diekivalenkan dengan waktu.
- Semakin banyak usaha yang diperlukan, yang berarti juga semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma kriptografinya, yang berarti semakin aman digunakan untuk menyandikan pesan.

## Dasar Matematika Cryptography

1. AND
2. OR
3. XOR
4. Penjumlahan Modulo
5. Pergeseran bit (shift)
6. Konversi bit to hexa
7. Konversi hexa to bit

## Algoritma-algoritma Kriptografi

Meskipun teknik enkripsi klasik tidak lagi diterapkan diaplikasi keamanan jaringan modern, pengetahuan tentang teknik-teknik ini akan sangat membantu kita.

### I. Book Key Cipher

Cipher ini menggunakan teks dari sebuah sumber (misalnya buku) untuk mengenkripsi plaintext.

### II. Codes

Codes berkaitan dengan kata-kata dan frase dan menghubungkan kata-kata ini sebagai frase untuk sekelompok angka atau huruf. Sebagai contoh, angka 526 dapat berarti “Attack at dawn”

### III. Steganografi

Metode steganografi mencoba menyempunyikan pesan kedalam sesuatu yang lain, misalnya menyembunyikan sebuah pesan di dalam pesan lain sehingga pesan asli tidak terlihat secara langsung.
Beberapa metode steganografi :

- Invisible ink
- Pin punctures : beberapa tusukan pin-pin kecil pada kertas secara biasa tidak akan kelihatan sampai kertas diletakkan pada sudut tertentu dengan cahaya terang
- Menyembunyikan pesan didalam sebuah gambar atau foto
- Yunani vs Persia : pesan disembunyikan di meja yang dilapisi lilin
- Histalaeus : pesan ditato dikepala budak yang telah digunduli
- Media yang digunakan dalam Steganografi: gambar, audio, text

Contoh :
Cari makna steganografi berikut :

> Setelah engkau rasakan akan nikmatnya gula, hisap aroma rambutan ini sampai engkau nyaman ingin nambah.

Jawaban : Serang hari senin

### IV. Caesar cipher dan shift cipher

Caesar cipher adalah cipher substitusi sederhana yang mencakup pergeseran alfabet 3 posisi ke kanan.
Plaintext : kriptografi
Ciphertext : nulswrjudil

Proses enkripsi dapat dilakukan menggunakan salah satu langkah berikut :

- Mencari huruf ketiga lanjutan dari setiap huruf plaintext
  Contoh : k -> n
  r -> u
- Menggunakan table berikut

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

Pada metoda shift cipher, pergeseran alphabet tidak harus 3 posisi ke kanan saja, tetapi bisa dimodifikasikan.

**PENYERANGAN PADA METODA CAESAR CHIPPER DAN SHIFT CHIPPER**

Teknik semacam ini sangat memungkinkan cryptoanalyst untuk melakukan pemecahan kode chipertext dengan mudah dengan mencoba 25 kunci yang memungkinkan. Metode yang dapat dipakai oleh cryptoanalyst dengan mencoba seluruh kemungkinan yang ada ini sering disebut metode brute-force (*exhaustive key search)*.

| KEY | PHHW PH DIWHU WKH WRJD SDUWB |
|---|---|
| 1 | oggv og chvgt vjg vqic rctva |
| 2 | nffu nf bgufs uif uphb qbsuz |
| 3 | meet me after the toga party |
| 4 | ldds ld zesdq sgd snfz ozqsx |
| 5 | kccr kc ydrcp rfc rmey nyprw |
| 6 | jbbq jb xcqbo qeb qldx mxoqv |
| 7 | iaap ia wbpan pda pkcw lwnpu |
| 8 | hzzo hz vaozm ocz ojbv kvmot |
| 9 | gyyn gy uznyl nby niau julns |
| 10 | fxxm fx tymxk max mhzt itkmr |
| 11 | ewwl ew sxlwj lzw lgys hsjlq |
| 12 | dvvk dv rwkvi kyv kfxr grikp |
| 13 | cuuj cu qvjuh jxu jewq fqhjo |
| 14 | btti bt puitg iwt idvp epgin |
| 15 | assh as othsf hvs hcuo dofhm |
| 16 | zrrg zr nsgre gur gbtn cnegl |
| 17 | yqqf yq mrfqd ftq fasm bmdfk |
| 18 | xppe xp lqepc esp ezrl alcej |
| 19 | wood wo kpdob dro dyqk zkbdi |
| 20 | vnnc vn jocna cqn cxpj yjach |
| 21 | ummb um inbmz bpm bwoi xizbg |
| 22 | tlla tl hmaly aol avnh whyaf |
| 23 | skkz sk glzkx znk zumg vgxze |
| 24 | rjjy rj fkyjw ymj ytlf ufwyd |
| 25 | qiix qi ejxiv xli xske tevxc |

Latihan :

Pecahkan sebuah *cipher* menggunakan algoritma *Caesar Cipher* yang terdiri dari kata – kata berikut ini :

**exxegoexsrgi**

## V. Mixed monoalphabetic

Dalam metode ini setiap kunci disubstitusi dengan sembarang kunci secara acak dalam batasan 26 huruf dalam alphabet.

Contoh :

Plain text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher text : DKVQFIBJWPESCXHTMYAUOLRGZN
Plain text : IF WE WISH TO REPLACE LETTERS
Cipher Text : WI RF RWAJ UH FYTSDVF SFUUFYA

## VI. Easier monoalphabetic (substitusi deret campuran kata kunci)

Dalam easier ini kata kunci (*keyword*) hanya menggunakan suatu kata atau sekelompok kata, kemudian dihilangkan / dihapus huruf yang sama dalam kata kunci tersebut dan kemudian untuk huruf berikutnya diteruskan dengan huruf terakhir dalam kata kunci tersebut dan seterusnya secara urut dalam 26 alphabet
Contoh :

Diberikan kata kunci : SISTEM BERKAS
Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher: SITEMBRKACDFGHJLNOPQUVWXYZ
maka jika dengan metode tersebut dilakukan enkripsi :
Plainteks : TEKNOLOGI INDUSTRI
Cipherteks : QMDHJFJRA AHEUPQOA

Easier monoalphabetic bisa menggunakan kunci seperti nama, alamat atau apa saja yang diinginkan oleh pengirim pesan.
Dalam proses enkripsi juga dapat dilakukan menggunakan lebih dari satu kunci.
Alternatif-alternatif penggunakan multi kunci pada easier monoalphabetic :

- Ciphertext keluaran dari kunci pertama dimasukkan kembali ke kunci kedua, dan demikian selanjutnya
  Contoh :
  K1 : UNIVERSITAS

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

  K2 : KOMPUTER

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

  K3 : INDONESIA

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

  Plaintext : informatika
  Ciphertext : GEH…

- Menggunakan pendistribusian kunci-kunci berdasarkan blok-blok
  Contoh :
  Plaintext : saya belajar keamanan komputer
  Plaintext terlebih dahulu dibentuk menjadi block-block yang terdaru dari enam huruf (misalnya) pada satu block
  SAYABE -> K1
  LAJARK -> K2
  EAMANA -> K3
  NKOMPU -> K1
  TERXXX -> K2
  Yaitu kunci K1 digunakan pada block pertama, K2 pada block kedua, K3 pada block ketiga dan seterusnya.

- Menggunakan pendistribusian kunci per huruf
  Pendistribusia kunci huruf per huruf juga dapat digunakan :
  S -> K1
  A -> K2
  Y -> K3
  A -> K1

## VII. General monoalphabetic

*General* spesifikasi enkripsi ditentukan oleh perulangan pada posisi kolom yang bersesuain dengan jumlah alphabet yang berbeda dalam kata kunci.

Contoh :

Diberikan suatu kata kunci : STARWARS
Maka alphabet yang sama dihapus : STARW
Lakukan dengan pengulangan kolom untuk huruf lain dalam 26 alphabet :

STARW
BCDEF
GHIJK
LMNOP
QUVXY
Z

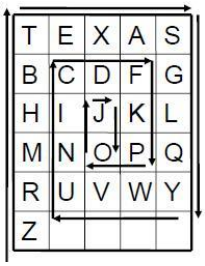
Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher: SBGLQZTCHMUADINVREJOXWFKPY
maka jika digunakan untuk melakukan enkripsi / dekripsi :

Plain : I KNOW ONLY THAT I KNOW NOTHING
Cipher : H UINF NIAP OCSO H UINF INOCHIT
HUIN FNIA POC SOHU INFINO CHIT

Latihan :
dekripsikan cipherteks berikut : DQITSVSUNDQIGHIOSHUXLHU
menggunakan kata kunci STARWARS enkrispsikan plainteks berikut
TAK ADA PROBLEM YANG TAK BISA DISELESAIKAN

## VIII. Substitusi secara spiral

Kata kunci : texas
Kemudian kata kunci digunakan untuk membentuk :




Sehingga diperoleh chipper :

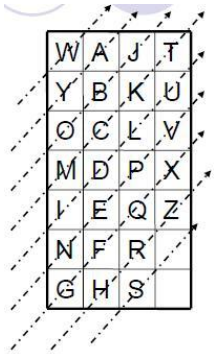
| Z | R | M | H | B | T | E | X | A | S | G | L | Q | Y | W | V | U | N | I | C | D | F | K | P | O | J |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Untuk plaintext :

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

## IX. Substitusi secara out by diagonal

Kata kunci : WYOMING
Kemudian kata kunci digunakan untuk membentuk :




Sehingga diperoleh chipper :

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

Untuk plaintext :

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

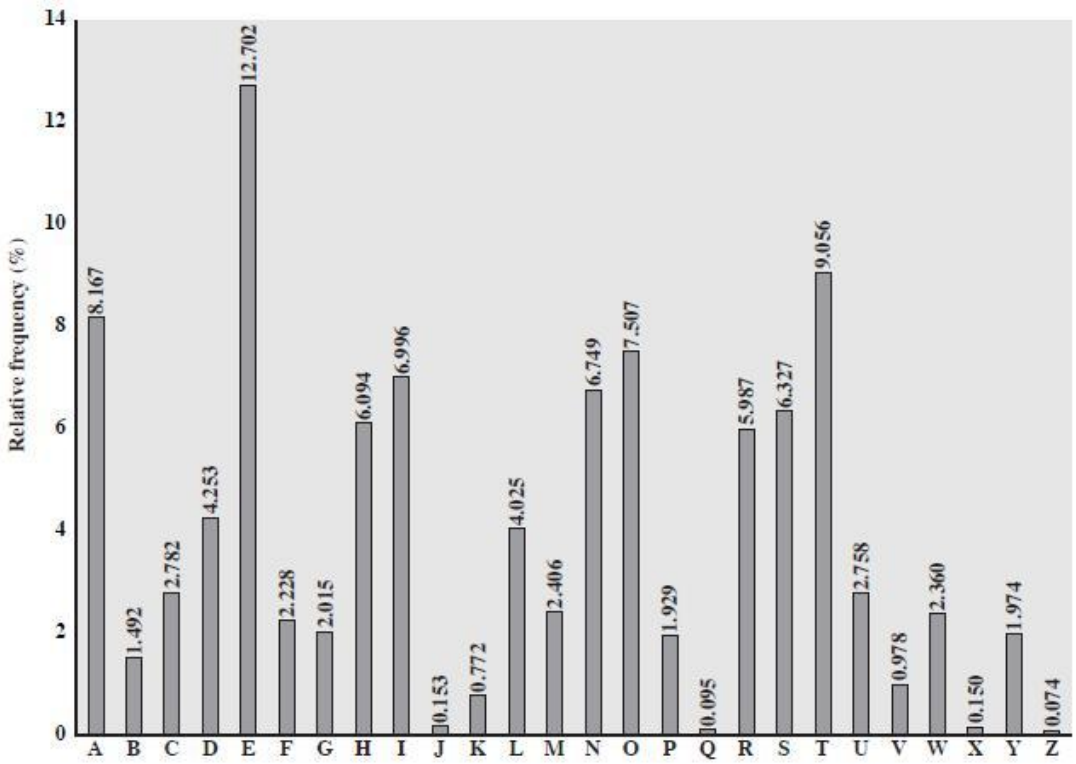
**PENYERANGAN PADA METODA MONOALPHABETIC**

Bagaimanapun juga jika cryptoanalyst dapat mengetahui bentuk alami dari plaintext, kemudian cryptoanalyst dapat mengeksploitasi susunan bahasa yang digunakan.

Sebagai contoh dari teknik ini adalah dengan melihat bagaimana seorang cryptoanalyst mencoba memecahkan chipertext berikut :

```
UZ QSO VUOHXMOPV GPOZPEVSG
ZWSZ OPFPESX UDBMETSX AIZ
VUEPHZ HMDZSHZO WSFP APPD TSVP
QUZW YMXUZUHSX EPYEPOPDZSZUPO
MB ZWP FUPZ HMDJ UD TMOHMQ
```

Pada langkah awal, frekuensi relative dari huruf-huruf tersebut dapat ditentukan dan dibandingkan dengan frekuensi distribusi standar (misalnya untuk bahasa Inggris), seperti pada table berikut ini :




Kemudian, frekuensi relative dapat ditetapkan dalam persentasi seperti dibawah ini :

| Huruf | % | Huruf | % | Huruf | % | Huruf | % |
|---|---|---|---|---|---|---|---|
| P | 13,33 | D | 5,00 | T | 2,50 | C | 0,00 |
| Z | 11,67 | E | 5,00 | A | 1,67 | K | 0,00 |
| S | 8,33 | V | 4,17 | B | 1,67 | L | 0,00 |
| U | 8,33 | X | 4,17 | G | 1,67 | N | 0,00 |
| O | 7,50 | F | 3,33 | Y | 1,67 | R | 0,00 |
| M | 6,67 | W | 3,33 | I | 0,83 | | |
| H | 5,83 | Q | 2,50 | J | 0,83 | | |

Dengan membandingkan frekwensi relatif dan tabel distribusi standar, sedikit kelihatan bahwa huruf P dan Z ekuivalen dengan huruf e dan t, tapi belum dapat ditentukan pasangan yang tepat dari keduanya. Huruf S,U,O,M dan H mempunyai frekuensi relative yang tinggi dan mungkin ekuivalen dengan r,n,i,o,a,s. Huruf dengan frekwensi relative terendah, yaitu A,B,G,Y,I,J kelihatannya sesuai dengan w,v,b,k,x,q,j,z.

Dari point ini, ada banyak cara yang dapat dilakukan untuk melanjutkan proses cryptoanalysis. Salah satu cara yang lebih efektif adalah dengan melihat frekuensi dari kombinasi dua buah huruf. Hal ini sering kita sebut sebagai digraph. Secara umum, digraph yang paling sering kita temui dalam bahasa Inggris adalah th. Di dalam chipertext yang kita miliki, digraph yang sering kita temui adalah ZW (muncul tiga kali). Jadi, kita dapat memasangkan Z dengan t dan W dengan h. Kemudian, dengan hipotesis yang lebih seksama kita dapat memasangkan P dengan e. Sekarang kita dapat menerjemahkan urutan ZWP dengan "the". Maka, sejau ini kita telah memasangkan beberapa huruf, sehingga dapat tersusun sebagai berikut :

```
UZ QSO VUOHXMOPV GPOZPEVSG
 t            e   e te
ZWSZ OPFPESX UDBMETSX AIZ
t  t  e e              t
VUEPHZ HMDZSHZO WSFP APPD TSVP
   e t    t  t     e  ee     e
QUZW YMXUZUHSX EPYEPOPDZSZUPO
  t            e  e e t z e
MB ZWP FUPZ HMDJ UD TMOHMQ
   t e   et
```

Dari percobaan tersebut kita telah mengidentifikasi 4 huruf, tetapi telah menjadi pesan yang mulai sedikit jelas. Dengan analisa yang lebih lanjut dan menggunakan metode trial and error, kita dapat membentuk pesan yang utuh dengan tidak lupa menambahkan spasi sehingga menjadi berikut :

```
IT WAS DISLOSED YESTERDAY
THAT SEVERAL INFORMAL BUT
DIRECT CONTACTS HAVE BEEN MADE
WITH POLITICAL REPRESENTATIVES
OF THE VIET CONG IN MOSCOW
```

Sepuluh huruf yang sering muncul dalam bahasa Indonesia :

| Huruf | Frekuensi kemunculan (%) |
|---|---|
| A | 17,50 |
| N | 10,30 |
| I | 8,70 |
| E | 7,50 |
| K | 5,65 |
| T | 5,10 |
| R | 4,60 |
| D | 4,50 |
| S | 4,50 |
| M | 4,50 |

Teknik monoalphabetic ini cukup mudah untuk dipecahkan karena teknik ini menggambarkan frekuensi dari data asli. Langkah yang diambil untuk dapat meningkatkan keamanan adalah dengan menerapkan lebih dari satu substitusi untuk huruf tunggal.

## X. Substitusi : XOR data

Data tersimpan dalam bentuk bilangan biner
Data di-XOR dengan sebuah kunci
Operasi XOR dapat dilihat pada tabel berikut :

| a | b | a XOR b (a ⊕ b) |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

## XI. Mulltiple letter encryption (Playfair)

Metode yang paling terkenal dari multiple letter encryption adalah playfair.
Teknik Playfair memperlakukan digraph sebagai satu unit dan menerjemahkan unit tersebut kedalam digrap ciphertext. Algoritma Playfair adalah algoritma yang didasarkan pada penggunaan matrix huruf berbasis 5x5 yang disusun dengan mengunakan kata kunci. Sebagai contoh :

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

Di dalam kasus ini, kata kuncinya adalah *monarchy*. Matrix dibentuk dengan memasukkan kata kunci tersebut (tanpa duplikasi) dari kiri ke kanan dan dari atas ke bawah, dan kemudian mengisi sisa elemen matrix yang kosong dengan sisa huruf alphabet secara terurut. Huruf I dan J dihitung sebagai satu elemen matrix. Plaintext dienkripsi dua huruf sekaligus dengan aturan sebagai berikut :

1) Huruf dari Plaintext yang terulang dipisahkan dengan huruf lain seperti X, jadi jika plaintextnya ballon maka akan dimasukkan sebagai ba lx lo on.
2) Huruf-huruf dari plaintext yang masuk di dalam satu baris digantikan dengan huruf ke kanan, dengan elemen pertama dari baris secara sirkular diikuti dengan yang terakhir. Sebagai contoh, ar dienkripsi menjadi RM
3) Huruf yang berada pada satu kolom digantikan dengan huruf dibawahnya, dengan elemen teratas dari baris secara sirkular diikuti dengan yang terakhir. Sebagai contoh, mu dienkripsi sebagai CM.
4) Selain itu, setiap huruf plaintext digantikan dengan huruf yang berada di barisnya sendiri dan di kolomnya diisi oleh huruf palaintext yang lain. Jadi, hs menjadi BP dan ea menjadi IM (atau JM sesuai dengan keinginan).

## XII. Vigenere Cipher Menggunakan Angka

Apabila pada teknik monoalphabetic setiap ciphertext selalu menggantikan nilai dari setiap plaintext tertentu, pada teknik substitusi vigenere setiap ciphertext bisa memiliki banyak kemungkinan plaintext-nya.
Hubungan setiap huruf dengan angka adalah sbb :

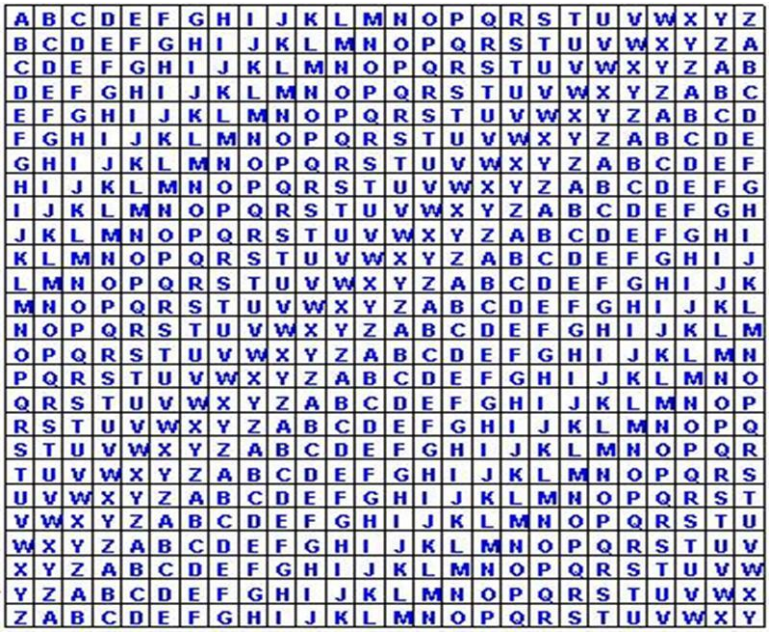
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Maka contoh dari vigenere cipher menggunakan angka :
Jika dimiliki kunci dengan 6 huruf CIPHER, maka jika ditukar dengan angka, maka akan menjadi K = (2, 8, 15, 7, 4, 17)

| T | H | I | S | C | R | Y | P |
|---|---|---|---|---|---|---|---|
| 19 | 7 | 8 | 18 | 2 | 17 | 24 | 15 |
| 2 | 8 | 15 | 7 | 4 | 17 | 2 | 8 |
| 21 | 15 | 23 | 25 | 6 | 8 | 0 | 23 |

## XIII. Vigenere Cipher Menggunakan Huruf

*Vigenere Cipher* ditemukan oleh Blaise de Vigenere pada abad ke 16. Untuk menggunakan algoritma ini, maka diperlukan sebuah bujursangkar *vigenere* dimana kolom paling kiri bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plaintext* dan setiap baris di dalam bujursangkar menyatakan huruf-huruf *ciphertext.*



Contoh:

*Plaintext*: ATTACKATDAWN

Maka, kita harus menentukan kata kuncinya. Apabila kata kunci yang digunakan lebih pendek dari panjang *plaintext* maka kata kunci diulang (sistem periodik) seperti berikut:

Panjang *plaintext*: 12 huruf

Kata kunci: LEMON (5 huruf)

Kata kunci: LEMONLEMONLE (12 huruf)

Huruf pertama dari *plaintext* adalah A, dienskripsi dengan menggunakan alfabet pada baris L, yang merupakan huruf pertama pada kata kunci. Ini dilakukan dengan melihat huruf yang terdapat pada baris L dan kolom A pada tabel *vigenere*, yaitu huruf L.Untuk huruf kedua pada *plaintext*, kita menggunakan huruf kedua pada kata kunci, yaitu pada baris E dan kolom T, yaitu huruf X. Lakukan terus hingga huruf terakhir *plaintext* sehingga menghasilkan enkripsi sebagai berikut:

*Ciphertext*: LXFOPVEFRNHR

Dekripsi dilakukan dengan cara sebaliknya. Misalkan untuk huruf pertama *ciphertext*, L, kita cari huruf pertama kata kunci pada baris L, dimana huruf pertama kata kunci juga merupakan huruf L. Kemudian kita dapat menemukan pada baris L, huruf L terdapat pada kolom A, yang mengartikan bahwa huruf A merupakan huruf pertama *plaintext*. Laukan terus hingga jumlah huruf pada kata kunci habis.

Latihan :

- ☐ Pecahkan sandi ini dengan vigenere
- ☐ KRLEX LVD
- ☐ Kunci : irwan
- ☐ Plainteks :???

Latihan :

## XIV. Hill Cipher

Ditemukan pada tahun 1929 oleh Lester S. Hill.

Jika $x$ adalah plaintext, $y$ adalah ciphertext, $m$ adalah jumlah elemen dan $K$adalah kunci berbentuk matriks berukuran $m \times m$, maka secara umum Hill Cipher melakukan perhitungan sebagai berikut :

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m)\begin{pmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,m} \\ k_{2,1} & k_{2,2} & \dots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \dots & k_{m,m} \end{pmatrix}$$

Dengan kata lain $y = xK$

Dikatakan bahwa ciphertext diperoleh dari plaintext dengan cara transformasi linier. Untuk melakukan deskripsi, kita menggunakan matriks invers $K^{-1}$. (matriks inverse dari A jika ada adalah $A^{-1}$ dimana $AA^{-1} = I_m$.

Contoh :

Kunci yang dipakai : $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$.

Dari perhitungan dapat diperoleh $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

Jika ingin mengenkripsikan plaintext JULY, maka akan dimiliki 2 elemen plaintext yang untuk deskripsi (jumlah elemen plaintext disesuaikan dengan ukuran kunci)

- (9 20) -> JU
- (11 24) -> LY

Kemudian kita lakukan perhitungan berikut :

$(9\ \ 20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60\ \ 72 + 140) = (3\ \ 4)$ -> DE

$(11\ \ 24)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (121 + 72\ \ 88 + 168) = (11\ \ 22)$ -> LW

Sehingga enkripsi untuk JULY adalah DELW

Untuk deskripsi, dapat dilakukan dengan cara :

$$(3\ \ 4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9\ \ 20)$$
$$(11\ \ 20)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (11\ \ 24)$$

Catatan cara memperoleh matriks invers :

$$A^{-1} = (\det A)^{-1}\begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

Contoh :

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Maka

$$det\ K = \det\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (11 * 7 - 8 * 3) mod 26$$
$$= 53\ mod\ 26 = 1$$

Kemudian matriks inversnya :

$$K^{-1} = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

**Latihan:**

Plaintext :

```
Semoga Anda berhasil dalam menempuh ujian akhir semester dua tahun ini.
```

Kunci : $K = \begin{pmatrix} 3 & 1 & 2 \\ 5 & 1 & 3 \\ 2 & 4 & 7 \end{pmatrix}$

Chipertext :

```
EAG WAY TWU JNG MOK FEF KWC HTK NFQ HEB YBP YFL ZHB GSG DRK QSE TTY PQD
BZU
```

**Latihan**

Tunjukkan untuk $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$, invers matriksnya adalah $K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 7 \end{pmatrix}$

Deskripsikan chipertext berikut : LNSHDLEWMTRW menggunakan $K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 7 \end{pmatrix}$

**Latihan 2**

It is known that the plaintext "friday" is encrypted using a 2×2 Hill Cipher to yield the ciphertext PQCFKU. Find the key matrix **K** for this cryptosystem.

## XV. Spartan style (scytale)

Tentara Sparta di Yunani pada permulaan tahun 400 SM menggunakan alat yang namanya scytale.
Scytale : pita panjang dari daun papyrus + sebatang silinder
Pesan ditulis horizontal (baris per baris)
Bila pita dilepaskan, maka huruf-huruf didalamnya telah tersusun membentuk pesan rahasia.
Untuk membaca pesan, penerima melilitakn kembali silinder yang diameternya sama dengan diameter silinder pengirim


## XVI. Transposisi kolom (rail fence)

Teknik yang paling sederhana adalah teknik rail fence, dimana plaintext ditulis dengan urutan kolom dan dibaca sebagai urutan baris. Sebagai contoh untuk mengenkripsi pesan "meet me after the toga party" dengan metode rail fence dengan kedalaman 2, kita dapat menuliskan sebagai :

```
mematrhtgpry
etefeteoaat
```

Pesan yang telah dienkripsi adalah :

MEMATRHTGPRYETEFETEOAAT

Cara deskripsinya yaitu pertama-tama jumlah ciphertext dibagi dengan nilai kunci.
Contoh (23/2 => 12 baris atas dan 11 baris bawah)
Lalu cipertext tersebut dibagi 2 baris menjadi 12 baris diatas dan 11 baris dibawah.

Pengembangan lebih lanjut dari transposisi kolom ini adalah dapat digunakannya kunci
Contoh dengan kunci : 431526
Plaintext : saya sedang belajar kriptografi

| Kunci | 4 | 3 | 1 | 5 | 2 | 6 |
|---|---|---|---|---|---|---|
| Plaintext | S | A | Y | A | S | E |
| | D | A | N | G | B | E |
| | L | A | J | A | R | K |
| | R | I | P | T | O | G |
| | R | A | F | I | Y | Z |

Dibaca dari atas ke bawah sesuai dengan urutan

Ciphertext : YNJPF SBROY AAAIA SDLRR AGATI EEKGZ
Catatan : jika jumlah huruf tidak mencukupi untuk membentuk segiempat maka sisa kebutuhannya dapat ditambahkan huruf-huruf yang disepakati

## XVII. Transposisi baris

Algoritma ini diperoleh dengan mengubah posisi *plaintext*nya

Contoh:

*Plaintext* : TECHNOLOGY(10 huruf)

Kunci : (10/5=2)

Enkripsi : TECHN

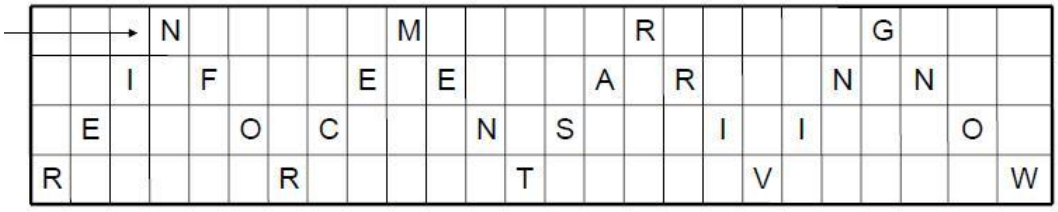
OLOGY

*Ciphertext* : TOELCOHGNY

Untuk membacanya, maka *ciphertext* dibaca berurutan dengan menggunakan kunci 2, yaitu dengan bergeser sebanyak 2 huruf.

## XVIII. Transposisi pola zig-zag

Plaintext : Reinforcementsarrivingnow

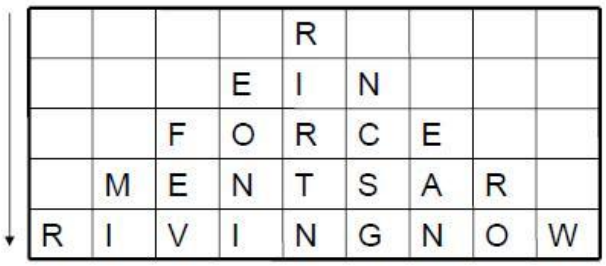



Keluaran ciphertext berupa baris

Ciphertext : NMRGIFEEARNNEOCNSIIORRTVW

## XIX. Transposisi pola segitiga

Plaintext : Reinforcementsarrivingnow




Dibaca dari atas ke bawah mulai dari kolom pertama

Ciphertext : RMIFEVEONIRIRTNNCSGEANROW

Catatan : jika jumlah huruf tidak mencukupi untuk membentuk segitiga maka sisa kebutuhannya dapat ditambahkan huruf-huruf yang disepakati

## XX. Simple Encryption Mechanism (Operator XOR)

Awalnya diperiksa jumlah karakter dari string yang akan diacak.

Lalu dilakukan *looping* sebanyak jumlah karakter.

Didalam *looping* dilakukan operasi XOR mulai dari karakter pertama sampai karakter terakhir

Karakter pertama akan di XOR dengan nilai dari jumlah karakter pada string, karakter berikutnya sampai yang terakhir akan di XOR dengan hasil XOR dari proses sebelumnya

Contoh : proses enkripsi **bulsara** -→ **e ► | ☼ n∟ }**

**bulsara** yang terdiri dari 7 karakter.

Bentuk kode ASCII dari masing-masing karakter itu adalah sebagai berikut:

- ☐ b <---- 62
- ☐ u <---- 75
- ☐ l <---- 6C
- ☐ s <---- 73
- ☐ a <---- 61
- ☐ r <---- 72
- ☐ a <---- 61

Proses XOR untuk setiap nilai ASCII adalah sebagai berikut :

- ☐ 62 XOR 7 = 65
- ☐ 75 XOR 65 = 10
- ☐ 6C XOR 10 = 7C
- ☐ 73 XOR 7C = 0F
- ☐ 61 XOR 0F = 6E
- ☐ 72 XOR 6E = 1C
- ☐ 61 XOR 1C = 7D

65 10 7C 0F 6E 1C 7D→**e ► | ☼ n∟}**

Deskripsi : membalikkan string yang sudah diacak menjadi bentuk semula.

- ☐ **65 10 7C 0F 6E 1C 7D**
- ☐ 65 XOR 7 = 62 → b
- ☐ 10 XOR 65 = 75→ u
- ☐ 7c XOR 10 = 6c→ l
- ☐ Dst

Nilai ASCII digunakan sebagai standarisasi peng-kodean karakter-karakter yang digunakan dikomputer. Sebagai contoh karakter huruf **A** memiliki kode ASCII yaitu **41h** (41 heksa atau 65 desimal),
Kode untuk karakter huruf **a** berbeda dengan **A** (kapital), yaitu **61h** (61 heksa atau 97 desimal).

Konversi karakter menjadi heksadesimal :

| Char | Dec | Oct | Hex | Char | Dec | Oct | Hex | Char | Dec | Oct | Hex | Char | Dec | Oct | Hex |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (nul) | 0 | 0000 | 0x00 | (sp) | 32 | 0040 | 0x20 | @ | 64 | 0100 | 0x40 | ` | 96 | 0140 | 0x60 |
| (soh) | 1 | 0001 | 0x01 | ! | 33 | 0041 | 0x21 | A | 65 | 0101 | 0x41 | a | 97 | 0141 | 0x61 |
| (stx) | 2 | 0002 | 0x02 | " | 34 | 0042 | 0x22 | B | 66 | 0102 | 0x42 | b | 98 | 0142 | 0x62 |
| (etx) | 3 | 0003 | 0x03 | # | 35 | 0043 | 0x23 | C | 67 | 0103 | 0x43 | c | 99 | 0143 | 0x63 |
| (eot) | 4 | 0004 | 0x04 | $ | 36 | 0044 | 0x24 | D | 68 | 0104 | 0x44 | d | 100 | 0144 | 0x64 |
| (enq) | 5 | 0005 | 0x05 | % | 37 | 0045 | 0x25 | E | 69 | 0105 | 0x45 | e | 101 | 0145 | 0x65 |
| (ack) | 6 | 0006 | 0x06 | & | 38 | 0046 | 0x26 | F | 70 | 0106 | 0x46 | f | 102 | 0146 | 0x66 |
| (bel) | 7 | 0007 | 0x07 | ' | 39 | 0047 | 0x27 | G | 71 | 0107 | 0x47 | g | 103 | 0147 | 0x67 |
| (bs) | 8 | 0010 | 0x08 | ( | 40 | 0050 | 0x28 | H | 72 | 0110 | 0x48 | h | 104 | 0150 | 0x68 |
| (ht) | 9 | 0011 | 0x09 | ) | 41 | 0051 | 0x29 | I | 73 | 0111 | 0x49 | i | 105 | 0151 | 0x69 |
| (nl) | 10 | 0012 | 0x0a | * | 42 | 0052 | 0x2a | J | 74 | 0112 | 0x4a | j | 106 | 0152 | 0x6a |
| (vt) | 11 | 0013 | 0x0b | + | 43 | 0053 | 0x2b | K | 75 | 0113 | 0x4b | k | 107 | 0153 | 0x6b |
| (np) | 12 | 0014 | 0x0c | , | 44 | 0054 | 0x2c | L | 76 | 0114 | 0x4c | l | 108 | 0154 | 0x6c |
| (cr) | 13 | 0015 | 0x0d | - | 45 | 0055 | 0x2d | M | 77 | 0115 | 0x4d | m | 109 | 0155 | 0x6d |
| (so) | 14 | 0016 | 0x0e | . | 46 | 0056 | 0x2e | N | 78 | 0116 | 0x4e | n | 110 | 0156 | 0x6e |
| (si) | 15 | 0017 | 0x0f | / | 47 | 0057 | 0x2f | O | 79 | 0117 | 0x4f | o | 111 | 0157 | 0x6f |
| (dle) | 16 | 0020 | 0x10 | 0 | 48 | 0060 | 0x30 | P | 80 | 0120 | 0x50 | p | 112 | 0160 | 0x70 |
| (dc1) | 17 | 0021 | 0x11 | 1 | 49 | 0061 | 0x31 | Q | 81 | 0121 | 0x51 | q | 113 | 0161 | 0x71 |
| (dc2) | 18 | 0022 | 0x12 | 2 | 50 | 0062 | 0x32 | R | 82 | 0122 | 0x52 | r | 114 | 0162 | 0x72 |
| (dc3) | 19 | 0023 | 0x13 | 3 | 51 | 0063 | 0x33 | S | 83 | 0123 | 0x53 | s | 115 | 0163 | 0x73 |
| (dc4) | 20 | 0024 | 0x14 | 4 | 52 | 0064 | 0x34 | T | 84 | 0124 | 0x54 | t | 116 | 0164 | 0x74 |
| (nak) | 21 | 0025 | 0x15 | 5 | 53 | 0065 | 0x35 | U | 85 | 0125 | 0x55 | u | 117 | 0165 | 0x75 |
| (syn) | 22 | 0026 | 0x16 | 6 | 54 | 0066 | 0x36 | V | 86 | 0126 | 0x56 | v | 118 | 0166 | 0x76 |
| (etb) | 23 | 0027 | 0x17 | 7 | 55 | 0067 | 0x37 | W | 87 | 0127 | 0x57 | w | 119 | 0167 | 0x77 |
| (can) | 24 | 0030 | 0x18 | 8 | 56 | 0070 | 0x38 | X | 88 | 0130 | 0x58 | x | 120 | 0170 | 0x78 |
| (em) | 25 | 0031 | 0x19 | 9 | 57 | 0071 | 0x39 | Y | 89 | 0131 | 0x59 | y | 121 | 0171 | 0x79 |
| (sub) | 26 | 0032 | 0x1a | : | 58 | 0072 | 0x3a | Z | 90 | 0132 | 0x5a | z | 122 | 0172 | 0x7a |
| (esc) | 27 | 0033 | 0x1b | ; | 59 | 0073 | 0x3b | [ | 91 | 0133 | 0x5b | { | 123 | 0173 | 0x7b |
| (fs) | 28 | 0034 | 0x1c | < | 60 | 0074 | 0x3c | \ | 92 | 0134 | 0x5c | \| | 124 | 0174 | 0x7c |
| (gs) | 29 | 0035 | 0x1d | = | 61 | 0075 | 0x3d | ] | 93 | 0135 | 0x5d | } | 125 | 0175 | 0x7d |
| (rs) | 30 | 0036 | 0x1e | > | 62 | 0076 | 0x3e | ^ | 94 | 0136 | 0x5e | ~ | 126 | 0176 | 0x7e |
| (us) | 31 | 0037 | 0x1f | ? | 63 | 0077 | 0x3f | _ | 95 | 0137 | 0x5f | (del) | 127 | 0177 | 0x7f |

Characters which appear as names in parentheses (e.g., (nl)) are non-printing characters.

| ASCII Name | Description | C Escape Sequence | | | |
|---|---|---|---|---|---|
| nul | null byte | \0 | nl | newline | \n |
| bel | bell character | \a | cr | carriage return | \r |
| bs | backspace | \b | vt | vertical tab | |
| ht | horizontal tab | \t | esc | escape | |
| np | formfeed | \f | sp | space | |