Kriptografi Klasik

Presented by

Dr. R. Rizal Isnanto, S.T., M.M., M.T.

Kriptografi klasik

- Ada 5 algoritma kriptografi klasik yang dipelajari di mata kuliah ini.
- Kelima algoritma tersebut adalah:
  - Caesar cipher
  - Vigenere cipher
  - Matrix encryption
  - Playfair
  - Vernam cipher

1. Caesar Cipher

- Ditemukan oleh Raja Romawi, Julius Caesar.
- Sistem ini mengharuskan kita menghitung pengganti sebuah huruf dengan menggeser posisi urutannya sesuai dengan kunci.
- Yang dipakai adalah huruf alfabet.

Langsung ke contohnya

- Misal :

  kita mempunyai plaintext “GADJAH”

  kuncinya = 6.

  - Bagaimana penyelesaiannya?

    sebelum membuat tabel penyelesaian, kita harus mengetahui konsepnya terlebih dahulu, inti dari caesar cipher adalah pergeseran posisi yang berurutan sesuai dengan jumlah nilai kuncinya.

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	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

Jawabannya....

Setelah diurutkan, jawabannya adalah “AUXDUB”

Vigenere cipher

- Merupakan perkembangan ide dari Caesar Cipher.
- Cipher ini menggunakan sebuah tabel yang berbentuk matriks alfabet, yang berisikan baris-baris alfabet yang telah digeser dari 1-25.
- Setiap baris dan kolom mendapat indeks sebuah huruf alfabet.
- Proses enkripsi dilakukan dengan cara mengambil karakter pertama kunci sebagai indeks baris dan karakter pertama plaintext sebagai indeks kolom.
- Elemen matriks yang ditunjuk oleh baris kolom tersebut merupakan karakter pada ciphertext.
- Proses diulangi sampai plaintext habis, jika kunci lebih pendek dari plaintext maka kunci boleh diulang.

Contoh soal:

- Misal : ada kunci = “gadjah”

  dan plaintext-nya = “helloelephant”

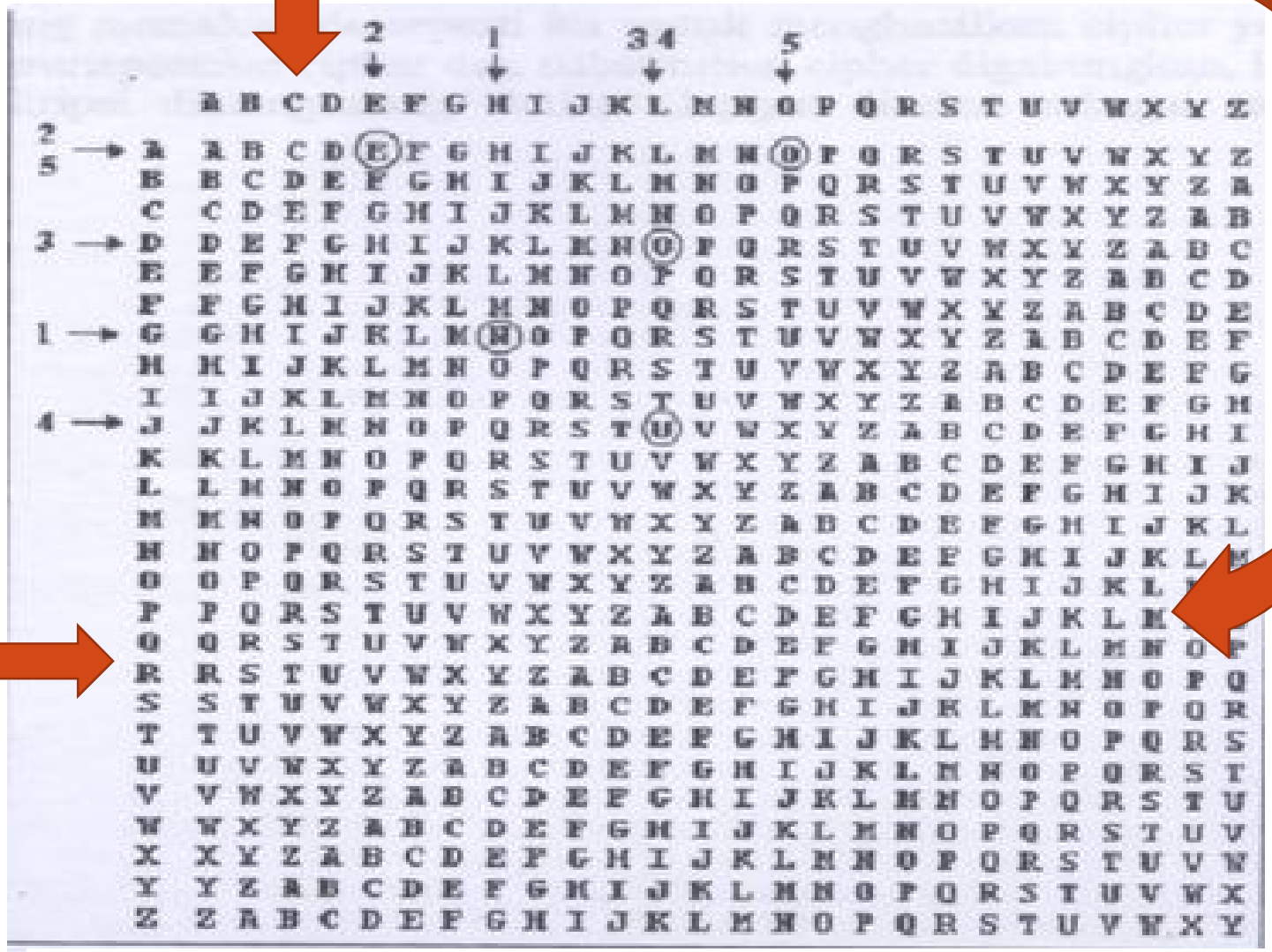
  *karena kunci lebih pendek dari plaintext maka dirangkaikan beberapa kali……

Plaintext	h	e	l	l	o	e	l	e	p	h	a	n	t
Key	g	a	d	j	a	h	g	a	d	j	a	h	g
ciphertext	n	e	o	u	o	l	r	e	s	q	a	u	z

Plaintext

Ciphertext

Kunci



Plaintext	h	e	l	l	o	e	l	e	p	h	a	n	t
Key	g	a	d	j	a	h	g	a	d	j	a	h	g
ciphertext	n	e	o	u	o	l	r	e	s	q	a	u	z

Matrix encryption

- Ide : plaintext diletakkan pada matriks bujursangkar.
- Contoh : UNIVERSITAS DIPONEGORO

  * spasi pada plaintext diabaikan.
- Jumlah karakter contoh plaintext di atas adalah 21 karakter, maka matriks yang dipakai adalah $25 = 5^2$.

Matriksnya menjadi:

1	2	3	4	5
U	N	I	V	E
R	S	I	T	A
S	D	I	P	O
N	E	G	O	R
O	X	X	X	X

- Misal : kunci = 41325 (berdasar kolom)
- Jadi chipertext =

VTPOX URSNO IIIGX NSDEX EAORX

dan digabung menjadi :

VTPOXURSNOIIIGXNSDEXEAORX

- Dekripsi :
  - Bagi 1 blok untuk 5 huruf
  - Buat matriks berdasar kolom (atas ke bawah)
  - Urutkan dalam posisi 12345
  - Baca per baris (UNIVERSITASDIPONEGORO)

PLAYFAIR

- Ide : buat matriks 5 x 5 untuk diisi 26 karakter,

  *ada 1 sel pada kolom tersebut diisi oleh 2 karakter : I/J

- Contoh : kunci = GADJAH

1	2	3	4	5
G	A	D	J/I	H
B	C	E	F	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

- Jika plaintext = KRIPTOGRAFI
- KR IP TO GR AF IX

  * bila jumlah karakter pada plaintext tersebut ganjil seperti contoh di atas maka ditambah karakter X untuk menggenapinya.
- Buat kunci, misal : GADJAH
- Buat sel matriks 5 x 5 (=25)

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

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

m	K	R	I	P	T	O	G	R	A	F	I	X
c	U	C	O	H	Y	T	Q	A	C	J	Y	D

Contoh:

- Plaintext : KRIPTOGRAFI → KR IP TO GR AF IX
- Kunci: GADJAH

  dienkripsi menjadi
- Ciphertext : UC OH YT QA CJ YD → UCOHYTQACJYD

  kemudian dideskripsikan lagi menjadi

  KR JP TO GR AF JX → KRJPTOGRAFJX

Vernam cipher

- Memanfaatkan konsep bit dan logika XOR untuk memecahkan kodenya.
- Contoh :
  - Plaintext : KAMU
  - Kunci : AKU
    - Bagaimana mencari ciphertextnya?
      - Untuk mencarinya kita ubah dulu plaintext dan kuncinya ke ASCII
      - K = (ASCII 75) = 01001011
      - A = (ASCII 65) = 01000001
      - M = (ASCII 77) = 01001101
      - U = (ASCII 85) = 01010101

- Maka plaintextnya menjadi
  - 01001011010000010100110101010101

  Dan kuncinya menjadi
  - 01000001010010110101010 1

    oleh karena kunci lebih pendek dari plaintext maka kunci diulang agar panjangnya sesuai dengan plaintext-nya
  - 01000001010010110101010101000001

- Kemudian plaintext dan kunci di-XOR-kan
- P : 01001011010000010100110101010101
- K : 01000001010010110101010101000001 XOR
- C : 00001010000010100001100000010100
- ASCII→ bisa dicari (jika angkanya kecil, biasanya merupakan fungsi kontrol yang tidak bisa dicetak)

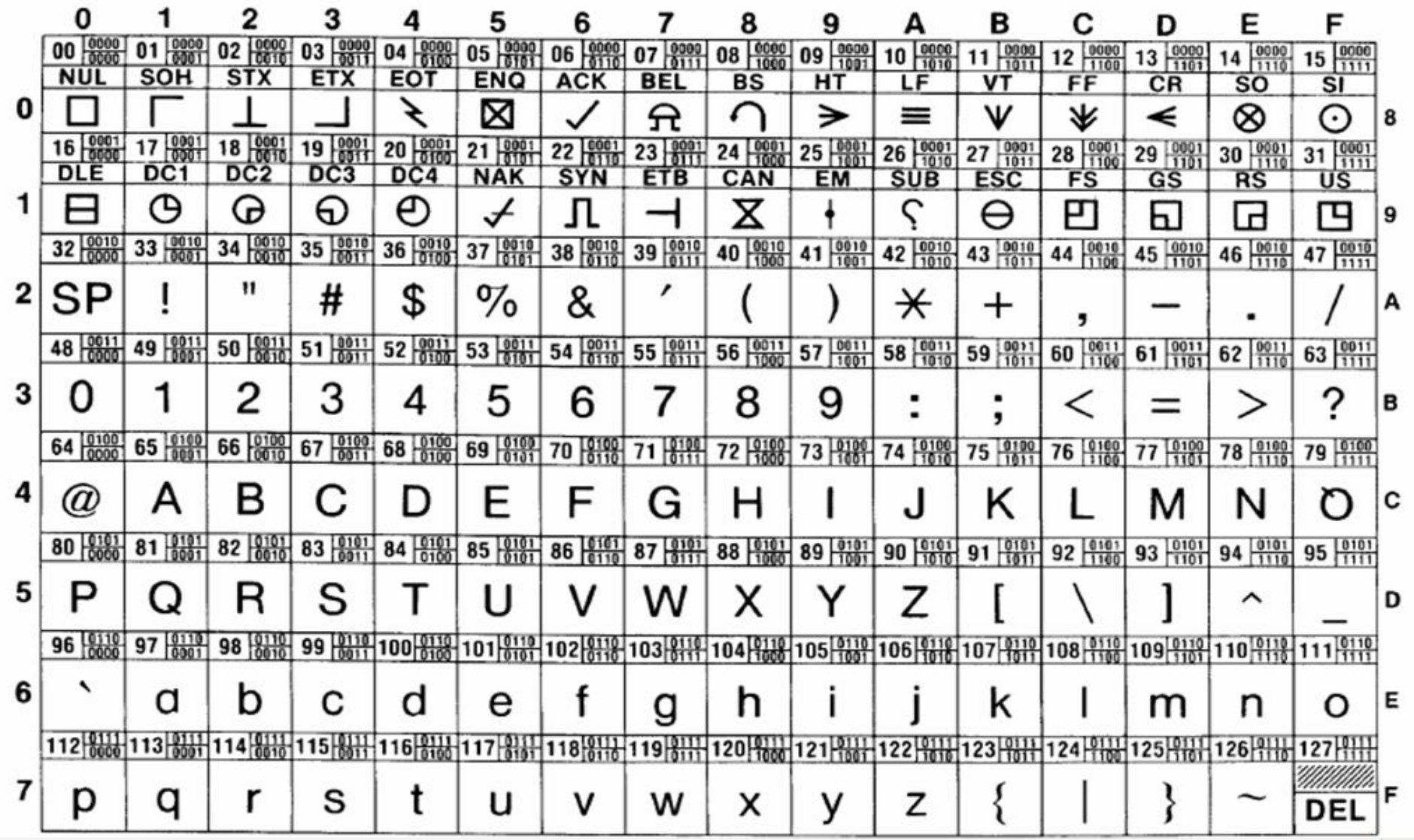
  00001010 = 10*d* → ?

  00001010 = 10*d* → ?

  00011000 = 24*d* → ?

  00010100 = 20*d* → ?
- Untuk proses deskripsi pesan juga melakukan operasi yang sama yaitu XOR antara cipher dan kuncinya maka didapat plaintext-nya.

TABEL ASCII


0 1 2 3 4 5 6 7 8 9 A B C D E F
00 NUL 01 SOH 02 STX 03 ETX 04 EOT 05 ENQ 06 ACK 07 BEL 08 BS 09 HT 10 LF 11 VT 12 FF 13 CR 14 SO 15 SI
16 DLE 17 DC1 18 DC2 19 DC3 20 DC4 21 NAK 22 SYN 23 ETB 24 CAN 25 EM 26 SUB 27 ESC 28 FS 29 GS 30 RS 31 US
32 SP 33 ! 34 " 35 # 36 $ 37 % 38 & 39 ′ 40 (41) 42 * 43 + 44 , 45 − 46 . 47 /
48 0 49 1 50 2 51 3 52 4 53 5 54 6 55 7 56 8 57 9 58 : 59 ; 60 < 61 = 62 > 63 ?
64 @ 65 A 66 B 67 C 68 D 69 E 70 F 71 G 72 H 73 I 74 J 75 K 76 L 77 M 78 N 79 O
80 P 81 Q 82 R 83 S 84 T 85 U 86 V 87 W 88 X 89 Y 90 Z 91 [92 \ 93] 94 ^ 95 _
96 ` 97 a 98 b 99 c 100 d 101 e 102 f 103 g 104 h 105 i 106 j 107 k 108 l 109 m 110 n 111 o
112 p 113 q 114 r 115 s 116 t 117 u 118 v 119 w 120 x 121 y 122 z 123 { 124 | 125 } 126 ~ 127 DEL
0 1 2 3 4 5 6 7 8 9 A B C D E F

- Terima kasih
- Ada pertanyaan?