

HERU ARBIANTO_22312004_IF22DX

Saya membuat fungsi kriptografi HillCipher, karena code ini bekerja di belakang layar atau BackEnd maka dokumentasinya saya lampirkan gambar saat saya mencoba menkonversikan rumus matematika ke bahasa pemrograman php.

Disini saya buat alurnya

Enkripsi :

1. Merubah Plaintext ke code ASCII 128
2. Penyesuaian panjang karakter plaintext (jika di mod 3 hasilnya $\neq 0$ maka tambahkan angka 0 di belakang karakter terakhir sampai mendapatkan hasil yang sesuai)
3. membagi code ASCII menjadi matriks array 2d
4. mengalikan code ASCII dengan matriks kunci
5. hasil perkalian dikembalikan ke array satu dimensi
6. kembalikan code ASCII ke plaintext

Dekripsi :

1. Merubah Plaintext ke code ASCII 128
2. Penyesuaian panjang karakter plaintext (jika di mod 3 hasilnya $\neq 0$ maka tambahkan angka 0 di belakang karakter terakhir sampai mendapatkan hasil yang sesuai)
3. mencari hasil determinan kunci
4. memodulo-kan hasil determinan kunci
5. mencari konfaktor kunci
6. mencari hasil Adjoin dari kunci. $\text{Adjoin} = (\text{transpose hasil konfaktor kunci})$
7. mencari persamaan modulo dengan algoritma Euclidean
8. mencari hasil invers
9. membagi code ASCII menjadi matriks array 2d
10. mengalikan code ASCII dengan matriks kunci
11. hasil perkalian dikembalikan ke array satu dimensi
12. kembalikan code ASCII ke plaintext

dokumentasi perumusan dihalaman berikutnya, mohon maaf jika dokumentasi sulit dipahami, karena memang hanya coret coretan yang penting hasilnya akurat

Perulangan Perkecilan

$$A \begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \\ 20 & 21 & 22 \end{bmatrix}$$

$$B \begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \end{bmatrix}$$

$$\begin{aligned} j0 &= j0 = k0 \ k1 \ k2 \\ j1 &= k0 \ k1 \ k2 \\ j2 &= k0 \ k1 \ k2 \end{aligned}$$

$$\begin{aligned} j1 &= j0 = k0 \ k1 \ k2 \\ j1 &= k0 \ k1 \ k2 \\ j2 &= k0 \ k1 \ k2 \end{aligned}$$

$$\begin{aligned} &00 \times 00 + 01 \times 01 + 02 \times 02 \\ &10 \times 00 + 11 \times 01 + 12 \times 02 \\ &20 \times 00 + 21 \times 01 + 22 \times 02 \end{aligned}$$

$$A[j][k] \times B[i][k]$$

$$\begin{aligned} &A[0][0] \times B[0][0] \\ &A[0][1] \times B[0][1] \\ &A[0][2] \times B[0][2] \end{aligned}$$

$$A[j_0][k_2] \times [i_0][k_2]$$

Per 2

$$A[j_1][k_0] \times [i_0][k_2]$$

Det kunci Matrik

$$\begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \\ 20 & 21 & 22 \end{bmatrix} \begin{bmatrix} 00 & 01 \\ 10 & 11 \\ 20 & 21 \end{bmatrix}$$

$$\begin{bmatrix} s1 & 11 \\ s2 & 12 \end{bmatrix} = A$$

$$\text{Det} = \begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \\ 20 & 21 & 22 \end{bmatrix} \begin{bmatrix} 00 & 01 \\ 10 & 11 \\ 20 & 21 \end{bmatrix}$$

$$\begin{aligned} 00 &= 00 \\ 10 &= 01 \\ 20 &= 02 \end{aligned}$$

0 0

0 1

Mercuri A0J

$$\begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \\ 20 & 21 & 22 \end{bmatrix} \begin{bmatrix} 22 & 31 & 20 \\ 11 & 25 & 6 \\ 7 & 8 & 9 \end{bmatrix} = \begin{bmatrix} 00 & 01 & 02 \\ 10 & 11 & 12 \\ 20 & 21 & 22 \end{bmatrix}$$

~~25x9 - 18.6~~

$$A = \begin{bmatrix} 11 & 12 \\ 21 & 22 \end{bmatrix}$$

$$D = \begin{bmatrix} 01 & 02 \\ 21 & 22 \end{bmatrix}$$

$$g = \begin{bmatrix} 01 & 02 \\ 11 & 12 \end{bmatrix}$$

$$\left[\begin{bmatrix} 10 \\ 20 \end{bmatrix} \times \begin{bmatrix} 12 \\ 22 \end{bmatrix} \right] \cdot 5 = \begin{bmatrix} 00 \\ 01 \end{bmatrix} \times \begin{bmatrix} 02 \\ 12 \end{bmatrix} \cdot 1 = \begin{bmatrix} 00 \\ 10 \end{bmatrix}$$

$$\left[\begin{bmatrix} 10 \\ 20 \end{bmatrix} \times \begin{bmatrix} 12 \\ 22 \end{bmatrix} \right] \cdot 5 = \begin{bmatrix} 00 \\ 01 \end{bmatrix} \times \begin{bmatrix} 02 \\ 12 \end{bmatrix} \cdot 1 = \begin{bmatrix} 00 \\ 10 \end{bmatrix}$$

$$00 = 00$$

$$10 = 01$$

$$01 = 02$$

R44-102

$$\begin{bmatrix} 2 & 2 & 3 \\ 1 & 2 & 0 \\ 0 & 4 & 5 \end{bmatrix} \times \begin{bmatrix} 72 \\ 72 \\ 72 \end{bmatrix} = \begin{bmatrix} 21.72 + 28.72 + 3.72 \\ 16.72 + 2.72 + 0.72 \\ 0.72 + 4.72 + 5.72 \end{bmatrix}$$

$$\begin{pmatrix} 504 \\ 216 \\ 648 \end{pmatrix} = \begin{pmatrix} 72 \\ 72 \\ 0 \end{pmatrix} = \begin{bmatrix} 2.72 + 2.72 + 3.0 \\ 1.72 + 2.72 + 0.0 \\ 0.72 + 4.72 + 5.0 \end{bmatrix} \begin{pmatrix} 89 \\ 288 \\ 216 \\ 288 \end{pmatrix}$$

$$128 = 2^{2^2} (5) + 18 \frac{6}{132}$$

$17 \cdot 2 = 34$
 $34 + 9 = 43$
 $43 \cdot 2 = 86$
 $86 + 22 = 108$
 $108 \cdot 2 = 216$
 $216 + 29 = 245$
 $245 \cdot 2 = 490$
 $490 + 22 = 512$
 $512 \cdot 2 = 1024$
 $1024 + 29 = 1053$
 $1053 \cdot 2 = 2106$
 $2106 + 22 = 2128$
 $2128 \cdot 2 = 4256$
 $4256 + 29 = 4285$
 $4285 \cdot 2 = 8570$
 $8570 + 22 = 8592$
 $8592 \cdot 2 = 17184$
 $17184 + 29 = 17213$
 $17213 \cdot 2 = 34426$
 $34426 + 22 = 34448$
 $34448 \cdot 2 = 68896$
 $68896 + 29 = 68925$
 $68925 \cdot 2 = 137850$
 $137850 + 22 = 137872$
 $137872 \cdot 2 = 275744$
 $275744 + 29 = 275773$
 $275773 \cdot 2 = 551546$
 $551546 + 22 = 551568$
 $551568 \cdot 2 = 1103136$
 $1103136 + 29 = 1103165$
 $1103165 \cdot 2 = 2206330$
 $2206330 + 22 = 2206352$
 $2206352 \cdot 2 = 4412704$
 $4412704 + 29 = 4412733$
 $4412733 \cdot 2 = 8825466$
 $8825466 + 22 = 8825488$
 $8825488 \cdot 2 = 17650976$
 $17650976 + 29 = 17651005$
 $17651005 \cdot 2 = 35302010$
 $35302010 + 22 = 35302032$
 $35302032 \cdot 2 = 70604064$
 $70604064 + 29 = 70604093$
 $70604093 \cdot 2 = 141208186$
 $141208186 + 22 = 141208208$
 $141208208 \cdot 2 = 282416416$
 $282416416 + 29 = 282416445$
 $282416445 \cdot 2 = 564832890$
 $564832890 + 22 = 564832912$
 $564832912 \cdot 2 = 1129665824$
 $1129665824 + 29 = 1129665853$
 $1129665853 \cdot 2 = 2259331706$
 $2259331706 + 22 = 2259331728$
 $2259331728 \cdot 2 = 4518663456$
 $4518663456 + 29 = 4518663485$
 $4518663485 \cdot 2 = 9037326970$
 $9037326970 + 22 = 9037326992$
 $9037326992 \cdot 2 = 18074653984$
 $18074653984 + 29 = 18074654013$
 $18074654013 \cdot 2 = 36149308026$
 $36149308026 + 22 = 36149308048$
 $36149308048 \cdot 2 = 72298616096$
 $72298616096 + 29 = 72298616125$
 $72298616125 \cdot 2 = 144597232250$
 $144597232250 + 22 = 144597232272$
 $144597232272 \cdot 2 = 289194464544$
 $289194464544 + 29 = 289194464573$
 $289194464573 \cdot 2 = 578388929146$
 $578388929146 + 22 = 578388929168$
 $578388929168 \cdot 2 = 1156777858336$
 $1156777858336 + 29 = 1156777858365$
 $1156777858365 \cdot 2 = 2313555716730$
 $2313555716730 + 22 = 2313555716752$
 $2313555716752 \cdot 2 = 4627111433504$
 $4627111433504 + 29 = 4627111433533$
 $4627111433533 \cdot 2 = 9254222867066$
 $9254222867066 + 22 = 9254222867088$
 $9254222867088 \cdot 2 = 18508445734176$
 $18508445734176 + 29 = 18508445734205$
 $18508445734205 \cdot 2 = 37016891468410$
 $37016891468410 + 22 = 37016891468432$
 $37016891468432 \cdot 2 = 74033782936864$
 $74033782936864 + 29 = 74033782936893$
 $74033782936893 \cdot 2 = 148067565873786$
 $148067565873786 + 22 = 148067565873808$
 $148067565873808 \cdot 2 = 296135131747616$
 $296135131747616 + 29 = 296135131747645$
 $296135131747645 \cdot 2 = 592270263495290$
 $592270263495290 + 22 = 592270263495312$
 $592270263495312 \cdot 2 = 1184540526990624$
 $1184540526990624 + 29 = 1184540526990653$
 $1184540526990653 \cdot 2 = 2369081053981306$
 $2369081053981306 + 22 = 2369081053981328$
 $2369081053981328 \cdot 2 = 4738162107962656$
 $4738162107962656 + 29 = 4738162107962685$
 $4738162107962685 \cdot 2 = 9476324215925370$
 $9476324215925370 + 22 = 9476324215925392$
 $9476324215925392 \cdot 2 = 18952648431850784$
 $18952648431850784 + 29 = 18952648431850813$
 $18952648431850813 \cdot 2 = 37905296863701626$
 $37905296863701626 + 22 = 37905296863701648$
 $37905296863701648 \cdot 2 = 75810593727403296$
 $75810593727403296 + 29 = 75810593727403325$
 $75810593727403325 \cdot 2 = 151621187454806650$
 $151621187454806650 + 22 = 151621187454806672$
 $151621187454806672 \cdot 2 = 303242374909613344$
 $303242374909613344 + 29 = 303242374909613373$
 $303242374909613373 \cdot 2 = 606484749819226746$
 $606484749819226746 + 22 = 606484749819226768$
 $606484749819226768 \cdot 2 = 1212969499638453536$
 $1212969499638453536 + 29 = 1212969499638453565$
 $1212969499638453565 \cdot 2 = 2425938999276907130$
 $2425938999276907130 + 22 = 2425938999276907152$
 $2425938999276907152 \cdot 2 = 4851877998553814304$
 4

Subtask

$$\begin{cases} 2 = 18 - 4(22 - (18 \cdot 1)) \\ 2 = 18 - 88 + 72 = 1 \\ 2 = 18 - 4(22 - (18 \cdot 1)) \end{cases}$$

$$128 = 22 \times 5 + 18 \Rightarrow 18 = 128 - (22 \cdot 5)$$

$$88 \quad 22 = 18 \times 1 + 4 \Rightarrow 4 = 22 - (18 \cdot 1)$$

$$215 \quad 18 = 4 \times 4 + 2 \Rightarrow 2 = 18 - (4 \cdot 4)$$

$$88 \quad 4 = 2 \times 2$$

$$r_1 = 22 \quad Q_1 = 5$$

$$r_2 = 18 \quad Q_1 = 1$$

$$r_3 = 4 \quad Q_1 = 4$$

$$r_4 = 2 \quad Q_1 = 2$$

$$r_5 = 0, t_1 = 1$$

0.49/15

22 31 0
 - 1 2 -
 0 - 2

22 31 20
 0 4 5
 6 + 8
 2 2
 0 6

$22 = 2 \times 12$

2 2
 4 18
 3
 8 8
 22x

$22 \bmod 28$

48 31 20
 6 4 5
 2 + 8 9
 20

277
 45

1385
 308
 4 8 6 5

277
 45
 1385
 108

2465