Date .....

Phương 1:

- Bài 10. a=3 k=22 / 25

k_i = 10110 T=4

b=1 ; A=3

i=0 $A = 3^2 \bmod 23 = 9$

$k_0 = 0$ b = 1

i=1 $A = 9^2 \bmod 23 = 12$

$k_1 = 1$ $b = 1.12 \bmod 23 = 12$

i=2 $A = 12^2 \bmod 23 = 6$

$k_2 = 1$; $b = 12.6 \bmod 23 = 3$

i=3 $A = 6^2 \bmod 23 = 13$

$k_3 = 0$ b = 3

i=4 $A = 13^2 \bmod 23 = 8$

$k_4 = 1$, $b = 8.3 \bmod 23 = 1$

- Bài 5. 145.

Theo đề X và Y là biến ngẫu nhiên nên ta có ($x \in X$ và $y \in Y$)

$$H(X,Y) = -\sum_y \sum_x p(x,y) \log_2 p(x,y)$$

mà $p(x,y) = p(x/y) \cdot p(y)$ nên

$$H(X,Y) = -\sum_y \sum_x p(x/y) \cdot p(y) \log_2 p(y) \cdot p(x/y)$$

$$= -\sum_y \sum_x p(x/y) \cdot p(y) \log_2 p(y) - \sum_y \sum_x p(x,y) p(y) \log_2 p(y)$$

Ta xét

$$-\sum_y \sum_x p(x/y) p_y \log_2 p(y)$$

$$= -\sum_y p(y) \log_2 p(y) \quad \text{vì } \sum_x p(x/y) = 1 \ \forall x,y$$

$$= H(Y)$$

$$-\sum_y \sum_x p(x/y) p(y) \cdot \log_2 p(x/y) = H(X/Y)$$

Vậy $H(X,Y) = H(Y) + H(X/Y)$

mà $H(XY) = H(Y) + H(X|Y)$

$\Rightarrow H(Y) + H(X|Y) \le H(X) + H(Y)$

$\Rightarrow H(X|Y) \le H(X)$

chỉ xảy ra khi X, Y độc lập

- Bài 9: Euclide

$a = 1573$ $b = 308$

đặt $(A_1\ A_2\ A_3) = (1, 0, 1573)$

$(B_1\ B_2\ B_3) = (0, 1, 308)$

$Q = A_3 / B_3 = 5$

đặt $(A_1, A_2, A_3) = (0, 1, 308)$

$(B_1, B_2, B_3) = (1, -4, 33)$

$Q = 9$

$(A_1, A_2, A_3) = (1, -4, 33)$

$(B_1, B_2, B_3) = (-9, 37, 11)$

$Q = 3$

$(A_1, A_2, A_3) = (-9, 37, 11)$

$(B_1, B_2, B_3) = (28, -115, 0)$

Vì $B_3 = 0 \Rightarrow$ UCLN$(1573, 308) = A_3 = 11$

- Bài 8: Tỉ mã toàn

$p_C(1) = \frac{1}{2} \cdot \frac{1}{3} + 1/6 \cdot 1/3 = 4/18$

$p_C(2) = (1/3 + 1/2) \cdot 1/3 = 5/18$

$p_C(3) = 1 \cdot 1/3 = 1/3$

$p_C(4) = (1/3 + 1/6) \cdot 1/3 = 1/6$

P/ số p_S có thể trên bản rõ ở đề ra: bản bản mã

$p_S(a|1) = \frac{1/2 \cdot 1/3}{4/18} = 3/4$ $\quad p_S(a|2) = 3/5$

$p_S(b|2) = 2/5$

$p_S(c|1) = \frac{1/6 \cdot 1/3}{4/18} = 1/4$ $\quad p_S(c|2) = 0$

$p_S(b|1) = 0$ $\quad p_S(a|3) = 3/6$

$p_S(a|4) = 2/6$

$p_S(c|4) = 1/9$ $\quad p_S(b|4) = 2/3$ $\quad p_S$ ~~bảo~~ p_S $a|5 = 1/6$

Grand - Diện mạo mới

Date .....

$H(D) = -\frac{1}{2}\log_2 \frac{1}{2} - \frac{1}{3}\log_2 \frac{1}{3} - \frac{1}{6}\log_2 \frac{1}{6} = 1,46$

$H(C) = -\frac{4}{18}\log_2 \frac{4}{18} - \frac{5}{18}\log_2 \frac{5}{18} - \frac{6}{18}\log_2 \frac{6}{18} - \frac{3}{18}\log_2 \frac{3}{18}$

$= 1,565$

$H(K) = -3\,\frac{1}{3}\log_2 \frac{1}{3} \approx 1,585$

$H(K|C) = H(K) + H(D) - H(C)$

$\Rightarrow$ a, (D, C, K, F, I) là 1 bộ mã

$\approx 1,429$

$H(D|C) = -\sum_{y}\sum_{x} P(y)\, P(x|y)\log_2 P(x|y)$

$x \in D$ và $y \in C$

Với $P(C) = -3/4 \cdot \frac{4}{18}\log_2 3/4 - 0.\frac{4}{18}\frac{1}{4}\log_2 \frac{1}{4}$

$= 0,18$

Xét $P(C) = \frac{5}{18}\left[\frac{3}{5}\log_2 \frac{3}{5} + \frac{2}{5}\log \frac{2}{5}\right) = -0,29$

Với $P(C) = 0,45$

Với $P(C) = 0,15$

Vậy $H D/C = 1,05$

- Bài 11 / 45

1. $\frac{a}{p} = 1$ $(a \in Q)$
2. $b = 16$ ($b \in Q$, và $1 \le b \le p-1$)
3. $p - 1 = 36 = 2^2 \cdot 9$ ($s=2$; $t=9$)

Với $12-1$ mod 37 Áp dụng Thuật toán Euclide mở rộng

$a = 37$ $b = 12$. $x_2 = 1$ $x_1 = 0$. $y_2 = a\,y_1 = 1$

Với $b > 0$ $\begin{cases} a = 3 & b = 1 \quad x = -3 \quad y = 1 \\ a = 12 & b \ne 1 \quad x_2 = 1 \quad x_1 = -3 \\ & y_2 = 0 \quad y_1 = 1 \end{cases}$

Date .....

xét $b>0$ $\begin{cases} a=19 & r=0 \quad x=37 \quad y=-19 \\ a=1 & b=0 \quad r_2=-3 \quad y_2=1 \end{cases}$

Vậy $d=1 \quad x=-3 \quad y=1$

Hay $12^{-1}=34$ Cho $34 \equiv -3 \bmod 37$)

7. $a \in 169 \bmod 37 \Rightarrow a=1$

$r \in 185 \bmod 37 \quad r=7$

6. $i=1 \quad d=(7^1 \cdot 34)^2 \bmod 37=1$

return $7:7$

Vậy căn bậc 2 của $1 \bmod 37$ là $\{7;-7\}$

- Bài 19.

$\varphi(19)=18=1 \cdot 9^2$

Tìm các số hữu nguyên thuỷ sao cho

$x^{18/2} \bmod 37 \neq 1 \quad (=) \quad x^9 \bmod 37 \neq 1$

$x^{18/3} \bmod 37 \neq 1 \quad (=) \quad x^6 \bmod 37 \neq 1$

Với $a=2 \quad 2^9 \bmod 37 \neq 1$

$2^6 \bmod 37 \neq 1$

$\Rightarrow 2$ là căn số nguyên tố của Z^*19

Để UCLN $(i, \varphi(19))=1$ thì $i \in Z_{18}^*$

$Z_{18}^* \in \{1;3,5,7;11,13,17\}$

$2^1 \bmod 19=2 \quad 2^5 \bmod 19=13 \quad 2^7 \bmod 19=11$

$2^{11} \bmod 19=15 \quad 2^{13} \bmod 19=3 \quad 2^{17} \bmod 19=10$

Vậy các căn số nguyên thuỷ của nhóm Z_{19}^*

$\{2, 3, 10, 13, 14, 15\}$

- Bài 13.

nghịch đảo 3 trong Z_{31}

$3x=1 \pmod{31}$

$(=) \quad 3x-1=31k$

$(=) \quad x=21$

Date .....

• Bài 15

φ(450) φ(768)

a) 450 = $2^1 5^2 3^1$

φ(450) = 450 (1 - 1/2) * (1 - 1/5) * (1 - 1/3) =

b) φ(768) 768 = $2^8 3$

φ(768) = 768 (1 - 1/2) · (1 - 1/3) =

* Bài 16

Giải pt đồng dư

5x = 20 mod 6

6x = 6 mod 5

4x = 5 mod 7

x = 4 mod 6 (1)

x = 1 mod 5 (2)

x = 3 mod 7

M = 210 = 5 x 6 x 7

M1 = 35 M2 = 42 M3 = 30

$35 y_1 = 4 \mod 6$ (=) $y_1 = 2$

$42 y_2 = 1 \mod 5$ (=) $y_2 = 3$

$30 y_3 = 3 \mod 7$ (=) $y_3 = 5$

= 346 mod 210 = 136 mod 210

Grand - Diện mạo mới

Date .....

Bài 17: Euclide mở rộng

a) $17^{-1} \bmod 101$

Đặt $(A_1, A_2, A_3) = (1, 0, 101)$

$(B_1, B_2, B_3) = (0, 1, 17)$

Q = 5

$(A_1, A_2, A_3) = (0, 1, 17)$

$(B_1, B_2, B_3) = (1, -5, 16)$

Q = 1

$(A_1, A_2, A_3) = (-1, -5, 16)$

$(B_1, B_2, B_3) = (-1, 6, 1)$

Vì $B_3 = 1$ nên $17^{-1} \bmod 101 = B_2 = 6$.

b) $357^{-1} \bmod 1234$

Đặt $(A_1, A_2, A_3) = (1, 0, 1234)$

$(B_1, B_2, B_3) = (0, 1, 357)$

Q = 3

$(0, 1, 357)$

$(1, -3, 163)$

Q = 2

$(1, -3, 163)$

$(-2, 7, 31)$

Q = 5

$(-2, 7, 31)$

$(11, -38, 8)$

Q = 3

$(11, -38, 8)$

$(-35, 121, 7)$

Q = 1

$(-35, 121, 7)$

$(-46, -159, 1)$

$B_3 = 1 \Rightarrow 357^{-1} \bmod 1234 = B_2 = -159$

c) $3125^{-1} \bmod 9967$

Đặt $(A_1, A_2, A_3) = (0, 9967)$

$(B_1, B_2, B_3) = (0, 1, 3125)$

Q = 3

$(0, 1, 3125)$

$(1, -3, 622)$

Q = 5

$(1, -3, 622)$

$(-5, 16, 65)$

Q = 9

$(-5, 16, 65)$

$(46, -147, 28)$

Q = 2

$(46, -147, 28)$

$(-58, 310, 11)$

Q = 2

$(-58, 310, 11)$

$(240, -767, 5)$

Q = 2

$(240, -767, 5)$

$(-537, 1844, 1)$

$B_3 = 1 \Rightarrow 3125^{-1} \bmod 9967 = B_2 = 1844$