Subject Date

حل تکلیف سری اول مفاهیم پیشرفته رمزهای کامپیوتری

①

$f(x) = x^{۳} + x^{۲} + ۱$

| لگاریتمی | PB | NB |
|---|---|---|
| 0 | — | — |
| ۱ | ۱ | $x^{۴}+x^{۲}+x$ |
| $x$ | $x$ | $x$ |
| $x^{۲}$ | $x^{۲}$ ~~+~~ | $x^{۲}$ |
| $x^{۳}$ | $x^{۲}$ ~~+x~~ $+۱$ | $x^{۴}+x$ |
| $x^{۴}$ | $x^{۲}+x+۱$ | $x^{۴}$ |
| $x^{۵}$ | $x+۱$ | $x^{۴}+x^{۲}$ |
| $x^{۶}$ | $x^{۲}+x$ | $x^{۲}+x$ |
| ⋮ | ⋮ | ⋮ |
| $x^{۸}$ | $x$ | $x$ |
| ⋮ | ⋮ | ⋮ |
| $x^{۱۵}$ | $x$ | $x$ |

$$x^{۱۵} + x^{۸} + x^{۵} + x^{۳} + x^{۲} + ۱ =$$
$$\cancel{x} + \cancel{۱} + \cancel{x^{۴}} + \cancel{x^{۲}} + \cancel{x^{۴}} + \cancel{x} + \cancel{x^{۴}} + x^{۴}$$
$$+ x^{۲} + \cancel{x} = \boxed{x^{۴} + x^{۲}}$$

②

$p = ۲^{۲۲۴} - ۲^{۹۶} + ۱ \qquad B = ۲^{۳۲}$

$p = B^{۷} - B^{۳} + ۱ \qquad d = (d_{۱۳}\, d_{۱۲} \cdots d_{۱}\, d_{0})_B$

$B^{۷} = B^{۳} - ۱ \qquad d = d_{۱۳}B^{۱۳} + d_{۱۲}B^{۱۲} + \cdots + d_{۱}B + d_{0}$

$B^{۸} = B^{۴} - B \qquad d_{۱۳}B^{۱۳} = (-d_{۱۳}, d_{۱۳}, 0, 0, -d_{۱۳}, 0, 0)_B$

$B^{۹} = B^{۵} - B^{۲} \qquad d_{۱۲}B^{۱۲} = (0, -d_{۱۲}, d_{۱۲}, 0, 0, -d_{۱۲}, 0)_B$

$B^{۱۰} = B^{۶} - B^{۳} \qquad d_{۱۱}B^{۱۱} = (0, 0, -d_{۱۱}, d_{۱۱}, 0, 0, -d_{۱۱})$

$B^{۱۱} = B^{۷} - B^{۴} = B^{۳} - ۱ - B^{۴} \qquad d_{۱۰}B^{۱۰} = (d_{۱۰}, 0, 0, -d_{۱۰}, 0, 0, 0)$

$B^{۱۲} = B^{۸} - B^{۵} = B^{۴} - B - B^{۵} \qquad d_{۹}B^{۹} = (0, d_{۹}, 0, 0, -d_{۹}, 0, 0)$

$B^{۱۳} = B^{۹} - B^{۶} = B^{۵} - B^{۲} - B^{۶} \qquad d_{۸}B^{۸}$

s.a.m

$d_{۷}B^{۷}$

Scanned by CamScanner

Subject:

Date:

$g=(d_{۶},d_{۵},d_{۴},d_{۳},d_{۲},d_{۱},d_{۰})$

$h=(-d_{۱۳},d_{۱۳},-d_{۱۱},d_{۱۱},۰,-d_{۱۳},۰,-d_{۱۱})$

$1/۲-1/۴=1/۴$ $\qquad$ $1/۲,1/۴=؟$ $\qquad$ ۳

$1/۲=۲^{-1}\Rightarrow ۴$ $\qquad$ $1/۲-1/۴=۴-۲=۲$ ✓

$1/۴=۴^{-1}\Rightarrow ۲$

مثال) $1/۶-1/۴=1/۱۲\rightarrow ۵-۲=۳$ ✓

$C=A\circ B \bmod f(x)$ $\qquad$ $D=A^{۲} \bmod f(x)$ $\qquad$ ۴

$f(x)=x^{۳}+x^{۲}+1$

$A=a_{۲}x^{۴}+a_{۱}x^{۳}+a_{۰}x$

$B=b_{۲}x^{۴}+b_{۱}x^{۳}+b_{۰}x$

$$A\circ B=a_{۲}b_{۰}x^{۵}+a_{۱}b_{۰}x^{۴}+a_{۰}b_{۰}x^{۲}+a_{۲}b_{۱}\overset{(x^{۳}+x)}{\cancel{x^{۷}}}+a_{۱}b_{۱}x^{۴}+a_{۰}b_{۱}\overset{(x^{۴}+x)}{\cancel{x^{۴}}}$$
$$+a_{۲}b_{۲}x^{۸}+a_{۱}b_{۲}x^{۷}+a_{۰}b_{۲}x^{۵}=(\qquad)x^{۴}+(\qquad)x^{۲}+(\qquad)x$$

$C=A\circ B \bmod f(x)$ $\qquad$ $A^{۰}=Ax^{۰}$ $\qquad$ ۵

$A^{۱}=Ax^{۱}$

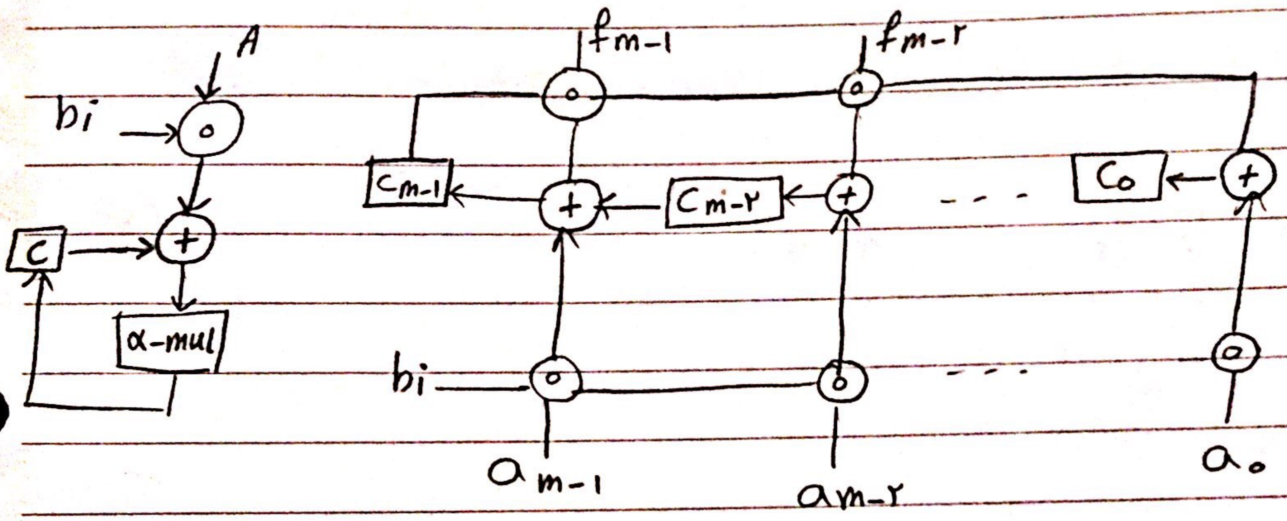
$L2H\rightarrow C=A(b_{۰}+b_{۱}x+\dots+b_{m-1}x^{m-1}) \bmod f(x)$

$C=Ab_{۰}+b_{۱}A^{۱}+\dots+b_{m-1}A^{m-1})$

s.a.m

Scanned by CamScanner

$H2L \longrightarrow C=((\cdots(((0+b_{m-1}A\alpha)+b_{m-۲}A)\alpha+b_{m-۳}A)\alpha\ldots b_0A)$



$AT=O(m^{۲})$

| | |
|---|---|
| m | زمن |
| ۲m-۱ | AND |
| ۲m | xoR |
| m | ff |