

$d = 11011011111001$

$i = 0$

while  $(d > 0)$  do

if  $(d \bmod 2) = 1$  then

$d_i = d \bmod 2^w$

$d = d - d_i$

else

$d_i = 0$

endif

$d = d/2$

$i = i + 1$

output  $(d_{i-1} \dots d_1 d_0)$

if  $(d \bmod 2^w) \geq 2^{w-1}$  8

Return  $(d \bmod 2^w) - 2^w$  16 16

else

$w = 4$

Return  $(d \bmod 2^w)$  16

1 0 0 1

0 0 -7 11

-10000

710170	777777	007
770777	000000	
110111	000000	
110111	000000	
770111	000000	
770111	000000	
770777	000000	
110777	000000	
770111		
110000		
770		
11		

-7  
0  
0  
0  
0  
0  
0  
0  
0  
7  
0  
0  
0  
3

Window = 4

3 000 7 000 0000 -7

0011000 0117 00000000 1001

60 11

نفران  
عبر 3 اس

3 000 7 000 0000 -7

0101 000 1001 000 0000 1001

125A

عرب : 5 تا غایب  
4

نمبر

19

101 000 1001 0000 000 1001

NAF: 100010010 000 1001  
 $\rightarrow$  ~~100010010~~  $\leftrightarrow$   
 $\rightarrow$  ~~100010010~~  $\leftrightarrow$

طوب:  $E_4$

جذب: 15. طرز کار در RSA شبیه جذب است

2  $\leftrightarrow$  4 طوب  
 13  $\leftrightarrow$  3 جذب  
 4 = W  
 13  $\leftrightarrow$  3

ایزعلیات این طوب و جذبات  
 Pre-computation

NAF  $\rightarrow$  . 7  $\leftrightarrow$  -7  $\leftarrow$  W=3

1, -1, 3, -3, 5, 2, -2

5 1 01  
 1 001  
 -1 001  
 -5 101  
 -3 101  
 3 101  
 6  $\rightarrow$  !  
 6  $\rightarrow$  !

$S_1 \downarrow$   $S_2$   
 $a \times a^2$   $a^3 \times a^2$   $a^{-1} \times a^{-2}$   $a^{-3} \times a^{-2}$   
 $M_1$   $M_2$   $M_2$   $M_4$   
 15

$$x^6 + x^4 + x^3 + x + 1$$

$$A^{1/2} = (x^6 + x^4 + 1)^{1/2} + (x(x^2 + 1))^{1/2} =$$

$$x^3 + x^2 + 1 + x^{1/2}(x+1)$$

$$x^7 \equiv x^2 \pmod{x^6 + x^4 + x^3 + x + 1} \Rightarrow x \equiv x^2 \pmod{x^6 + x^4 + x^2}$$

$$\Rightarrow A^{1/2} = x^3 + x^2 + 1 + (x^4 + x^2)(x+1) =$$

$$\cancel{x^5 + x^2 + 1} + x^5 + x^4 + \cancel{x^2} = x^5 + x^4 + 1$$



