Homework Assignment 03

Machiry Aravind Kumar

UCSB

1 Problem 1

Consider the exponent d = 49 = (110001). Show the steps and all intermediate powers in the computation of m^d for the algorithms

1.1 the left-to-right binary method

i	e_i	Step 2a	Step 2b
4	1	$(m)^2 = m^2$	$m^2.m = m^3$
3	0	$(m^3)^2 = m^6$	m^6
2	0	$(m^6)^2 = m^{12}$	m^{12}
1	0	$(m^{12})^2 = m^{24}$	m^{24}
0	1	$(m^{24})^2 = m^{48}$	$m^{48}.m = m^{49}$

1.2 the right-to-left binary method

$R_0 = 1, R_1 = m, i = 0$

i	d_i	R_0	R_1
0	1	1.m	m^2
1	0	m	$(m^2)^2$
2	0	m	$(m^4)^2$
3	0	m	$(m^8)^2$
4	1	$m.m^{16}$	$(m^{16})^2$
5	1	$m^{17}.m^{32}$	$(m^{32})^2$

$R_0 = m^{49}$

1.3 the square-and-multiply-always algorithm

$R_0 = 1, R_1 = 1$

i	d_i	b	R_0	R_b
5	1	0	$R_0 = 1^2$	$R_0 = 1.m$
4	1	0	$R_0 = m^2$	$R_0 = m^2.m$
3	0	1	$R_0 = (m^3)^2$	$R_1 = 1.m$
2	0	1	$R_0 = (m^6)^2$	$R_1 = m.m$
1	0	1	$R_0 = (m^{12})^2$	$R_1 = m^2.m$
0	1	0	$R_0 = (m^{24})^2$	$R_0 = m^{48}.m$

$R_0 = m^{49}$

1.4 the Montgomery powering ladder

$R_0 = 1, R_1 = m$

i	d_i	b	R_b	R_{d_i}
5	1	0	$R_0 = 1.m$	$R_1 = m^2$
4	1	0	$R_0 = m.m^2$	$R_1 = (m^2)^2$
3	0	1	$R_1 = m^3.m^4$	$R_0 = (m^3)^2$
2	0	1	$R_1 = m^6.m^7$	$R_0 = (m^6)^2$
1	0	1	$R_1 = m^{12}.m^{13}$	$R_0 = (m^{12})^2$
0	1	0	$R_0 = m^{24}.m^{25}$	$R_1 = (m^{25})^2$

$R_0 = m^{49}$

1.5 the Atomic square-and-multiply algorithm

$R_0 = 1, R_1 = m$

i	d_i	b_{before}	R_b	R_0	b_{after}
5	1	0	$R_0 = 1$	1.1	1
5	1	1	$R_1 = m$	1.m	0
4	1	0	$R_0 = m$	m.m	1
4	1	1	$R_1 = m$	$m^2.m$	0
3	0	0	$R_0 = m^3$	$m^3.m^3$	0
2	0	0	$R_0 = m^6$	$m^6.m^6$	0
1	0	0	$R_0 = m^{12}$	$m^{12}.m^{12}$	0
0	1	0	$R_0 = m^{24}$	$m^{24}.m^{24}$	1
0	1	1	$R_1 = m$	$m^{48}.m$	0

$R_0 = m^{49}$

1.6 the Atomic right-to-left algorithm

$R_0 = 1, R_1 = m, b = 1, i = 0$

i	d_i	$b = b \bigoplus d_i$	R_b
0	1	0	$R_0 = 1.m$
0	1	1	$R_1 = m.m$
1	0	1	$R_1 = m^2.m^2$
2	0	1	$R_1 = m^4.m^4$
3	0	1	$R_1 = m^8.m^8$
4	1	0	$R_0 = m.m^{16}$
4	1	1	$R_1 = m^{16}.m^{16}$
5	1	0	$R_0 = m^{17}.m^{32}$
5	1	1	$R_1 = m^{32}.m^{49}$

$R_0 = m^{49}$

2 Let an RSA key be determined by the parameters {p,q,n,$\phi(n)$,e,d} = {97,103,9991,9792,2015,8927}. Compute S = M^d (mod n) for M = 25 using each of these DPA-type countermeasure algorithms by selecting suitable random parameters:

2.1 Randomizing m, where e is known

Picking random r = 17.
$m^* = (17)^{2015}.25 mod(9991) = 7111$.
S* = $(7111)^{8972} mod(9991) = 6660$.
$r^{-1} = 4114$.
$S = 6660.4114$ mod (9991) = 7406.

i	j	Step	(C,S)	Partial t
0	0	$t_0 + a_0b_0 + C$	(0,*)	000000
		0 + 6*5 + 0	(3,0)	00000**0**
	1	$t_1 + a_1b_0 + C$		
		0 + 5*5 + 3	(2,8)	0000**8**0
	2	$t_2 + a_2b_0 + C$		
		0 + 4*5 + 2	(2,2)	000**2**80
				00**2**280
1	0	$t_1 + a_0b_1 + C$	(0,*)	
		8 + 6*5 + 0	(3,8)	0022**8**0
	1	$t_2 + a_1b_1 + C$		
		2 + 5*5 + 3	(3,0)	002**0**80
	2	$t_3 + a_2b_1 + C$		
		2 + 4*5 + 3	(2,5)	00**5**080
				0**2**5080
2	0	$t_2 + a_0b_2 + C$	(0,*)	
		0 + 6*5 + 0	(3,0)	025**0**80
	1	$t_3 + a_1b_2 + C$		
		5 + 5*5 + 3	(3,3)	02**3**080
	2	$t_4 + a_2b_2 + C$		
		2 + 4*5 + 3	(2,5)	0**5**3080
				253080

3 Illustrate the steps of the standard squaring algorithm for computing c =a * a = 456 * 456

i	j	Step	(C,S)	Partial t
0	1	$\mathrm{t}_0 + a_0 a_0$		000000
		0 + 6*6	(3,6)	00000**6**
		$\mathrm{t}_1 + 2a_1 a_0 + C$	(3,*)	000006
		0 + 2*5*6 + 3	(6,3)	000**3**6
0	2	$\mathrm{t}_2 + 2a_2 a_0 + C$	(6,*)	000036
		0 + 2*4*6 + 6	(5,4)	000**4**36
				00**5**436
1	2	$\mathrm{t}_2 + a_1 a_1$		005436
		4 + 5*5	(2,9)	005**9**36
		$\mathrm{t}_3 + 2a_2 a_1 + C$	(2,*)	005936
		5 + 2*4*5 + 2	(4,7)	00**7**936
				0**4**7936
2	2	$\mathrm{t}_4 + a_2 a_2$		047936
		4 + 4*4	(2,0)	0**0**7936
				207936

4 Let r = 32, n = 21, a = 13, and b = 15. Compute $c = a * b * r^{-1}$ mod n using the standard Montgomery multiplication algorithm. Illustrate the steps and give all temporary results

iteration	q	g_0	g_1	u_0	u_1	v_0	v_1
0	-	32	21	1	0	0	1
1	1	21	11	0	1	1	-1
2	1	11	10	1	-1	-1	2
3	1	10	1	-1	2	2	-3
4	10	1	0	2	-21	-3	32
		•		•		•	

From Table **??**, GCD = 1, $r^{-1} = 2$, $n' = 3$.
Consider $\overline{x}$ = a = 13, such that x = $\overline{x} * r^{-1}$ mod n = 5. $\overline{y}$ = b = 15, such that y = $\overline{y} * r^{-1}$ mod n = 9.
Now, $a * b * r^{-1}$ mod n is same as $\overline{x} * \overline{y} * r^{-1}$ mod n.
So, $a * b * r^{-1}$ mod n = $\overline{x} * \overline{y} * r^{-1}$ mod n = MonPro($\overline{x}$ = 13,$\overline{y}$ = 15).

4.1 function MonPro($\overline{a}$ = 13 , $\overline{b}$ = 15)

1. t = 13*15 = 195
2. m = (195*3) mod 32 = 9
3. u = (195 + 9 * 21) / 32 = 384/32 = 12
4. 12 < 21 **return** 12

Final result is : 12.

5 Let p = 29, a = 23, and g = 10. Compute g^a (mod p) using the binary method of exponentiation and the Montgomery multiplication where r = 32. Show the steps and temporary values.

Consider n=p=29, M=g=10, e=a=23.

iteration	q	g_0	g_1	u_0	u_1	v_0	v_1
0	-	32	29	1	0	0	1
1	1	29	3	0	1	1	-1
2	9	3	2	1	-9	-1	10
3	1	2	1	-9	10	10	-11
4	2	1	0	10	-29	-11	32
		•		•		•	

From Table **??**, GCD = 1, r^{-1} = 10, n' = 11.

- Step 2
  $\overline{M}$ = M * r mod n = 10 * 32 mod 29 = 1
- Step 3
  $\overline{C}$ = 1 * r mod n = 1 * 32 mod 29 = 3
- Step 4

e_i	Step 5	Step 6
1	MonPro(3,3) = 3	MonPro(1,3) = 1
0	MonPro(1,1) = 10	
1	MonPro(10,10) = 14	MonPro(1,14) = 24
1	MonPro(24,24) = 18	MonPro(1,18) = 6
1	MonPro(6,6) = 12	MonPro(1,12) = 4

$MonPro(3,3)$
t = 3 * 3 = 9
m = 9 * 11 mod 32 = 3
u = (9 + 3 * 29) / 32 = 3

$MonPro(1,3)$
t = 1 * 3 = 3
m = 3 * 11 mod 32 = 1
u = (3 + 1 * 29) / 32 = 1

$MonPro(1,1)$
t = 1 * 1 = 1
m = 1 * 11 mod 32 = 11
u = (1 + 11 * 29) / 32 = 10

$MonPro(10, 10)$
t = 10 * 10 = 100
m = 100 * 11 mod 32 = 12
u = (100 + 12 * 29) / 32 = 14

$MonPro(1, 14)$
t = 1 * 14 = 14
m = 14 * 11 mod 32 = 26
u = (14 + 26 * 29) / 32 = 24

$MonPro(24, 24)$
t = 24 * 24 = 576
m = 576 * 11 mod 32 = 0
u = (576 + 0 * 29) / 32 = 18

$MonPro(1, 18)$
t = 1 * 18 = 18
m = 18 * 11 mod 32 = 6
u = (18 + 6 * 29) / 32 = 6

$MonPro(6, 6)$
t = 6 * 6 = 36
m = 36 * 11 mod 32 = 12
u = (36 + 12 * 29) / 32 = 12

$MonPro(1, 12)$
t = 1 * 12 = 12
m = 12 * 11 mod 32 = 4
u = (12 + 4 * 29) / 32 = 4

- Step 7
  C = MonPro(4,1) = 11

Result of 10^{23} (mod 29) = **11**

6 Let an RSA key be determined by the parameters {p,q,n,e,d} = {17,23,391,29,85}. Compute S = M^d (mod n) for M = 175 with and without the Chinese remainder theorem and the binary exponentiation.

6.1 Chinese remainder theorem

d_1 = 85 mod (16) = 5
d_2 = 85 mod (22) = 19

iteration	quotient	g_0	g_1	u_0	u_1	v_0	v_1
0	-	23	17	1	0	0	1
1	1	17	6	0	1	1	-1
2	2	6	5	1	-2	-1	3
3	1	5	1	-2	3	3	-4
4	5	1	0	3	-17	-4	23
		•		•		•	

In Table **??**, Initial values of g_0 = q = 23 and g_1 = p = 17. This p^{-1} = -4 and q^{-1} = 3.
$M_1 = M^{d_1}$ mod p = 175^5 mod 17 = 14.
$M_2 = M^{d_2}$ mod q = 175^{19} mod 23 = 10.
S = M_1 + p *((M_2 - M_1) * p^{-1} mod q) = 14 + 17*((10-14)*-4 mod 23) = 14 + 272 = **286**.

6.2 Binary Exponentiation.

Representing 85 in binary results in: 1 0 1 0 1 0 1
Following table shows computation of RSA decryption using binary exponentiation.

i	e_i	Step 2a	Step 2b
6	0	$((175)^2)$ mod 391 = 127	127
5	1	$((127)^2)$ mod 391 = 98	98*175 mod 391 = 337
4	0	$((337)^2)$ mod 391 = 179	179
3	1	$((179)^2)$ mod 391 = 370	370*175 mod 391 = 235
1	0	$((235)^2)$ mod 391 = 94	94
0	1	$((94)^2)$ mod 391 = 234	234*175 mod 391 = **286**