Assignment 8

Benjmain Boudra

March 7, 2016

Contents

1 Prompt

Write up a careful example of the entire RSA process, including d, encrypting a, and decrypting c, with $p = 137$, $q = 241$, $e = 53$, and $a = 12345$. You will be expected to do all of this (including efficient modular exponentiation and the extended Euclidean Algorithms) by hand during the test, so do the exercise that way, just using an ordinary calculator.

2 Solution

2.1 Step 1: Solve for n and ϕ

$$n = p * q = 137 * 241 = 33017, \qquad n = 33017$$

$$\phi(n) = (p - 1) * (q - 1) = 136 * 240 = 32640, \qquad \phi = 32640$$

2.2 Step 2: Solve for d

ϕ	e	q	r	s	d
32640	53	615	45	-20	12317
53	45	1	8	17	-20
45	8	5	5	-3	17
8	5	1	3	2	-3
5	3	1	2	-1	2
3	2	1	1	1	-1
2	1	2	0	0	1
1	0			1	0

Equation I used for calculating the d values on the right side of the table.

$$d = s - d * q$$

Verification:

$$1 = \phi * s + e * d \qquad 1 = 32640 * -20 + 53 * 12317 \qquad 1 = -652800 + 652801 \qquad 1 = 1$$

The equation is true, Thus the d value is accurate.
$d = 12317$

2.3 Step 3: Calculate c

$$c = a^e \tag{1}$$

Since we are calculating the value in the world Z_n

$$c = a^e \ mod \ n \tag{2}$$

Also recognize that:

$$c = a^{53}, \qquad c = a^{32} * a^{16} * a^4 * a^1 \tag{3}$$

Now to calculate those values, we will create a table of a^{2^m} for $a^{2^m} < a^{53}$

n	a^{2^n}
0	12345
1	25570
2	22266
3	24501
4	16924
5	32318

$$c = a^{53} = 32318 * 16924 * 22266 * 12345 \ mod \ 33017, \qquad c = 24983 \tag{4}$$

Thus, $c = 24983$

2.4 Step 4: Calculate c^d

$$a = c^d \qquad a = a^{e^d} \tag{5}$$

Since we are calculating the value in the world Z_n

$$a = c^d \ mod \ n \tag{6}$$

Also recognize that c^d is some subset of:

$$S = \{c^{2^m} \mid c^{2^m} < c^{12317}\}$$

we will use the method of dividing by 2 and using odd remainders to find the subset:

n	Current Value	$\frac{Currentvalue}{2}$	remainder
0	12317	6158	1
1	6158	3079	0
2	3079	1539	1
3	1539	769	1
4	769	384	1
5	384	192	0
6	192	96	0
7	96	48	0
8	48	24	0
9	24	12	0
10	12	6	0
11	6	3	0
12	3	1	1
13	1	0	1

Thus $c^{12317} = c^{2^{13}} * c^{2^{12}} * c^{2^4} * c^{2^3} * c^{2^2} * c^{2^0}$

Now to calculate those values, we will create a table of the values in set S.

m	c^m
0	24983
1	29938
2	4362
3	9252
4	19440
5	1018
6	12797
7	31906
8	12692
9	29938
10	4362
11	9252
12	19440
13	1018

$a = 1018 * 19940 * 19440 * 9252 * 4362 * 24983 \ mod \ n = 12345$

2.5 Result

12345 = 12345 Therefore, The RSA Process is complete and correct