Cryptography

Homework 3

1) $p = 43 \quad q = 37 \quad b = 23$

a) $N = p \cdot q = 43 \cdot 37 = 1591$

$\phi(N) = (p-1)(q-1) = (43-1)(37-1) = 1512$

$k_{priv} = a = b^{-1} \bmod \phi(N)$

$= 23^{-1} \bmod 1512$

gcd(23, 1512)

$1512 = 23 \cdot 65 + 17 \quad 17 = 1512 - 23 \cdot 65$

$23 = 17 \cdot 1 + 6 \quad 6 = 23 - 17 \cdot 1$

$17 = 6 \cdot 2 + 5 \quad 5 = 17 - 6 \cdot 2$

$6 = 5 \cdot 1 + 1 \rightarrow 1 = 6 - 5 \cdot 1$

$5 = 1 \cdot 5 + 0$

gcd(23, 1512) = 1

Substitution

$1 = 6 - (17 - 6 \cdot 2) \cdot 1$

$1 = -17 \cdot 1 + 6 \cdot 3$

$1 = -17 \cdot 1 + (23 - 17 \cdot 1) \cdot 3$

$1 = 23 \cdot 3 - 17 \cdot 4$

$1 = 23 \cdot 3 - (1512 - 23 \cdot 65) \cdot 4$

$1 = 23 \cdot 263 - 1512 \cdot 4$

$263 = a$

b) $y = x^b \bmod N \Rightarrow y = 91^{23} \bmod 1591$

$23 = (10111) = b_4 b_3 b_2 b_1 b_0$

$2^4 \; 2^3 2^2 1 2^0$

$1 \; 0 \; 1 \; 1 \; 1$

2 | 23	1
2 | 11	1
2 | 5	1
2 | 2	0
2 | 1	1
0	

$l = 5$ so $i = 4$

$z = x = 91$

for $i = 4$ to 1

do $z^2 \bmod n$

if $b_{i-1} = 1$ then $z = z \cdot x \bmod n$

$z^2 \bmod n$
$z \cdot x \bmod n$

$i = 4$ $z^2 = 8281 \bmod 1591 = 326 \bmod 1591$
$b_3 = 0$ $z = 326$

$i = 3$ $z^2 = 326^2 \bmod 1591 = 1270 \bmod 1591$
$b_2 = 1$ $z = 1270 \cdot 91 \bmod 1591$
$= 1018 \bmod 1591$

$i = 2$ $z^2 = 1018^2 \bmod 1591 = 583 \bmod 1591$
$b_1 = 1$ $z = 583 \cdot 91 \bmod 1591$
$= 550 \bmod 1591$

$i = 1$ $z^2 = 550^2 \bmod 1591 = 210 \bmod 1591$
$b_0 = 1$ $z = 210 \cdot 91 \bmod 1591$
$= 18 \bmod 1591$

1c) $X = y^a \bmod n$
$X = 18^{263} \bmod 1591$
$x = 91$
x is supposed to be 91
So this is correct ✓
$91 = 91$

2a) $X = y^a \bmod n$
The variables that Eve doesn't know are "a" and of course X. Since the numbers are small in this example (not a very large n), Eve will be able to find X. She just needs to compute a in the equation above. Since she knows the public key with parameters N and b, she can find "a" through this equation: $a = b^{-1} \bmod \phi(N)$
The next question discusses how to find $\phi(N)$.

2b) Eve can recover $\phi(N)$ because there is a small N which is possible to compute. Since she knows N from the public key, she can factor it into p and q and then easily find $\phi(N)$ by computing $(p-1)\cdot(q-1)$.

2c) Eve knows Y, N, and b

$N = 1591$ Factors of 1591: 1, 37, 43, 1591

So, p and q must be 43 and 37.

$\phi(N) = (43-1)(37-1) = 1512$

$a = b^{-1} \bmod \phi(N)$ $\quad a = 23^{-1} \bmod 1512$

$1 = \gcd(23, 1512) \rightarrow$ use extendend euclidean alg.

$1512 = 23 \cdot 65 + 17 \quad 17 = 1512 - 23 \cdot 65$

$23 = 17 \cdot 1 + 6 \quad 6 = 23 - 17 \cdot 1$

$17 = 6 \cdot 2 + 5 \quad 5 = 17 - 6 \cdot 2$

$6 = 5 \cdot 1 + 1 \rightarrow 1 = 6 - 5 \cdot 1$

$5 = 1 \cdot 5 + 0$

Substitution

$1 = 6 - (17 - 6 \cdot 2) \cdot 1$

$1 = -17 \cdot 1 + 6 \cdot 3$

$1 = -17 \cdot 1 + 23 - (7 \cdot 1) \cdot 3$

$1 = 23 \cdot 3 - 17 \cdot 4$

$1 = 23 \cdot 3 - (1512 - 23 \cdot 65) \cdot 4$

$1 = 23 \cdot 263 - 1512 \cdot 4$

$263 = a$

Now that we know a, we can find X using $X = y^a \bmod n$

$X = 18^{263} \bmod 1591$

$X = 91$

2d) No, because it would take too much time which makes it impossible to do a message recovery attack for a large N value.

2e) For a large N such as in part d, then it would be impossible to find a. However for this small example, you can find a such as in part c.

3a) $17^{-1} \bmod 37$ $\quad \gcd(17, 37) = 1$

$37 = 17 \cdot 2 + 3$ $\quad 3 = 37 - 17 \cdot 2$

$17 = 3 \cdot 5 + 2$ $\quad 2 = 17 - 3 \cdot 5$

$3 = 2 \cdot 1 + 1 \rightarrow 1 = 3 - 2 \cdot 1$

$2 = 1 \cdot 2 + 0$

Substitution

$1 = 3 - (17 - 3 \cdot 5) \cdot 1$

$= 3 \cdot 6 - 17 \cdot 1$

$= (37 - 17 \cdot 2) \cdot 6 - 17 \cdot 1$

$= 37 \cdot 6 - 13 \cdot 17$

$17^{-1} = 24 \bmod 37$

3b) $13^{-1} \bmod 91$ $\quad \gcd(13, 91) = 13$

$91 = 13 \cdot 7 + 0$

No multiplicative inverse since gcd(13, 91) is not equal to 1.

3c) $13^{-1} \bmod 448$ $\quad \gcd(13, 448) = 1$

$448 = 13 \cdot 34 + 6$ $\quad 6 = 448 - 13 \cdot 34$

$13 = 6 \cdot 2 + 1 \rightarrow 1 = 13 - 6 \cdot 2$

$6 = 1 \cdot 6 + 0$

Substitution

$1 = 13 - (448 - 13 \cdot 34) \cdot 2$

$= 13 \cdot 69 - 2 \cdot 448$

$13^{-1} = 69 \bmod 448$

3d) $16^{-1} \bmod 4725$ $\quad \gcd(16, 4725) = 1$

$4725 = 16 \cdot 295 + 5 \quad 5 = 4725 - 16 \cdot 295$

$16 = 5 \cdot 3 + 1 \rightarrow 1 = 16 - 5 \cdot 3$

$5 = 1 \cdot 5 + 0$

Substitution

$1 = 16 - (4725 - 16 \cdot 295) \cdot 3$

$= 16 \cdot 886 - 4725 \cdot 3$

$16^{-1} = 886 \bmod 4725$