10

Cryptography I
Homework sheet 12

Erwin van Duijnhoven
0719562

Rick Staals
0716184

December 18, 2013

Question 1

Compute $\varphi(37800)$.

Solution:

$$\begin{aligned} 37800 &= 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^1 \\ \Rightarrow \varphi(37800) &= (2^3 - 2^2)(3^3 - 3^2)(5^2 - 5^1)(7^1 - 7^0) \\ &= 4 \cdot 18 \cdot 20 \cdot 6 \\ &= 8640 \end{aligned}$$

Question 2

Compute $\varphi(193920134995885916749824 0)$.

Solution:

$$\begin{aligned} 1939201349958859167498240 &= 2^{17} \cdot 3^{12} \cdot 5^1 \cdot 7^5 \cdot 11^7 \cdot 17^1 \\ \Rightarrow \varphi(1939201349958859167498240) &= (2^{17} - 2^{16})(3^{12} - 3^{11})(5^1 - 5^0)(7^5 - 7^4)(11^7 - 11^6)(17^1 - 17^0) \\ &= 65536 \cdot 354294 \cdot 4 \cdot 14406 \cdot 17715610 \cdot 16 \\ &= 379247933987370471260160 \end{aligned}$$

Question 3

Execute the RSA key generation where $p = 239$, $q = 433$ and $e = 23441$.

Solution:

The public key we send is (e, n) and the private key is d. Below are the calculations.

$$n = pq = 239 \cdot 433 = 103487$$
$$\varphi(n) = 238 \cdot 432 = 102816$$

Because we chose $e = 23441$, we now need to check if $\gcd(102816, 23441) = 1$, and $d \equiv e^{-1} \mod \varphi(n)$. We do this by using the extended Euclidean algorithm.

Step	a	b
1	$(102816, 1, 0)$	$(23441, 0, 1)$
2	$(23441, 0, 1)$	$(9052, 1, -4)$
3	$(9052, 1, -4)$	$(5337, -2, 9)$
4	$(5337, -2, 9)$	$(3715, 3, -13)$
5	$(3715, 3, -13)$	$(1622, -5, 22)$
6	$(1622, -5, 22)$	$(471, 13, -57)$
7	$(471, 13, -57)$	$(209, -44, 193)$
8	$(209, -44, 193)$	$(53, 101, -443)$
9	$(53, 101, -443)$	$(50, -347, 1522)$
10	$(50, -347, 1522)$	$(3, 448, -1965)$
11	$(3, 448, -1965)$	$(2, -7515, 32962)$
12	$(2, -7515, 32962)$	$(1, 7963, -34927)$
13	$(1, 7963, -34927)$	$(0, -23441, 102816)$

So it follows that $\gcd(102816, 23441) = 1$, and $d \equiv -34927 \equiv 67889 \mod 102816$. This means that the public key is $(23441, 103487)$ and the private key is 67889.

Question 4

RSA-encrypt the message 23 to a user with public key $(e, n) = (17, 11584115749)$. Document how you compute the exponentiation if you only have a pocket calculator.

Solution:

We calculate $C \equiv M^e \mod n \equiv 23^{17} \mod 11584115749$. We do this with the following steps:

$$\begin{aligned} C &\equiv (((23^2)^2)^2)^2 \cdot 23 \\ &\equiv ((529^2)^2)^2 \cdot 23 \\ &\equiv (279841^2)^2 \cdot 23 \\ &\equiv 8806290787^2 \cdot 23 \\ &\equiv 6518322 5840 \cdot 23 \\ &\equiv 10912105332 \mod 11584115749 \end{aligned}$$

Question 5

Find the smallest positive integer x satisfying the following system of congruences, should such a solution exist.

$$x \equiv a_3 \equiv 0 \mod 3$$
$$x \equiv a_5 \equiv 1 \mod 5$$
$$x \equiv a_8 \equiv 2 \mod 8$$

Solution:

Since 3, 5 and $8 = 2^3$ are coprime, this solution exists.
Now we calculate x the following way

$$x = a_3c_3y_3 + a_5c_5y_5 + a_8c_8y_8 \mod 120$$

with $c_i = \prod_{j \neq i} j$ and $y_i \equiv c_i^{-1} \mod i$. We calculate the c_i by using the extende Euclidean algorithm (which we won't include).

$$a_3 = 0$$
$$a_5 = 1$$
$$a_8 = 2$$
$$c_3 = 40$$
$$c_5 = 24$$
$$c_8 = 15$$
$$y_3 = 1$$
$$y_5 = 4$$
$$y_8 = 7$$
$$\Rightarrow x \equiv 0 \cdot 40 \cdot 1 + 1 \cdot 24 \cdot 4 + 2 \cdot 15 \cdot 7 \equiv 306 \equiv 66 \mod 120$$

So $x = 66$ is the smallest positive integer satisfying the system of congruences.

Question 6

Show how to retrieve the message m in RSA-OAEP from $m' \| r'$.

Solution:

First we retrieve r by calculating $r = r' \bigoplus H(m')$. After that, we retrieve $m \| 00 \ldots 0$ by calculating $m \| 00 \ldots 0 = m' \bigoplus G(r)$. Our last step is to retrieve m, this is simply done by removing the last k_1 bits, which should all be zeroes.