Homework 9 in Cryptography I
- Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
30.06.2011

Solution to Exercise 27.

Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

(a) Let $n = p$ be prime. It follows
$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\} = \{1, 2, \dots, p - 1\} \Rightarrow \varphi(p) = p - 1$.

(b) Let $n = p^k$ for a prime p and $k \in \mathbb{N}$. For $1 \le a \le p^k$ it holds

1) $p \nmid a \Rightarrow \gcd\left(a, p^k\right) = 1$, and
2) $p \mid a \Rightarrow \gcd\left(a, p^k\right) \ge p$.

It follows $\mathbb{Z}_{p^k}^* = \underbrace{\{1 \le a \le p^k\}}_{p^k \text{ elements}} \setminus \underbrace{\{1 \le a \le p^k \mid p \mid a\}}_{p^{k-1} \text{ elements}}$. Consequently, it holds
$\varphi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

(c) Let $n = p\,q$ for two primes $p \ne q$. It holds

1) $p \mid a \vee q \mid a \Rightarrow \gcd\left(a, p\,q\right) > 1$, and
2) $p \nmid a \wedge q \nmid a \Rightarrow \gcd\left(a, p\,q\right) = 1$.

It follows

$$\mathbb{Z}_{p\,q}^* = \underbrace{\{1 \le a \le p\,q - 1\}}_{p\,q-1 \text{ elements}} \setminus \left[\underbrace{\{1 \le a \le p\,q - 1 \mid p \mid a\}}_{q-1 \text{ elements}} \,\dot\cup\, \underbrace{\{1 \le a \le p\,q - 1 \mid q \mid a\}}_{p-1 \text{ elements}}\right].$$

Consequently,
$\varphi\left(p\,q\right) = p\,q - 1 - (q - 1 - p - 1) = p\,q - p - q + 1 = (p - 1)(q - 1) = \varphi(p)\,\varphi(q)$.

(d) $\varphi(4913) = \varphi\left(17^3\right) \overset{(b)}{=} 17^2(17 - 1) = 4624$ and
$\varphi(899) = \varphi\left(30^2 - 1^2\right) = \varphi((30 - 1)(30 + 1)) = \varphi(29 \cdot 31) \overset{(c)}{=} 28 \cdot 30 = 840$.

Solution to Exercise 28.

(a) By the Miller-Rabin Primality Test it will be proven that 341 is composite.
Write $n = 341 = 1 + 85 \cdot 2^2 = 1 + q \cdot 2^k$.

Algorithm 1 Miller-Rabin Primality Test (MRPT)

```
Write n = 1 + q2^k, q odd
Choose a ∈ {2, ..., n − 1} uniformly distributed at random
y ← a^q mod n
if (y = 1) OR (y = n − 1) then
    return „n prime“
end if
for (i ← 1; i < k; i++) do
    y ← y^2 mod n
    if (y = n − 1) then
        return „n prime“
    end if
end for
return „n composite“
```

Choose $a = 2$.
Calculate $a^q \mod n$, i.e., $2^{85} \mod 341$.
Note that $2^{10} = 1024 = 3 \cdot 341 + 1 \equiv 1 \mod 341$.
It follows $2^{85} = (\underbrace{2^{10}}_{\equiv 1})^8 \cdot \underbrace{2^5}_{=32} \equiv 32 \mod 341$.
Alternatively, $2^{85} \mod 341$ is calculated by Square and Multiply, see below. As $y = 32 \notin \{1, n-1\}$ the for-loop starts with $i = 1$.
$y^2 = 32^2 = (2^5)^2 = 2^{10} \equiv 1 \mod 341$, see above.
Furthermore, $y = 1 \neq 340 \mod 341$.
As $i = 2 = k = 2$ the for-loop terminates and n is stated as composite, which is a reliable result.

(b) A number n is decomposed according to MRPT as $n = 1 + q\,2^k$. It follows that MRPT has at most k squarings. The worst case occurs, if $q = 1$, then $n = 1 + 2^k \Leftrightarrow k = \log_2(n-1)$. With n having 300 digits it follows:
$n < 10^{301} = (\underbrace{10^3}_{<2^{10}})^{100} \cdot \underbrace{10}_{<2^4} < 2^{1004} \Rightarrow k \leq 1004$.
Consequently, less than 1004 squarings are needed. ($k \approx 999.9$)

Note, evaluating $a^q \mod n$ with Square and Multiply takes t squarings. But as $2^t \leq q$ holds, the worst case is reached, for equality which means $t = 0$, i.e., $q = 1$, as otherwise q would be not odd.

Determining $2^{85} \mod 341$ by Square and Multiply.
It holds $a = 2$, $x = 85 = (1010101)_2$, i.e., $t = 6$.

Algorithm 2 Square and multiply

Require: $x = (x_t, \dots, x_0) \in \mathbb{N}, a \in \mathbb{N}$
Ensure: $a^x \mod n$

$y \leftarrow a$
for $(i = t - 1, i \geq 0, i\text{--})$ **do**
  $y \leftarrow y^2 \mod n$
  if $(x_i = 1)$ **then**
    $y \leftarrow y \cdot a \mod n$
  end if
end for
return y

The following tabular denotes the evaluation of the Square and Multiply algorithm. The table is initialized in the first line with $i = t = 6$ and $y = 1$. There are $t + 1$ lines numbered from t down to 0. The binary representation of $x = (x_t. \dots .x_0)$ is given in column two. Using those values the columns four and five are evaluated row by row. For each row the y value is taken from the last column of the row above. The final value in the fifth column is the result of $a^x \mod n$.

i	x_i	y	$y^2 \mod n$	$y^2(1 + x_i \cdot (a - 1)) \mod n$
6	1	1	1	2
5	0	2	4	4
4	1	4	16	32
3	0	32	$1024 \equiv 1 \mod 341$	1
2	1	1	1	2
1	0	2	4	4
0	1	4	16	32

The solution is $2^{85} \equiv 32 \mod 341$.