Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 11
- Proposed Solution -

Friday, July 8, 2016

Solution of Problem 1

Let a be a primitive element modulo n, i.e., $\mathbb{Z}_n^* = \{a^1, a^2, \ldots, a^{\varphi(n)} \equiv 1 \equiv a^0\}$.

Let $j \in \{1, \ldots, \varphi(n) - 1\}$ and $b = a^j \pmod n$. Then,

$$
\begin{aligned}
& b \text{ is a primitive element modulo } n \\
\Leftrightarrow\ & b^k \not\equiv 1 \,(\operatorname{mod} n),\ \forall k = 1, \ldots, \varphi(n) - 1 \ \wedge\ b^{\varphi(n)} \equiv 1 \,(\operatorname{mod} n) \\
\Leftrightarrow\ & a^{jk} \not\equiv 1 \,(\operatorname{mod} n),\ \forall k = 1, \ldots, \varphi(n) - 1 \ \wedge\ a^{j\varphi(n)} \equiv 1 \,(\operatorname{mod} n) \\
\Rightarrow\ & a^{jk} \not\equiv a^0 \,(\operatorname{mod} n) \\
\Leftrightarrow\ & jk \not\equiv 0 \,(\operatorname{mod} \varphi(n)) \qquad (1) \\
\Leftrightarrow\ & \gcd(j, \varphi(n)) = 1. \qquad (2)
\end{aligned}
$$

Proof of (2):

"$\Rightarrow$" Assume $\gcd(j, \varphi(n)) = c > 1$:

$$\underbrace{\left(\frac{\varphi(n)}{c}\right)}_{\in \{1, \ldots, \varphi(n)-1\}} \cdot j \equiv \varphi(n) \cdot \frac{j}{c} \equiv 0 \,(\operatorname{mod} \varphi(n)),$$

but $jk \not\equiv 0 \,(\operatorname{mod} \varphi(n))$, $\forall k \in \{1, \ldots, \varphi(n) - 1\}$ is a contradiction. $\lightning$

"$\Leftarrow$" Assume $\gcd(j, \varphi(n)) = 1$:

$$
\begin{aligned}
&\Rightarrow j \text{ is invertible modulo } \varphi(n) \\
&\Rightarrow \exists l \in \mathbb{Z} : jl \equiv 1 \,(\operatorname{mod} \varphi(n)).
\end{aligned}
$$

Assume: $jk \equiv 0 \,(\operatorname{mod} \varphi(n))$ for some $k \in \{1, \ldots, \varphi(n) - 1\}$:

$$
\begin{aligned}
&\Rightarrow l \cdot 0 \equiv \underbrace{l \cdot j}_{\equiv 1} \cdot k \,(\operatorname{mod} \varphi(n)) \\
&\Rightarrow 0 \ \equiv k \,(\operatorname{mod} \varphi(n)),
\end{aligned}
$$

But $0 \notin \{1, \ldots, \varphi(n - 1)\}$ is a contradiction. $\lightning$

Thus, $jk \not\equiv 0 \,(\operatorname{mod} \varphi(n))$ is necessary.

- Altogether, a^j is a primitive element modulo $n \Leftrightarrow \gcd(j, \varphi(n)) = 1$.
- The number of primitive elements modulo n is equal to:

$$|\{j \in \{1, \ldots, \varphi(n) - 1\} \mid \gcd(j, \varphi(n)) = 1\}| = \varphi(\varphi(n)). \ \square$$

Solution of Problem 2

Shamir's no-key protocol with the parameters: $p = 31337, a = 9999, b = 1011, m = 3567$.

a)

$$\begin{aligned} c_1 &= m^a \mod p = 3567^{9999} \mod 31337 \equiv 6399 && (3)\\ c_2 &= c_1^b \mod p = 6399^{1011} \mod 31337 \equiv 29872 \text{ (given by hint)} && (4)\\ c_3 &= c_2^{a^{-1}} \mod p = 29872^{14767} \mod 31337 \equiv 24982 && (5) \end{aligned}$$

To compute c_1 we use the square-and-multiply algorithm (SAM) (in chart):

The binary representation of $a = 9999$ is 10011100001111_2.

Hint: If your calculator can not convert a large number $\Rightarrow$ convert it by hand.

For illustration, we can represent the exponentiation in terms of squareings by:

$$m^a \equiv (\dots(m^1)^2m^0)^2m^0)^2m^1)^2m^1)^2m^1)^2m^0)^2m^0)^2m^0)^2m^0)^2m^1)^2m^1)^2m^1)^2m^1 \mod p$$

op	exp	modulo
1	1	3567
S	0	667
S	0	6171
SM	1	13498
SM	1	23177
SM	1	3298
S	0	2865
S	0	29268
S	0	18929
S	0	31120
SM	1	143
SM	1	20384
SM	1	30182
SM	1	6399

Hint: Feel free to implement the SAM in order to check your results.

To compute a^{-1} modulo $p - 1$, we use the EEA:

$$\begin{aligned} 31336 &= 3 \cdot 9999 + 1339\\ 9999 &= 7 \cdot 1339 + 626\\ 1339 &= 2 \cdot 626 + 87\\ 626 &= 7 \cdot 87 + 17\\ 87 &= 5 \cdot 17 + 2\\ 17 &= 8 \cdot 2 + 1 \Rightarrow \gcd(31336, 9999) = 1 \end{aligned}$$

To compute the inverse of a, we reorganize the last equation w.r.t. the remainder one and substitute the factors backwards:

$$\begin{aligned}
1 &= 17 - 8 \cdot 2 \\
&= 17 - 8 \cdot (87 - 5 \cdot 17) = 41 \cdot 17 - 8 \cdot 87 \\
&= 41 \cdot 626 - 295 \cdot 87 \\
&= 631 \cdot 626 - 295 \cdot 1339 \\
&= 631 \cdot 9999 - 4712 \cdot 1339 \\
&= \underbrace{14767}_{a^{-1}} \cdot \underbrace{9999}_{a} - 4712 \cdot 31336
\end{aligned}$$

Hint: Check if result is equal to one in each step!

The computation of $c_2^{a^{-1}} \mod p = 29872^{14767} \mod 31337$ with SAM provides:

op	exp	modulo
1	1	29872
SM	1	9607
SM	1	15639
S	0	24373
S	0	18957
SM	1	16656
SM	1	26421
S	0	6229
SM	1	8290
S	0	2059
SM	1	28387
SM	1	13917
SM	1	9317
SM	1	24982

Solution of Problem 3

a) The public parameters and the received ciphertext are:

- $e = d^{-1} \mod \varphi(n)$,
- $n = p\,q$,
- $c = m^e \mod n$.

The plaintext m is not relatively prime to n , i.e., $p \mid m$ or $q \mid m$ and $p \neq q$.

Hence, $\gcd(m,n) \in \{p,q\}$ holds. The $\gcd(m,n)$ can be easily computed such that both primes can be calculated by either $q = \frac{n}{p}$ or $p = \frac{n}{q}$.

The private key d can be computed since the factorization of $n = p\,q$ is known.

$$d = e^{-1} \mod \varphi(p\,q) = e^{-1} \mod (p-1)(q-1).$$

This inverse is computed using the extended Euclidean algorithm.

b) m, n have common divisors.

The number of relatively prime numbers to n are $\varphi(n) = (p-1)(q-1) = p\,q - (p+q) + 1$.

$$\mathrm{P}(\gcd(m,n) = 1) = \frac{\varphi(n)}{n-1}.$$

The complementary probability is computed by:

$$\begin{aligned} P = \mathrm{P}(\gcd(m,n) \neq 1) = 1 - \frac{\varphi(n)}{n-1} &= \frac{n-1-\varphi(n)}{n-1} \\ &= \frac{p\,q - p\,q + p + q - 2}{p\,q - 1} = \frac{p+q-2}{p\,q-1}. \end{aligned}$$

c) $n : 1024$ Bits $\Rightarrow p \approx \sqrt{n} = 2^{512}, q \approx \sqrt{n} = 2^{512}$. From (b) we compute:

$$P = \frac{2^{512} + 2^{512} - 2}{2^{1024} - 1} = \frac{2^{513} - 2}{2^{1024} - 1} \approx 2^{-511} = (2^{-10})^{51} 2^{-1} \approx (10^{-3})^{51} \frac{5}{10} = 5 \cdot 10^{-154}$$

In general: $n = 2^k$, $p, q \approx 2^{\frac{k}{2}}$ for k Bits.

$$P = \frac{2^{\frac{k}{2}} + 2^{\frac{k}{2}} - 2}{2^k - 1} = \frac{2^{\frac{k}{2}+1} - 2}{2^k - 1} \approx 2^{\frac{k}{2}+1} 2^{-k} = 2^{-\frac{k}{2}+1}.$$

Thus, the probability that m and n are coprime is marginal, if n has sufficiently many bits.

Solution of Problem 4

a) $\varphi(n) = (u-1)(v-1)$, since u and v are distinct and prime.

$$x^{\varphi(n)/2} \equiv x^{(u-1)(v-1)/2} \equiv (x^{u-1})^{(v-1)/2} \equiv 1^{(v-1)/2} \equiv 1 \pmod{u}$$

Since v is an odd prime, it holds $2|(v-1)$ so that $(v-1)/2$ is an integer.

(Remark: Note that $(x^{\frac{1}{2}})^{\varphi(n)} \pmod{n}$ is not defined!)

With analogous arguments, $x^{\varphi(n)/2} \equiv 1 \mod v$ is computed.

b) Since, u and v are coprime, we may apply the Chinese Remainder Theorem (solution is $r \equiv x^{\varphi(n)/2} \mod n$):

$$\begin{aligned}
x^{\varphi(n)/2} &\equiv 1 \pmod{u}, \\
x^{\varphi(n)/2} &\equiv 1 \pmod{v}, \\
M &= pq, \\
M_1 &= v, y_1 = v^{-1} \mod u, \\
M_2 &= u, y_1 = u^{-1} \mod v \\
r &= (1 \cdot v \cdot (v^{-1} \mod u) + 1 \cdot u \cdot (u^{-1} \mod v)) \pmod{u \cdot v} \\
&= (v(v^{-1} \pmod{u}) + u(u^{-1} \pmod{v})) \pmod{u \cdot v} \\
&= 1 \quad \text{, from definition of } \gcd(u,v) = 1
\end{aligned}$$

Note that since $\gcd(u,v) = 1$ holds, it follows from the Extended Euclidean Algorithm, that $ux + vy = \gcd(u,v) = 1$. The unique solutions for x and y are $x \equiv u^{-1} \mod v$ and $y \equiv v^{-1} \mod u$. (cf. lecture section 'The Extended Euclidean Algorithm')

c) If $ed \equiv 1 \pmod{\frac{1}{2}\varphi(n)}$ it follows that:

$$\begin{aligned}
ed &= 1 + \tfrac{1}{2}\varphi(n)k, \;\; k \in \mathbb{Z}, \\
\Leftrightarrow x^{ed} &\equiv x^{1+\frac{1}{2}\varphi(n)k} \\
&\equiv x(x^{\frac{1}{2}\varphi(n)})^k \\
&\equiv x \cdot 1^k \equiv x \pmod{n}
\end{aligned}$$