**Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He**

# Exercise 1
# - Proposed Solution -

Friday, October 27, 2017

## Solution of Problem 1

**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 2

**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:

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

## Solution of Problem 3

Decipher $m = \sqrt{c} \mod n$ with $c = 1935$.

- Check $p, q \equiv 3 \mod 4$ ✓
- Compute the square roots of $c$ modulo $p$ and $c$ modulo $q$.

$$\begin{aligned}
k_p &= \frac{p+1}{4} = 17, \quad k_q = \frac{q+1}{4} = 18,\\
x_{p,1} &= c^{k_p} \equiv 1935^{17} \equiv 59^{17} \equiv 40 \mod 67,\\
x_{p,2} &= -x_{p,1} \equiv 27 \mod 67,\\
x_{q,1} &= c^{k_q} \equiv 1935^{18} \equiv 18^{18} \equiv 36 \mod 71,\\
x_{q,2} &= -x_{q,1} \equiv 35 \mod 71.
\end{aligned}$$

- Compute the resulting square root modulo $n$. $m_{i,j} = ax_{p,i} + bx_{q,j}$ solves $m_{i,j}^2 \equiv c \mod n$ for $i, j \in \{1, 2\}$. We substitute $a = tq$ and $b = sp$. Then $tq + sp = 1$ yields $1 = 17 \cdot 71 + (-18) \cdot 67 = tq + sp$ from the Extended Euclidean Algorithm.

$$\Rightarrow a \equiv tq \equiv 17 \cdot 71 \equiv 1207 \mod n$$
$$\Rightarrow b \equiv -sp \equiv -18 \cdot 67 \equiv -1206 \mod n.$$

The four possible solutions for the square root of ciphertext $c$ modulo $n$ are:

$$\begin{aligned} m_{1,1} &\equiv ax_{p,1} + bx_{q,1} \equiv 107 \mod n \Rightarrow 00000011010\underline{11}, \\ m_{1,2} &\equiv ax_{p,1} + bx_{q,2} \equiv 1313 \mod n \Rightarrow 0010100100001, \\ m_{2,1} &\equiv ax_{p,2} + bx_{q,1} \equiv 3444 \mod n \Rightarrow 0110101110100, \\ m_{2,2} &\equiv ax_{p,2} + bx_{q,2} \equiv 4650 \mod n \Rightarrow 1001000101010. \end{aligned}$$

The correct solution is $m_1$, by the agreement given in the exercise.

## Solution of Problem 4

**a)** Given $x \equiv -x \mod p$, prove that $x \equiv 0 \mod p$.

*Proof.* The inverse of 2 modulo p exists. Then,

$$\begin{aligned} -x &\equiv x \mod p \\ \Leftrightarrow \quad 0 &\equiv 2x \mod p \\ \Leftrightarrow \quad 0 &\equiv x \mod p\,. \end{aligned}$$

□

**b)** Looking at the protocol, we can show that Bob always loses to Alice, if she chooses $p = q$.

**i)** Alice calculates $n = p^2$ and sends $n$ to Bob.

**ii)** Bob calculates $c \equiv x^2 \mod n$ and sends $c$ to Alice. With high probability $p \nmid x \Leftrightarrow x \not\equiv 0 \mod p$ (therefore, Bob *almost* always loses).

**iii)** The only two solutions $\pm x$ are calculated by Alice (see below) and sent to Bob. Bob cannot factor $n$, as

$$\gcd(x - (\pm x), n) = \begin{cases} \gcd(0, n) = n \\ \gcd(2x, n) = \gcd(2x, p^2) = 1 \end{cases}.$$

Alice always wins.

**c)** If Bob asks for the secret key as confirmation, the square is revealed and Alice will be accused of cheating. Bob can factor $n$ by calculating $p = \sqrt{n}$ as a real number and win the game.

*Note:* The two solutions $\pm x$ to $x^2 \equiv c \mod p^2$ can be calculated as follows.

Let $p$ be an odd prime and $x, y \not\equiv 0 \mod p$. If $x^2 \equiv y^2 \mod p^2$, then $x^2 \equiv y^2 \mod p$, so $x \equiv \pm y \mod p$.

Let $x \equiv y \mod p$. Then

$$x = y + \alpha p\,.$$

By squaring we get

$$\begin{aligned} x^2 &= y^2 + 2\alpha p y + (\alpha p)^2 \\ \Rightarrow x^2 &\equiv y^2 + 2\alpha p y \mod p^2\,. \end{aligned}$$

Since $x^2 \equiv y^2 \mod p^2$, we obtain

$$0 = 2\alpha p y \mod p^2\,.$$

Divide by $p$ to get

$$0 = 2\alpha y \mod p\,.$$

Since $p$ is odd and $p \nmid y$, we must have $p \mid \alpha$. Therefore, $x = y + \alpha p \equiv y \mod p^2$. The case $x \equiv -y \mod p$ is similar.

In other words, if $x^2 \equiv y^2 \mod p^2$, not only $x \equiv \pm y \mod p$, but also $x \equiv \pm y \mod p^2$. At this point, we have shown that only two solutions exist.

Now, we show how to find $\pm x$, where $x^2 \equiv c \mod p^2$. As we can find square roots modulo a prime $p$, we have $x = b$ solves $x^2 \equiv c \mod p$. We want $x^2 \equiv c \mod p^2$. Square $x = b + ap$ to get

$$\begin{aligned} b^2 + 2bap + (ap)^2 \equiv b^2 + 2bap &\equiv c \mod p \\ \Rightarrow b^2 &\equiv c \mod p\,. \end{aligned}$$

Since $b^2 \equiv c \mod p$ the number $c - b^2$ is a multiple of $p$, so we can divide by $p$ and get

$$2ab \equiv \frac{c - b^2}{p} \mod p\,.$$

Multiplying by the multiplicative inverse modulo $p$ of 2 and $b$, we obtain:

$$a \equiv \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} \mod p\,.$$

Therefore, we have $x = b + ap$.

This procedure can be continued to get solutions modulo higher powers of $p$. It is the numberic-theoretic version of Newton's method for numerically solving equations, and is usually referred to as Hensel's Lemma.

*Example:* $p = 7$, $p^2 = 49$, $c = 37$. Then

$$\begin{aligned} b = c^{\frac{p+1}{4}} = 37^{\frac{7+1}{4}} = 37^2 &\equiv 4 \mod p\,, \\ b^{-1} \equiv 2 \mod p\,,\ 2^{-1} &\equiv 4 \mod p\,, \\ a = \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} = \frac{37 - 4^2}{7} \cdot 4 \cdot 2 &\equiv 3 \mod p \\ x = b + ap = 4 + 3 \cdot 7 &= 25 \end{aligned}$$

Check: $x^2 = 25^2 \equiv 37 = c \mod p^2$.