Exercise 1 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-04-16

Solution of Problem 1

a) Division with remainder is computed as follows:

Algorithm 1 Division with remainder

input: Two integers, the dividend a and the divisor d with $a \geq d$

output: Integer division: a div d, and remainder: a mod d)

```
procedure DIVMOD(a, b)
    Find the unique q ∈ ℕ such that a = q · d + r holds with 0 ≤ r < d
    return (q, r)
end procedure
```

Ordinary long division yields $1234 : 357 = 3 + \frac{163}{357} \approx 3.456$
We obtain $q = 1234 \text{ div } 357 = 3$, and $r = 1234 \mod 357 \equiv 163$

b) The greatest common divisor (gcd) is computed as follows:

Algorithm 2 Euclid's algorithm to compute the greatest common divisor

input: Two integers a and b with $a \geq b$

output: The greatest common divisor $\gcd(a, b)$

```
procedure GCD(a, b)
    while b ≠ 0 do
        r ← a mod b
        a ← b
        b ← r
    end while
    return a
end procedure
```

To compute gcd(357, 1234), we can compactly write:

$$\begin{aligned}
1234 &= 357 \cdot 3 + 163 \\
357 &= 163 \cdot 2 + 31 \\
163 &= 31 \cdot 5 + 8 \\
31 &= 8 \cdot 3 + 7 \\
8 &= 7 \cdot 1 + 1 \\
(7 &= 1 \cdot 7 + 0) \quad //\text{but, } r = 0 ↯
\end{aligned}$$

Hence, we obtain $\gcd(357, 1234) = 1$.

c) The extended Euclidean algorithm (EEA) is used to compute multiplicative inverses:

Algorithm 3 Extended Euclid's algorithm

input: Two integers a and b with $a \geq b$

output: An integer tuple (u, d, v) satifying $a \cdot u + b \cdot v = d = \gcd(a, b)$

```
procedure EXTGCD(a, b)
    u ← 1
    v ← 0
    d ← a
    v1 ← 0
    v3 ← b
    while v3 ≠ 0 do
        q ← ⌊d / v3⌋
        t3 ← d mod v3
        t1 ← u − q · v1
        u ← v1
        d ← v3
        v1 ← t1
        v3 ← t3
        return a
    end while
    v ← (d − a·u) / b
    return (u, d, v)
end procedure
```

A compact computation of the inverse using this algorithm is, e.g.:

$$\begin{aligned}
1 &= 8 - 7 \cdot 1 \checkmark \\
&= 8 - (31 - 8 \cdot 3) \cdot 1 \\
&= 8 \cdot 4 - 31 \cdot 1 \checkmark \\
&= (163 - 31 \cdot 5) \cdot 4 - 31 \cdot 1 \\
&= 163 \cdot 4 - 31 \cdot 21 \checkmark \\
&= 163 \cdot 4 - (357 - 163 \cdot 2) \cdot 21 \\
&= 163 \cdot 46 - 357 \cdot 21 \checkmark \\
&= (1234 - 357 \cdot 3) \cdot 46 - 357 \cdot 21 \\
&= 1234 \cdot 46 - 357 \cdot 159 \checkmark
\end{aligned}$$

Thus, the multiplicative inverse to 357 is -159 modulo 1234.

d) We consider the two polynomials $b(x) = x^3 + x + 1$ and $m(x) = x^5 + x^3 + 1$.
Since the coefficients are in $\{0, 1\}$ addition and substraction is equivalent here.
We compute $\gcd(b(x), m(x))$ using polynomial division:

$$\begin{array}{l} (x^5 + x^3 + 1) : (x^3 + x + 1) = x^2 + \frac{x^2+1}{x^3+x+1} \\ -(x^5 + x^3 + x^2) \\ \hline 0 + 0 + x^2 + 1 \end{array}$$

This yields the first step of the Euclidean algorithm:
$x^5 + x^3 + 1 = (x^3 + x + 1) \cdot x^2 + (x^2 + 1)$
In the second step of the Euclidean Algorithm, we again use polynomial division:

$$\begin{array}{l} (x^3 + x + 1) : (x^2 + 1) = x + \frac{1}{x^2+1} \\ -(x^3 + x) \\ \hline 0 + 1 \end{array}$$

This yields $x^3 + x + 1 = (x^2 + 1) \cdot x + 1$, so that $\gcd(x^5 + x^3 + 1, x^3 + x + 1) = 1$
Applying the extended Euclidean algorithm to these polynomials yields:

$$\begin{aligned} 1 &= (x^3 + x + 1) + x(x^2 + 1) \\ &= (x^3 + x + 1) + x[(x^5 + x^3 + 1) + x^2(x^3 + x + 1)] \\ &= (x^3 + x + 1)(1 + x^3) + x(x^5 + x^3 + 1) \end{aligned}$$

Thus, the multiplicative inverse to $b(x) = x^3 + x + 1$ is $a(x) = b^{-1}(x) = x^3 + 1$

Solution of Problem 2

a) Show that from $a \,|\, b$ and $b \,|\, c$ it follows that $a \,|\, c$.
$a|b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$
$b|c \Rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 \cdot b$
$\Rightarrow c = k_1 \cdot k_2 \cdot a$
$\Rightarrow k = k_1 \cdot k_2$
$\Rightarrow \exists k \in \mathbb{Z} : c = k \cdot a$
$\Rightarrow a|c$

b) Show that from $a \,|\, b$ and $c \,|\, d$ it follows that $(ac) \,|\, (bd)$.
$a|b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$
$c|d \Rightarrow \exists k_2 \in \mathbb{Z} : d = k_2 \cdot c$
$\Rightarrow b \cdot d = k_1 \cdot a \cdot k_2 \cdot c$
$\Rightarrow k = k_1 \cdot k_2$
$\Rightarrow \exists k \in \mathbb{Z} : b \cdot d = k \cdot a \cdot c$
$\Rightarrow (a \cdot c)|(b \cdot d)$

c) Show that from $a \,|\, b$ and $a \,|\, c$ it follows that $a \,|\, (xb + yc) \quad \forall\, x, y \in \mathbb{Z}$.
$a|b \Rightarrow \exists k_1 \in \mathbb{Z} : b = k_1 \cdot a$
$\Rightarrow x \in \mathbb{Z}, x \cdot b = xk_1 \cdot a$
$a|c \Rightarrow \exists k_2 \in \mathbb{Z} : c = k_2 \cdot a$
$\Rightarrow y \in \mathbb{Z}, y \cdot c = yk_2 \cdot a$
$xb + yc = xk_1 \cdot a + yk_2 \cdot a = (xk_1 + yk_2)a$
$\Rightarrow k = xk_1 + yk_2$
$\Rightarrow \exists k \in \mathbb{Z} : (xb + yc) = k \cdot a$
$\Rightarrow a|(xb + yc)$

Solution of Problem 3

It is helpful to organize the plaintext $\boldsymbol{m} = (m_1, m_2, m_3, ..., m_{kl})$ in a matrix with l rows and k columns as shown on the left hand side. The second matrix on the right hand side describes the mapping of the positions to the ciphertext.

$$\begin{array}{cccc|cccc} m_1 & m_{l+1} & \cdots & m_{(k-1)l+1} & 1 & 2 & \cdots & k \\ m_2 & \cdots & \cdots & \vdots & k+1 & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & \vdots & \vdots & \cdots & \cdots & \vdots \\ \vdots & \cdots & \cdots & m_{kl-1} & \vdots & \cdots & \cdots & (l-1)k \\ m_l & \cdots & \cdots & m_{kl} & (l-1)k+1 & \cdots & \cdots & kl \end{array}$$

From this the encryption of the Skytale is described by a permutation $\boldsymbol{\pi}$ with:

$$\boldsymbol{\pi} = \begin{pmatrix} 1 & 2 & \dots & l & l+1 & \dots & (k-1)l+1 & \dots & kl-1 & kl \\ 1 & k+1 & \dots & (l-1)k+1 & 2 & \dots & k & \dots & (l-1)k & kl \end{pmatrix}$$