Cryptographic Applications
Lab 1 Euclidean Algorithms *

Caroline Sheedy
School of Informatics and Creative Media
DKIT

Semester 1

Algorithm 1.1 Euclidean algorithm for computing the greatest common divisor of two integers

INPUT: two non-negative integers a and b with $a \geq b$
OUTPUT: the greatest common divisor of a and b

1. while $b \neq 0$ do the following:
   Set $r \leftarrow a \bmod b, a \leftarrow b, b \leftarrow r$.
2. return (a)

Recall, the Euclidean algorithm is based on the fact that if a and b are positive integers with $a > b$, then $gdc(a, b) = gcd(b, a \bmod b)$.

Example (Euclidean algorithm)

The following are the division steps of Algorithm 1.1 for computing $gcd(4864, 3458)$

$$4864 = 1 \cdot 3458 + 1406$$
$$3458 = 2 \cdot 1406 + 646$$
$$646 = 5 \cdot 114 + 76$$
$$114 = 1 \cdot 76 + 38$$
$$76 = 2 \cdot 38 + 0$$

*ref Handbook of Applied Cryptography, chapter 2

Thus $gcd(4864, 3458) = 38$.
The Euclidean algorithm can be extended so that it yields both the greatest common divisor of two integers a and b, but also integers x and y satisfying $ax + by = d$.

Algorithm 1.2 Extended Euclidean algorithm

INPUT: two non-negative integers a and b with $a \geq b$
OUTPUT: $d = gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

1. if $b = 0$ then set $d \leftarrow a, x \leftarrow 1, y \leftarrow 0$, and return (d, x, y)
2. Set $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   - $q \leftarrow \lfloor a/b \rfloor, r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$
   - $a, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1$ and $y_1 \leftarrow y$.
4. Set $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$, and return (d, x, y).

For the worked example above, this would return $x = 32, y = -45$ and $d = 38$.

Excercise: Implementation in java

You are required to implement *EITHER* the Euclidean algorithm *OR* the extended Euclidean algorithm in java. You may use the values presented here to test your code. You are required to upload your code to moodle.