B-it **IPEC Winter 2009**

Lecturer: Laila El Aimani

Exercise scheet 3: Subliminal channels in digital signature schemes

I Reminders in number theory

I.1 The integers

The set of integers $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ is denoted by the symbol $\mathbb{Z}$.

Definition 1. *Let a and b be integers. Then a divides b (equivalentely: a is a divisor of b, or a is a factor of b) if there exists an integer c such that $b = ac$. If a divides b, then this is denoted by $a \mid b$.*

Example 1. $-3 \mid 18$, $173 \mid 0$,...

Fact 1.

1. $a \mid a$,
2. *if* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$,
3. *if* $a \mid b$ *and* $a \mid c$ *then* $a \mid bx + cy$ $\forall x, y \in \mathbb{Z}$,
4. *if* $a \mid b$ *and* $b \mid a$ *then* $a = \pm b$

Definition 2. *(Division algorithm for integers) If a and b are integers with $b \geq 1$, then ordinary long division of a and b yields two integers : q (the quotient) and r (the remainder) such that*

$$a = qb + r \text{ where } 0 \leq r < b$$

Moreover, q and r are unique. The remainder of the division is denoted $a \bmod b$ and the quotient is denoted $a \operatorname{div} b$.

Example 2. $a = 73, b = 17 \Rightarrow q = 4, r = 5$

Definition 3. *An integer c is a common divisor of a and b if $c \mid a$ and $c \mid b$.*

Definition 4. *A non-negative integer d is the greatest common divisor of integers a and b denoted $d = \gcd(a, b)$ if:*

1. *d is a common divisor of a and b and*

2. whenever $c \mid a$ and $c \mid b$, then $c \mid d$

Equivalently, $\gcd(a, b)$ *is the largest positive integer that divides both* a *and* b *with the exception that* $\gcd(0, 0) = 0$.

Example 3. *The common divisors of* 12 *and* 18 *are* $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ *and* $\gcd(18, 12) = 6$

Definition 5. *A non negative integer* m *is the least common multiple of integers* a *and* b *, denoted* $m = lcm(a, b)$ *if:*

1. $a \mid m$ *and* $b \mid m$ *and*

2. whenever $a \mid c$ *and* $b \mid c$*, then* $m \mid c$

Equivalently, $lcm(a, b)$ *is the smallest non-negative integer divisible by both* a *and* b.

Example 4. $lcm(12, 18) = 36$

Definition 6. *Two integers* a *and* b *are said to be relatively prime or co-prime if* $\gcd(a, b) = 1$.

Definition 7. *An integer* $p \geq 2$ *is said to be prime if its only positive divisors are* 1 *and* p*. Otherwise,* p *is called composite.*

Fact 2. *(Fundamental theorem of arithmetic) Every integer* $n \geq 2$ *has a factorization as a product of prime powers:*

$$n = p_1^{e_1} ... p_k^{e_k}$$

where p_i *are distinct primes and* e_i *are positive integers. Furthermore, the factorization is unique.*

Fact 3. *if* $a = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ *and* $p_1^{f_1} p_2^{f_2} ... p_k^{e_k}$ *then:*

$$\gcd(a, b) = p_1^{min(e_1, f_1)} p_2^{min(e_2, f_2)} ... p_k^{min(e_k, f_k)}$$

$$lcm(a, b) = p_1^{max(e_1, f_1)} p_2^{max(e_2, f_2)} ... p_k^{max(e_k, f_k)}$$

Remark 1. *The above definition implies that* $a.b = \gcd(a, b).lcm(a, b)$

I.2 Algorithms in $\mathbb{Z}$

Let a and b be non negative integers of size $|a|$ and $|b|$ respectively. We will consider that $|a|, |b| \leq n$, in other terms, their binary representation needs at most n bits. The number of bit operations (or the complexity) of the four basic integer operations of addition, substraction, multiplication and division using the classical algorithms is summarized in the following table.

Operation	**Bit complexity**
Addition $a + b$	$O(max(\|a\|, \|b\|)) = O(n)$
Substraction $a - b$	$O(max(\|a\|, \|b\|)) = O(n)$
Multiplication $a.b$	$O(\|a\|.\|b\|) = O(n^2)$
Division $a = qb + r$	$O(\|q\|.\|b\|) = O(n^2)$

I.3 The integers modulo n

Let n be a positive integer.

Definition 8. *If a and b are integers, then a is said to be* congruent to b modulo n*, written $a \equiv \pmod{n}$, if n divides $(a-b)$. The integer n is called the* modulus *of the congruence.*

Example 5. *1.* $24 \equiv 9 \pmod{5}$ *since* $24 - 9 = 3.5$

2. $-11 \equiv 17 \pmod{7}$ *since* $-11 - 17 = -4.7$

Fact 4. ***(properties of congruences)*** *For all $a, a_1, b, b_1, c \in \mathbb{Z}$, the following are true:*

1. *$a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.*
2. *(reflexivity) $a \equiv a \pmod{n}$*
3. *(symmetry) if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$*
4. *(transitivity) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$*
5. *if $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$, then $a + b \equiv a_1 + b_1 \pmod{n}$ and $ab \equiv a_1 b_1 \pmod{n}$.*

The *equivalence class* of an integer a, denoted $cl(a)$, is the set of all integers congruent to a modulo n. From properties $2, 3$ and 4, it can be seen that for a fixed n, the relation of *congruence modulo n* **partitions** $\mathbb{Z}$ into equivalence classes. In fact, for all $i \in \mathbb{Z}$, $a \in cl(a)$ (reflexivity) thus $\mathbb{Z} = \bigcup_{i \in \mathbb{Z}} cl(i)$. From the other hand, if $x \in cl(a) \cap cl(b)$, then $a \in cl(b)$ (symmetry + transitivity), it follows by the same properties that $cl(a) = cl(b)$, which proves that the equivalence classes are disjoint.
Now if $a = qn + r$, where $0 \leq r < n$, then $a \equiv r \pmod{n}$. Hence, each integer a is congruent modulo n to a unique integer between 0 and $n - 1$. Thus a and r are in the same equivalence class, and so r may simply be used to represent this equivalence class.

Definition 9. *The* integers modulo n*, denoted $\mathbb{Z}_n$, is the set of (equivalence classes of) integers $\{0, 1, ...n-1\}$. Addition, substraction and multiplication in $\mathbb{Z}_n$ are performed modulo n.*

Example 6. $\mathbb{Z}_2 = \{0, 1\}$. *In $\mathbb{Z}_2$, $1 + 1 = 0$, since $1 + 1 = 2 = 0 \pmod{2}$. Similarly $1.1 = 1$ in $\mathbb{Z}_2$. It is obvious that the relation* congruent modulo 2 ***partitions*** *$\mathbb{Z}$ into two dsjoints sets, the set of integers congruent to 1 modulo 2 , and the set of integers congruent to 0 modulo 2, in other terms, it partions $\mathbb{Z}$ into the set of odd integers and the set of even integers.*

Definition 10. *Let $a \in \mathbb{Z}_n$. The multiplicative inverse of $a \pmod n$ is an integer $x \in \mathbb{Z}_n$ such that $ax = 1 \pmod n$. If such inverse exists, it is unique and is denoted a^{-1}.*

Fact 5. *a is inversible if and only if $\gcd(a, n) = 1$. Moreover, this inverse can be efficientely computed using the Extended Euclidean Algorithm.*

Proof. Extended Euclidean Algorithm. □

II Extended Euclidean Algorithm

The greatest common divisor of two integers a and b can be computed via Fact 3. However, computing a gcd by first obtaining the prime factorization of the given numbers does not result in an efficient algorithm, as the problem of factoring integers appears to be difficult. The `Euclidean Algorithm` is an efficient algorithm for computing the greatest common divisor of two integers that does not require the factorization of the integers. It is based on the following fact:

Fact 6. *If a and b are positive integers with $a \geq b$, then $\gcd(a, b) = \gcd(b, a \bmod b)$*

1. prove the above fact.
2. write the `Euclidean Algorithm` that computes the gcd of two integers.
3. compute the $\gcd(4864, 3458)$.
4. The Euclidean algorithm can be extended so that it does not only yield the greatest common divisor of two integers a and b, but also integers a and b satisfying $ax + by = \gcd(a, b)$. We first notice that the `Euclidean Algorithm` calculates a sequence defined by a two term recurrence:

   $$a_0 = a, a_1 = b, a_{n-1} = q_n a_n + a_{n+1}$$

   where $q_n = \lfloor \frac{a_{n-1}}{a_n} \rfloor$.
   In other terms:

   $$a_{n+1} = -q_n a_n + a_{n-1}$$

   Now, we consider the sequences (x_n) and y_n defined by:

   $$x_0 = 1, x_1 = 0, x_{n+1} = -q_n x_n + x_{n-1}$$
   $$y_0 = 0, y_1 = 1, y_{n+1} = -q_n y_n + y_{n-1}$$

- prove, by induction, that $a_n = ax_n + by_n$.
- write the `Extended Euclidean Algorithm` that computes the gcd of two integers a and b in addition to two integers x and y such that $ax + by = \gcd(a, b)$.
- example: a=4864, b=3458.

III Subliminal channels in digital signature schemes

A digital signature scheme is given by three algorithms, namely, the *key generation*, the *signing* and the *verification* algorithms.
In this exercise, we show how to exploit the weakness of the Elgamal's signature scheme in order to communicate invisibly.
The Elgamal's scheme is defined as follows:

- **Setup.** Choose a prime p and a generator g of $\mathbb{Z}_p^\times$.
- **Key generation.** Choose a random number $x \in_R \mathbb{Z}_{p-1}$ and calculate $y = g^x \bmod p$. The private (signing) key is x and the public (verifying) key is y.
- **Signing.** To sign a message $m \in \mathbb{Z}_{p-1}$: pick a random number $k \in_R \mathbb{Z}_{p-1}$ and compute $a = g^k \bmod p$ and $b = k^{-1}(m - xa) \bmod (p - 1)$. The signature is the pair (a, b).

1. Write the verification equation.
2. Explain how Alice could communicate inivisibly with Bob, using this signature scheme, and how an active warden manages to foil such a communication.