Cryptography – BCS
Public-Key Cryptography – RSA

Pierre-Alain Fouque

Université de Rennes 1

September, 15 2020

Agenda

Group

Definition (Group)

A group G is a set of elements with a binary operation $\cdot$ such that

1. Closure : For all $a, b \in G$, $a \cdot b \in G$.
2. Associativity : For all a, b and c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Identity element : Let G, st $e \cdot a = a \cdot e = a$. It is unique and is called the identity element.
4. Inverse element : For each $a \in G$, there exists an element $b \in G$, denoted a^{-1} (or $-a$, if the operation is denoted "+"), st $a \cdot b = b \cdot a = e$, where e is the identity element.
5. abelian – optional : If $a \cdot b = b \cdot a$, G is called abelian.

Definition (Group morphism)

A function $a : G \to H$ between two groups $(G, \cdot)$ and $(H, \star)$ is called a homomorphism if for all $g, k \in G$, $a(g \cdot k) = a(g) \star a(k)$

Example & Subgroup

Examples

- $(\mathbb{N}, +)$, $(\mathbb{Z}, \times)$ are not group
- $(\mathbb{Z}, +)$, $(\{-1, +1\}, \times)$, $(\mathbb{Q}, \times)$ are groups

Definition (Subgroup)

It is a group H contained within a bigger one, G. The identity element of G is in H, and whenever h_1 and h_2 are in H, then so are $h_1 \cdot h_2$ and h_1^{-1}. The elements of H, equipped with the group operation on G restricted to H, form a group

Example

- $(3\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$ as $0 \in 3\mathbb{Z}$, and if $h_1, h_2 \in 3\mathbb{Z}$, $h_1 + h_2$ is in $3\mathbb{Z}$ and $-h_1 \in 3\mathbb{Z}$
- The quotient group $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ where $\bar{a} = \{k \in \mathbb{Z} | k = a \bmod n\}$

Ring, Field

Definition (Ring - Example $(\mathbb{Z}, +, \cdot)$)

1. R is an abelian group under addition, i.e. :
   $+$ is associative : $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$
   $+$ is commutative : $a+b = b+a$ for all $a, b \in R$
   0 is the additive identity : $0 \in R$ st $a+0 = a$ for all $a \in R$
   $-a$ is the additive inverse of a : If $a, -a \in R$, st $a+(-a) = 0$
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$ ($\cdot$ is associative)
   There is an element $1 \in R$ st $a \cdot 1 = a$ and $1 \cdot a = a$ for all $a \in R$ (1 is the multiplicative identity)
3. Multiplication is distributive with respect to addition
   $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$
   $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$

Definition (Field - Example $(\mathbb{Q}, +, \cdot)$)

A ring with an identity element for $\cdot$ st all non-zero element has an inverse for $\cdot$

Euclidean Division

Proposition (Euclidean Division)

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$*. There exists a unique pair* $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ *st*

$$a = bq + r \text{ and } 0 \leq r < |b|.$$

q, r *are called the quotient and the remainder of the euclidean division of* a *by* b*.*

Lemma

Let H *be a subgroup of* $\mathbb{Z}$*. There exists a unique* $n \in \mathbb{N}$ *st* $H = n\mathbb{Z}$*.*

Example

Let a and b two non-zero integers. The set $a\mathbb{Z} + b\mathbb{Z} = \{au + bv | u, v \in \mathbb{Z}\}$, is a subgroup of $\mathbb{Z}$. There exists a unique integer $d \geq 1$ st $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Greatest common divisor

Definition

The integer d is called the Greatest common divisor of a and b, and written $d = \gcd(a, b)$.

Bézout Property

There exist two integers u and v st $d = au + bv$.

Lemma

The gcd of a and b is the unique integer st :

1. *it is a divisor of a and b.*
2. *it is a multiple of any common divisor of a and b.*

Definition

a and b are coprime (a is prime with b), if $\gcd(a, b) = 1$.

Greatest common divisor

Lemma

a and b are coprime iff $\exists\ (u, v) \in \mathbb{Z}^2$ *st* $au + bv = 1$.

Corollary

The integers $\frac{a}{d}$ *and* $\frac{b}{d}$ *are coprime.*

Least Common Multiple

Definition

Given two non-zero integers a and b, the set $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. The integer m st

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

is called the least common multiple of a and b.

Proposition

$$\gcd(a, b)\,\mathrm{lcm}(a, b) = |ab|.$$

Euclidean Algorithm (Computation of the gcd)

Definition

Define a finite sequence of integers $(r_i)_{i \geq 0}$, called the sequence of remainders (defined to a and b), as follows : we define

$$r_0 = a \text{ and } r_1 = b.$$

Let $r_0, r_1, \cdots, r_i$ for $i \geq 1$. It $r_i \neq 0$, r_{i+1} is the remainder of the euclidean division of r_{i-1} by r_i. If $r_i = 0$, the process will stop and the sequence of remainders is $r_0, r_1, \cdots, r_{i-1}, r_i$. There exists a unique integer $n \geq 1$ st :

$$0 < r_n < r_{n-1} < \ldots < r_1 < r_0 \text{ and } r_{n+1} = 0.$$

Proposition

$$r_n = \gcd(a, b).$$

Computation of Bézout Relation

Definition

Two sequences of integers $(u_i)_{0 \leq i \leq n}$ and $(v_i)_{0 \leq i \leq n}$ st

$$u_0 = 1, u_1 = 0 \text{ and } v_0 = 0, v_1 = 1,$$

$$u_{i+1} = u_{i-1} - u_i q_i \text{ and } v_{i+1} = v_{i-1} - v_i q_i \text{ for } i = 1, \ldots, n-1,$$

where q_i is the quotient of the euclidean division of r_{i-1} by r_i.

Proposition

$$r_n = a u_n + b v_n$$

Theorem (Complexiy)

$$n \leq \frac{3}{2 \log 2} \log b + 1$$

Computation of inverse mod n

Inverse of a mod n

- The inverse of a mod n is an integer $b + n\mathbb{Z}$ such that

$$ab = 1 \bmod n$$

- If we compute the Extended Euclidean Algorithm on a, n we get two integers u, v such that

$$au + nv = \gcd(a, n)$$

- If $\gcd(a, n) = 1$, $au + nv = 1$ and we compute this relation mod n, we get

$$au = 1 \bmod n$$

  meaning that u is the inverse of a mod n.
- Sometimes, we have to add a multiple of n to get a value between 1 and $n - 1$.

Prime Numbers

Definition (Prime Number)

Any integer $p \geq 2$ whose only positive divisors are 1 and p.

Lemma

Let p an integer ≥ 2*. Then, p is prime iff p is not the product of two integers strictly larger than* 1*.*

Corollary (Euclide)

The set of prime numbers is infinite.

Fundamental Theorem of Arithmetic

Theorem

Any integer $n \geq 2$ can be uniquely written as

$$n = p_1^{n_1} \dots p_r^{n_r},$$

where the n_i are non negative integers, and the p_i are primes st $p_{i-1} < p_i$ for all $i = 2, \dots, r$, called the decomposition of n into prime factors.

Theorem ($\pi(x)$: Number of primes $\leq x$ - $\pi(x) \simeq \frac{x}{\log x}$)

For all real $x \geq 2$, we have

$$\left(\frac{\log 2}{2}\right)\frac{x}{\log x} \leq \pi(x) \leq (9 \log 2)\frac{x}{\log x}.$$

Numeration in base $b \geq 2$

Theorem

Let x a non negative integer. We can write x uniquely as

$$x = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0$$

where $n \in \mathbb{N}$, $a_0, \ldots, a_n \in \mathbb{N}$ st $0 \leq a_i \leq b - 1$ and a_n is non zero.
$x = a_n a_{n-1} \ldots a_1 a_0$: decomposition of x in base b and
$x = (a_n \cdots a_0)_b$.

Theorem (Fast Exponentiation)

We can compute x^n with $O(\log n)$ multiplications

Chinese Remainder Theorem

Theorem

Let m and n two non negative coprime integers.

$$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

defined st for all $a \in \mathbb{Z}$

$$f(a) = (a + m\mathbb{Z}, a + n\mathbb{Z}),$$

is an onto ring morphism, whose kernel is $mn\mathbb{Z}$*.*
The rings $\mathbb{Z}/mn\mathbb{Z}$ *et* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *are isomorphs given the map* $a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$

Euler Totient Function

Definition

For all $n \geq 1$, the integer $\varphi(n)$ is the number of integers between 1 and n, and coprime with n.

$$\varphi(n) = \{1 \leq k \leq n : \gcd(k, n) = 1\}$$

Lemma

For all prime p and integer $r \geq 1$, we get

$$\varphi(p^r) = p^r - p^{r-1}$$

Lemma

Let $n \geq 1$. An integer a and $\bar{a}$ its class mod $n\mathbb{Z}$. Then, $\bar{a}$ is invertible in $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(a, n) = 1$.

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}$$

Euler Totient Function

Corollary (The order of $(\mathbb{Z}/n\mathbb{Z})^*$ is $\varphi(n)$.)

The ring $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.

Corollary

Let m and n two non-negative coprime integers. We get

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Theorem

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Euler Theorem

Theorem (Euler, 1760)

Let n a non-negative integer. For all integer a coprime with n,

$$a^{\varphi(n)} = 1 \bmod n$$

Proposition

Let G an abelian group of order n, with identity element e.

$$\textit{For all } x \in G, \textit{ we have } x^n = e.$$

Corollary (Fermat Little Theorem)

Let p be a prime number. For all integer a non divisible by p,

$$a^{p-1} = 1 \bmod p$$

In particular, for all integer a, we get $a^p = a \bmod p$