Appunti sulla Dimostrazione dell’Algoritmo RSA

Federico Zotti

21/12/2022

Indice

Definizioni di base

Semigruppo

Consideriamo un insieme G non vuoto e un'operazione binaria ($\otimes$) che agisce sugli elementi di G.

> Per operazione binaria si intende un'operazione con due operandi.

L'operazione non può restituire un elemento non appartenente al gruppo di partenza. Questa proprietà viene detta di **chiusura**:

$$\forall a, b \in G, \exists c \in G : c = a \otimes b$$

Un'altra proprientà è l'**associatività**:

$$\forall a, b, c \in G : (a \otimes b) \otimes c = a \otimes (b \otimes c)$$

Ogni insieme che gode di queste due proprietà è detto **semigruppo**.

Monoide

Se nel semigruppo G:

$$\exists e \in G : \forall a \in G, a \otimes e = e \otimes a = a$$

allora e è elemento neutro e $(G, \otimes)$ è un **monoide**.

Gruppo

Se in un monoide G:

$$\forall a \in G, \exists b \in G : a \otimes b = b \otimes a = e$$

allora b è elemento inverso di a:

$$a = \overline{b}$$

$$b = \overline{a}$$

Se ogni elemento di G è invertibile allora $(G, \otimes)$ è un **gruppo**.

Gruppo abeliano o commutativo

Se nel gruppo $(G, \otimes)$ l'operazione $\otimes$ è commutativa allora esso è un **gruppo abeliano** o **commutativo**.

Ordine di un gruppo

L'ordine di un gruppo finito $(G, \otimes)$, indicata con $o(G)$ è la cardinalità di quel gruppo.

Gruppo ciclico

Un gruppo finito è **ciclico** quando hanno almeno un elemento che applicato all'operazione del gruppo un determinato numero di volte può generare tutti gli altri elementi del gruppo stesso.

$$\text{Se } \exists g, n \in G : \forall a \in G, a = g \otimes g \otimes \cdots \otimes g \, [n \text{ volte}] = g^n \Rightarrow G \text{ è ciclico}$$

Se un gruppo è *commutativo* allora ha almeno un generatore (e viceversa).

Prendendo (x) l'insieme degli elementi generati da x:

$$\forall x \in G, (x) = H \subseteq G$$

Lemmi

L'elemento neutro di un gruppo è unico

Dimostrazione:

$$\exists\, e, f : e \neq f : \forall a \in G \Rightarrow e + a = a + e = f + a = a + f = a \Rightarrow e = e + f = f$$

Leggi di cancellazione

Dato un gruppo G e tre elementi a, x, y appartenenti a G se $a + x = a + y \Rightarrow x = y$, e viceversa, se $x + a = y + a \Rightarrow x = y$.

Dimostrazione:

$$x = e + x = (b + a) + x = b + (a + x) = b + (a + y) = (b + a) + y = e + y = y$$

Unicità dell'inverso

$$\forall a \in G \exists! b \in G : b + a = a + b = e$$

Dimostrazione:

$$\forall a \in G \exists b, c \in G : b = \overline{a} \land c = \overline{a} \land b \neq c$$
$$e = a + b \land e = a + c$$
$$b = c$$

L'inverso dell'inverso è l'elemento stesso

$$\forall a \in G : \overline{(\overline{a})} = a$$

Dimostrazione:

$$b = \overline{a}$$
$$\overline{b} + b = e$$
$$\overline{b} + \overline{a} = e$$
$$\overline{b} + \overline{a} + a = e + a$$
$$\overline{b} + e = a$$
$$\overline{b} = a$$
$$\overline{(\overline{a})} = a$$

$\overline{(a + b)} = \overline{b} + \overline{a}$

Dimostrazione:

$$(\overline{b} + \overline{a}) + (a + b) = \overline{b} + (\overline{a} + (a + b) = \overline{b} + (\overline{a} + a) + b = \overline{b} + e + b = \overline{b} + b = e$$