Appunti sulla Dimostrazione dell'Algoritmo RSA

Federico Zotti

21/12/2022

Indice

1 Definizioni di base

1.1 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**.

1.2 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**.

1.3 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**.

1.4 Gruppo abeliano o commutativo

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

1.5 Ordine di un gruppo

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

1.6 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.

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

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

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

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