Il cifrario RSA

Un'applicazione dell'algebra alla vita quotidiana

Davide Borra

Lezioni Entusiasmanti in Serata Accademica

26 marzo 2023

UNIVERSITÀ DI TRENTO

Sommario

Introduzione

La crittografia è una parte fondamentale della vita di tutti i giorni. Oggi più che mai è fondamentale avere degli strumenti per scambiare messaggi senza che il loro contenuto possa essere decifrato da altri.
Con il tempo si sono sviluppati due sistemi di crittografia:

- **Crittografia simmetrica:** la chiave per utilizzata per crittare è la stessa utilizzata per decrittare. Questi cifrari sono in generale più efficienti ma hanno il problema che bisogna comunicare al destinatario la chiave.
- **Crittografia asimmetrica:** per crittare e decrittare vengono utilizzate due chiavi diverse. Questo sistema risolve il problema dello scambio di chiavi ma è meno efficiente.

Crittografia asimmetrica

Consideriamo un'analogia: la chiave pubblica è il lucchetto e la chiave che apre il lucchetto è chiave privata. Quando vengono generate le chiavi, il destinatario genera contemporaneamente chiave e lucchetto, e rende pubblico il lucchetto. Chi vuole mandargli un messaggio "chiuderà" quindi il messaggio con il lucchetto, e solo l'effettivo destinatario sarà in possesso della chiave per aprirelo.

Crittografia asimmetrica

Consideriamo un'analogia: la chiave pubblica è il lucchetto e la chiave che apre il lucchetto è chiave privata. Quando vengono generate le chiavi, il destinatario genera contemporaneamente chiave e lucchetto, e rende pubblico il lucchetto. Chi vuole mandargli un messaggio "chiuderà" quindi il messaggio con il lucchetto, e solo l'effettivo destinatario sarà in possesso della chiave per aprirelo.

Il più usato sistema di crittografia simmetrica è il cifrario RSA, dai nomi dei suoi ideatori (Ronald Rivest, Adi Shamir e Leonard Adleman), e si basa su alcuni semplici concetti di algebra dei resti.

Algebra dei resti

DEF (Congruenze)

Definiamo una relazione di equivalenza $\equiv \subset \mathbb{Z}^2$ tale che

$$x \equiv y \mod n \iff \exists k \in \mathbb{Z} \text{ tale che } a - b = kn$$

Ovvero se il resto della divisione di a per n è uguale a quello della divisione di b per n.

Consideriamo ad esempio le congruenze di resto modulo 3, allora si individuano le tre classi:

$$\cdots \equiv -9 \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv 12 \equiv \cdots$$

$$\cdots \equiv -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv 13 \equiv \cdots$$

$$\cdots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv 11 \equiv 13 \equiv \cdots$$

Reciproci

Scelto un n (d'ora in poi scriverò "in $\mathbb{Z}_{/n\mathbb{Z}}$"), definiamo il reciproco di un numero a come quel numero b tale che

$$ab \equiv 1 \mod n$$

Osservazione

Se a è il reciproco di b modulo n, allora anche b è il reciproco di a.

Osservazione

Non tutti i numeri hanno un reciproco in $\mathbb{Z}_{/n\mathbb{Z}}$. Quando un numero ha reciproco si dice "invertibile". Se l'MCD tra a e n, a è invertibile, di conseguenza se n è un numero primo, tutti i numeri sono invertibili.

La funzione di Eulero

DEF (Funzione di Eulero)

Definiamo la funzione $\varphi : \mathbb{N}_0 \to \mathbb{N}_0$, tale che $\varphi(n) = \#\{k \in \mathbb{N} \,|\, k < n \wedge MCD(n, k) = 1\}$, ovvero che conta il numero di interi positivi minori di n e “coprimi” con n.

Segue dalla definizione di numero primo che, se p è un numero primo. $\varphi(p) = p - 1$
Essa ha una peculiare proprietà, se p e q sono due interi tali che $MCD(p, q) = 1$, allora

$$\varphi(pq) = \varphi(p) \cdot \varphi(q)$$

In particolare, se sono primi $\varphi(pq) = (p - 1)(q - 1)$.

Il teorema di Eulero

Teorema (Eulero)

Se $MCD(a, n) = 1$, *allora*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Uno strumentopolo misterioso che ci servirà più tardi: osserviamo che se $b \equiv 1 \mod n$, è come scrivere che per qualche k,

$$b = kn + 1$$

In particolare se $b \equiv 1 \mod \varphi(n)$, allora

$$a^b = a^{k\varphi(n)+1} = a^{k\varphi(n)} \cdot a = \left(a^{\varphi(n)}\right)^k \cdot a \equiv 1^k \cdot a = a \mod n$$

Il cifrario RSA

Come detto prima, il cifrario RSA è un sistema di crittografia asimmetrica. Esso si basa quindi su due chiavi, la chiave pubblica 🔒 e la chiave privata 🔑. Vediamo quindi l'algoritmo per generare le chiavi:

1. Si scelgono due numeri primi p e q, che devono restare segreti, e si calcola il loro prodotto N, che viene invece reso pubblico.
   I numeri p e q scelti sono molto grandi, quindi è quasi impossibile risalirvi conoscendo N.

Il cifrario RSA

Come detto prima, il cifrario RSA è un sistema di crittografia asimmetrica. Esso si basa quindi su due chiavi, la chiave pubblica 🔒 e la chiave privata 🔑. Vediamo quindi l'algoritmo per generare le chiavi:

1. Si scelgono due numeri primi p e q, che devono restare segreti, e si calcola il loro prodotto N, che viene invece reso pubblico.
   I numeri p e q scelti sono molto grandi, quindi è quasi impossibile risalirvi conoscendo N.
2. Si calcola inoltre il valore di $\varphi(N)$, che deve rimanere segreto.

Il cifrario RSA

Come detto prima, il cifrario RSA è un sistema di crittografia asimmetrica. Esso si basa quindi su due chiavi, la chiave pubblica e la chiave privata. Vediamo quindi l'algoritmo per generare le chiavi:

1. Si scelgono due numeri primi p e q, che devono restare segreti, e si calcola il loro prodotto N, che viene invece reso pubblico.
   I numeri p e q scelti sono molto grandi, quindi è quasi impossibile risalirvi conoscendo N.
2. Si calcola inoltre il valore di $\varphi(N)$, che deve rimanere segreto.
3. Si calcola quindi il più piccolo numero e coprimo con $\varphi(n)$ e il suo reciproco d

Riassumendo

	p	primo	privato
	q	primo	privato
	N	pq	pubblico
	$\varphi(N)$	$(p-1)(q-1)$	privato
	e	$\min\{z \in \mathbb{N} \mid MCD(z, \varphi(n))\}$	pubblico
	d	reciproco di e	privato

Il funzionamento

Sia m il messaggio che vogliamo trasmettere. Il mittente è a conoscenza della chiave pubblica del destinatario, per cui può sfruttarla per crittarlo. Calcola quindi

$$m^{🔒} \equiv m^e \mod N$$

Il funzionamento

Sia m il messaggio che vogliamo trasmettere. Il mittente è a conoscenza della chiave pubblica del destinatario, per cui può sfruttarla per crittarlo. Calcola quindi

$$m^{\text{🔒}} \equiv m^e \mod N$$

Il destinatario riceve quindi $m^{\text{🔒}}$, e solo lui è in grado di decrittarlo perchè solo sui possiede la propria chiave privata d. Calcola quindi

$$\left(m^{\text{🔒}}\right)^d = (m^e)^d = m^{de} \equiv m \mod N$$

risalendo quindi al messaggio originale

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**
  1. Scegliamo $p = 5$ e $q = 11$, allora $N = pq = 55$.

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**
  1. Scegliamo $p = 5$ e $q = 11$, allora $N = pq = 55$.
  2. Calcoliamo $\varphi(55) = (5-1)(11-1) = 40$

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**
  1. Scegliamo $p = 5$ e $q = 11$, allora $N = pq = 55$.
  2. Calcoliamo $\varphi(55) = (5 - 1)(11 - 1) = 40$
  3. Il più piccolo numero coprimo con 40 è $e = 3$, e ha reciproco $d = 27$, infatti $27 \cdot 3 = 81 \equiv 1 \mod 40$.

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**
  1. Scegliamo $p = 5$ e $q = 11$, allora $N = pq = 55$.
  2. Calcoliamo $\varphi(55) = (5-1)(11-1) = 40$
  3. Il più piccolo numero coprimo con 40 è $e = 3$, e ha reciproco $d = 27$, infatti $27 \cdot 3 = 81 \equiv 1 \mod 40$.
- **Trasmissione del messaggio**

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**
  1. Scegliamo $p = 5$ e $q = 11$, allora $N = pq = 55$.
  2. Calcoliamo $\varphi(55) = (5-1)(11-1) = 40$
  3. Il più piccolo numero coprimo con 40 è $e = 3$, e ha reciproco $d = 27$, infatti $27 \cdot 3 = 81 \equiv 1 \mod 40$.
- **Trasmissione del messaggio**
  1. Il mittente calcola
  $$m^{🔒} \equiv 13 \mod N \quad (7^3 = 343 \equiv 13 \mod 55)$$

Un esempio

Supponiamo di voler trasmettere il messaggio $m = 7$:

- **Generazione delle chiavi**
  1. Scegliamo $p = 5$ e $q = 11$, allora $N = pq = 55$.
  2. Calcoliamo $\varphi(55) = (5-1)(11-1) = 40$
  3. Il più piccolo numero coprimo con 40 è $e = 3$, e ha reciproco $d = 27$, infatti $27 \cdot 3 = 81 \equiv 1 \mod 40$.
- **Trasmissione del messaggio**
  1. Il mittente calcola
     $$m^{\text{🔒}} \equiv 13 \mod N \quad (7^3 = 343 \equiv 13 \mod 55)$$
  2. Il destinatario riceve quindi $m^{\text{🔒}}$, che decritta calcolando
     $$m = \left(m^{\text{🔒}}\right)^d = 13^{27} = 1192533292512492016559195008117 \equiv 7 \mod 55$$
     risalendo quindi al messaggio originale