

Teoria dei numeri e Crittografia

Christian Ferrari

Introduzione alla crittografia ed alcuni esempi introduttivi

Presentazione

In questa serie di attività affronteremo un tema di matematica applicata con lo scopo di mostrare come questa disciplina non è fine a se stessa, come spesso si sente affermare, ma che possiede delle applicazioni nella vita di tutti i giorni. Gli scambi di informazione sono sempre stati di fondamentale importanza nelle società, sia civile sia militare. Ai giorni nostri, in una società in cui la tecnologia legata all'informazione avanza ad una velocità sempre più frenetica, la possibilità di scambiare informazione in modo sicuro è diventata una necessità di primaria importanza. Già ai tempi dell'impero romano Giulio Cesare aveva concepito una tecnica in grado di scambiare informazione in modo (abbastanza) sicuro, poi durante la prima e la seconda guerra mondiale altri sforzi in questa direzione furono intrapresi. Nell'era dell'informatica, e in particolare di Internet, la questione dello scambio sicuro di informazione riguarda non più solo l'ambito militare ma anche quello civile e ci concerne tutti: pensiamo ad esempio alle carte bancarie oppure all'acquisto on-line.

Con questa serie di attività vedremo diversi aspetti della matematica in azione, con lo scopo ultimo di approfondire e capire il sistema maggiormente utilizzato per rendere sicuro lo scambio di informazione, avremo quindi la possibilità di approfondire diversi aspetti dell'aritmetica in un contesto applicato come la *crittografia*, ossia la scienza che si occupa della sicurezza dell'informazione.

Per tutte queste attività è fondamentale avere la calcolatrice!

Introduzione alla crittografia

I possibili metodi crittografici si suddividono in due grandi classi.

- La *crittografia a chiave privata*: Alice e Bob vogliono scambiare informazione in modo segreto, Alice nasconde il messaggio originale grazie ad una chiave k conosciuta solo da lei e Bob, il quale grazie alla *stessa* chiave k decifra il messaggio, per questo motivo questo sistema è anche chiamato *crittografia a chiave simmetrica*.
- La *crittografia a chiave pubblica*: Alice e Bob vogliono scambiare informazione in modo segreto, Alice nasconde il messaggio originale grazie ad una chiave e fornita da Bob e di dominio pubblico, quest'ultimo grazie ad un'altra chiave d , conosciuta solo da lui, decifra il messaggio, per questo motivo questo sistema è anche chiamato *crittografia a chiave asimmetrica*.

Possiamo rappresentarci i due metodi con la seguente analogia. Metaforicamente la crittografia a chiave privata corrisponde alla situazione in cui Alice e Bob (e solo loro) possiedono la *stessa* chiave per chiudere una cassaforte nella quale viene inserito il messaggio; mentre la crittografia a chiave pubblica metaforicamente corrisponde alla situazione in cui Bob (che sarà il destinatario) invia ad Alice una cassaforte con due aperture ed una chiave monouso (la chiave pubblica), la quale dopo aver inserito il messaggio la chiude ed invia il tutto a Bob, che avendo la chiave della seconda apertura (la chiave privata) può accedere al messaggio.

Entrambi i metodi hanno vantaggi e svantaggi.

- *Crittografia a chiave privata*: il vantaggio è l'assoluta segretezza della comunicazione; lo svantaggio (non irrilevante!) è la necessità che Alice e Bob si incontrino per scambiarsi in modo assolutamente sicuro la chiave k , a tal proposito è importante osservare che affinché la comunicazione sia assolutamente sicura è necessario che la chiave k sia utilizzata una sola volta.
- *Crittografia a chiave pubblica*: il vantaggio è che Alice e Bob non necessitano di incontrarsi, il destinatario è sufficiente che comunichi (anche non in modo sicuro) la **chiave pubblica** e con la quale il mittente cifra il messaggio (mentre la **chiave privata** per decifrare è unicamente conosciuta dal destinatario); lo svantaggio sta nel fatto che conoscendo la chiave pubblica e è fondamentale essere certi che nessuno sia in grado di recuperare la chiave privata d , questo dipende dal dettaglio del sistema di crittografia.

Tra i metodi di crittografia a chiave pubblica vi è la crittografia RSA che si fonda sulla teoria dei numeri e la cui sicurezza, come vedremo, è garantita dalla difficoltà di fattorizzare in numeri primi numeri con molte cifre.

Un esempio storico

Una delle prime tecniche di crittografia è il **cifrario di Cesare**, esso consiste nello scrivere il messaggio originale e poi di sostituire tutte le lettere con la terza lettera seguente. Ad esempio la A è sostituita con la D , la B con la E e via di seguito, e una volta raggiunta l'ultima lettera si ricomincia da capo, esattamente come se le lettere fossero disposte in modo circolare, per esempio la Z è sostituita con la C . Il destinatario per decifrare il messaggio non fa altro che operare la sostituzione al contrario.

- Ad ogni lettera dell'alfabeto (composto dalle 26 lettere)

$ABCDEFGHIJKLMNOPQRSTUVWXYZ$

si associa un numero da 0 a 25 nel modo seguente:

$A \leftrightarrow 0 \quad B \leftrightarrow 1 \quad C \leftrightarrow 2 \quad \dots \quad Y \leftrightarrow 24 \quad Z \leftrightarrow 25$

al messaggio viene poi assegnata una lista di numeri e viceversa.

- Per *cifrare* il messaggio è sufficiente aggiungere ad ogni numero 3 (che gioca il ruolo di *chiave* e che può essere cambiata) considerando i numeri da 0 a 25 disposti in modo circolare, la lista di numeri così ottenuta costituisce il messaggio da inviare.
- Per *decifrare* il messaggio è sufficiente sottrarre ad ogni numero della lista 3 o aggiungere $23 (= 26 - 3)$ sempre con i numeri disposti in modo circolare.

Questo protocollo è un esempio concreto di *crittografia a chiave privata*, infatti il numero 3 gioca il ruolo della chiave ed è la stessa per il mittente ed il destinatario, i quali devono essere gli unici ad esserne a conoscenza.

Osserviamo che, se ai tempi di Cesare poteva funzionare, questo sistema è poco sicuro, perché conoscendo il messaggio cifrato ma non la chiave è sufficiente provare le 26 possibilità per decifrare il messaggio.

Esercizio Da svolgere in gruppi (3/4 persone).

1. Provate a scambiare alcuni messaggi semplici.
2. Costruite poi la tavola di addizione per l'insieme dei numeri da 0 a 25 disposti circolarmente.
3. Che relazione esiste tra l'equivalenza $24 + 3 \equiv 1$ ed il resto della divisione euclidea $27 : 26$ o tra l'equivalenza $2 + 3 \equiv 5$ ed il resto della divisione euclidea $5 : 26$?
4. Conoscete altri esempi di numeri circolari?

Un'introduzione al protocollo RSA con Maple

Come prima attività possiamo simulare il protocollo RSA grazie ad una serie di operazioni eseguite dal software Maple, lo scopo non è quello di capire in dettaglio come si eseguono le operazioni, bensì di conoscere quali sono le operazioni necessarie sia alla *trasmissione dell'informazione* sia alla *generazione delle chiavi* pubblica e privata.

Esercizio

1. Riassumi le operazioni fondamentali della crittografia RSA.
2. Qual è la differenza tra crittografia a chiave privata e crittografia a chiave pubblica?
3. Perché la crittografia RSA è a chiave pubblica?

Cominciamo ad eseguire il protocollo RSA

Lo scopo di questo esempio semplice è di impratichirsi con il protocollo RSA senza però la necessità di conoscere tutti i concetti di aritmetica alla sua base, si tratta quindi di eseguire determinate operazioni semplici. L'attività è da svolgere in gruppi di 3/4 persone e quando si incontrano difficoltà di calcolo (numeri troppo grandi) ci si rivolgerà al docente.

Sia dato un messaggio $\mathcal{M} = \mathcal{M}_1\mathcal{M}_2 \dots \mathcal{M}_\ell$ costituito da una sequenza di lettere dove per ogni $1 \leq i \leq \ell$

$$\mathcal{M}_i \in \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}.$$

Più avanti avremo bisogno di introdurre lo spazio tra caratteri, ad esso assoceremo il numero 0, la corrispondenza carattere \leftrightarrow numero vista sopra è quindi spostata a destra di un'unità, ossia

$$A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \dots \quad Y \leftrightarrow 25 \quad Z \leftrightarrow 26.$$

Dopo aver associato al messaggio una lista di numeri, lo scopo è di cifrare alcuni messaggi *lettera per lettera* grazie alla chiave pubblica, costituita dalla coppia di numeri (n, e) , ed inviarli a due compagni del gruppo, i quali dovranno decifrarli grazie alla chiave privata, anch'essa data da una coppia di numeri (n, d) . Ecco le chiavi fornite.

Chiave numero	Chiave pubblica	Chiave privata
1	$(n = 35, e = 7)$	$(n = 35, d = 7)$
2	$(n = 33, e = 7)$	$(n = 33, d = 3)$
3	$(n = 34, e = 3)$	$(n = 34, d = 11)$
4	$(n = 39, e = 5)$	$(n = 39, d = 5)$
5	$(n = 51, e = 11)$	$(n = 51, d = 3)$
6	$(n = 38, e = 5)$	$(n = 38, d = 11)$
7	$(n = 33, e = 9)$	$(n = 33, d = 9)$
8	$(n = 33, e = 9)$	$(n = 3, d = 9)$
9	$(n = 35, e = 5)$	$(n = 35, d = 5)$

Per codificare e decodificare esegui le seguenti operazioni, M_i indica il numero associato alla lettera \mathcal{M}_i del messaggio:

- *codifica*: calcola $(M_i)^e$ e determina il resto della divisione euclidea

$$(M_i)^e : n$$

sia C_i questo numero;

- *decodifica*: calcola $(C_i)^d$ e determina il resto della divisione euclidea

$$(C_i)^d : n$$

il risultato è il numero M_i .

Per concludere analizziamo brevemente le chiavi utilizzate.

Esercizio Per ogni chiave qui sopra:

1. scomponi in fattori primi il numero n , troverai una fattorizzazione del tipo $n = pq$;
2. calcola il valore di $f = (p - 1)(q - 1)$;
3. calcola $\text{MCD}(e, f)$;
4. considerando i numeri circolari da 0 a $f - 1$, determina a cosa equivale il prodotto ed .

Riassumi le caratteristiche della chiave.

Esercizio Da svolgere in gruppi (3/4 persone).

1. Considera la chiave pubblica $(n = 10, e = 3)$, determina la chiave privata (n, d) .
2. Considera la chiave pubblica $(n = 15, e = 5)$, determina la chiave privata (n, d) .
3. Prova a costruire la tavola di moltiplicazione per i numeri circolari da 0 a $f - 1$ nel caso $n = 10$ e $n = 15$.
4. Considera il messaggio di quattro lettere *MATE*. Codifica il messaggio nel modo seguente: ad ogni lettera associa il numero m_i come sopra, ma invia ai destinatari (due per gruppo) il numero c_i tale che $m_i c_i \equiv 1$ nell'insieme dei numeri circolari da 0 a 26. Ai destinatari il compito di decodificare il messaggio.
(*Attenzione*: questo non è il protocollo di crittografia RSA).