Crittografia ed Aritmetica Modulare
– II incontro –

PLS - CAM

Padova, 24 ottobre 2014

Introduzione

Problema: A deve fare arrivare a B un certo messaggio, senza che alcun C venga a conoscenza del contenuto.

Soluzione: A codifica il messaggio in base a regole concordate tra A e B e spedisce il messaggio a B. B, conoscendo le regole di cifratura, è in grado di decodificare il messaggio e risalire all'originale. Se C viene in possesso del messaggio cifrato ma non conosce le regole di cifratura, non è in grado di risalire al messaggio originale.

Terminologia

Ingredienti:

$$\mathcal{T} = \{\text{messaggi in forma originale}\} \quad (\mathcal{T}\text{esto in chiaro})$$

$$\mathcal{C} = \{\text{messaggi in forma codificata}\} \quad (\text{testo in } \mathcal{C}\text{odice})$$

Una applicazione f invertibile da $\mathcal{T}$ a $\mathcal{C}$

$$\mathcal{T} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{T}$$

La quaterna $(\mathcal{T}, \mathcal{C}, f, f^{-1})$ è detta crittosistema, la funzione f chiave di cifratura (o di codifica) e la funzione f^{-1} chiave di decifrazione (o di decodifica).

Esempi

Metodo di Cesare$n \leq 21$ un intero fissato; data una lettera x, sia

$$f(x) = \begin{cases} x + n & \text{se } x + n \leq 21 \\ x + n - 21 & \text{se } x + n > 21 \end{cases}$$

Chiavi possibili: 21.

Esempio: $n = 7$

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C	D	E	F	G

GIULIO CESARE $\rightarrow$ PRESRV LNCHBN

Esempi

Cifratura Monoalfabeticadell'alfabeto fissato, e si sostituisca ogni lettera con la lettera corrispondente.

Chiavi possibili: 21!

Esempio:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
Q	E	R	T	U	I	O	P	A	S	D	F	G	H	L	Z	C	V	B	N	M

CIAO $\rightarrow$ RSQG

Metodo di Vigenère

Questa parola individua 4 funzioni del tipo "Cesare": $f_1 = x + 17$, $f_2 = x + 13$, $f_3 = x + 10$, $f_4 = x + 5$.

Per cifrare un messaggio con questa chiave, la prima lettera si cifra con f_1, la seconda con f_2, la terza con f_3, la quarta con f_4, la quinta con f_1, la sesta con f_2, ...

Esempio: QUESTO METODO NON È SICURO $\longrightarrow$ MMQA PEZB...

Possibili chiavi: infinite.

Problemi

1. La cifratura di Cesare è facilmente decifrabile, dato il numero ristretto di possibili chiavi.
2. Le cifrature monoalfabetiche e di Vigenère, pur avendo un numero elevato di possibili chiavi, sono decifrabili tramite considerazioni di tipo linguistico (ripetizioni di gruppi di lettere, analisi delle frequenze, . . .)
3. Anche complicando notevolmente i precedenti sistemi di cifratura (cfr. la macchina elettromeccanica "Enigma", 1920) la conoscenza del messaggio cifrato e della chiave di cifratura comporta la decifrazione del messaggio. Pertanto la chiave di cifratura deve rimanere segreta.

Il problema maggiore è quello della distribuzione delle chiavi.

Chiave pubblica

Nella maggior parte delle transazioni moderne (telefonia mobile, posta elettronica, acquisti internet con carta di credito, utilizzo di carte magnetiche presso esercenti) la chiave di cifratura NON PUO' essere tenuta segreta.

1. La chiave di cifratura deve essere resa pubblica a tutti gli utenti affinchè la utilizzino per comunicare con il suo possessoreOvviamente la chiave di decifrazione deve restare segretaIn altre parole, la conoscenza della sola chiave di codifica non deve permettere che si venga a conoscenza della chiave di decodifica (sistema crittografico ASIMMETRICO).
2. La inviolabilità del sistema crittografico non può basarsi sulla "ingegnosità" del metodo, la ipotetica scoperta del quale renderebbe violata la sicurezza di tutte le transazioni in attoOccorre istituire un metodo noto per il quale la inviolabilità della chiave di decifrazione sia basata sulla complessità algoritmica del calcolo di quest'ultima.

Comunicazione in chiave pubblica

Un sistema moderno per comunicare in modo sicuro si basa dunque sull'esistenza di due funzioni (f, f^{-1}) per cui è estremamente complicato determinare f^{-1}, conoscendo solo f.

1. B costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica solo la chiave di cifratura f (ad esempio inserendola in un elenco pubblico), e tiene invece segreta f^{-1}.
2. Se A vuole comunicare con B, trova f nell'elenco, codifica il messaggio utilizzando f e lo spedisce a B.
3. B riceve il messaggio e lo decodifica utilizzando la chiave di decifrazione f^{-1}, nota solo a lui.
   - f è detta chiave pubblica.
   - f^{-1} è detta chiave privata.

Metodo RSA (Rivest, Shamir e Adleman)

Serve dunque un metodo algoritmico per il quale la complessità computazionale che permette di calcolare f^{-1} una volta nota f sia estremamente più elevata di quella che consente di definire f.

Il sistema crittografico più noto (RSA - Ronald Rivest, Adi Shamir e Leonard Adleman - 1978) è basato sulla conoscenza di due numeri primi molto grandi p e q, tenuti segreti, dei quali viene reso pubblico solo il loro prodotto $n = pq$La chiave di cifratura pubblica sarà costituita da una opportuna "elevazione a potenza" nell'alfabeto con n-simboli (cioè $f(x) = x^e$, con e e n pubblici)La chiave di decifrazione (che è rappresentata dall' "estrazione della radice e-esima" nell'alfabeto con n-simboli) sarà facile da calcolare per chi privatamente conosce i fattori primi p e q di $n$impossibile da calcolare (tempo macchina "infinito") per chi conosce solo la chiave pubblica costituita da n ed e.

Primalità e fattorizzazione

Tutto ciò è reso possibile dal fatto che al momento attuale i migliori algoritmi noti per la determinazione dei fattori primi (p e q) di un assegnato grande numero intero $n = pq$ (dell'ordine delle 500 cifre decimali) hanno un grado di complessità computazionale immensamente più elevato di quello necessario per il calcolo di due (nuovi) grossi numeri primi p e q.
Dai teorici del settore, è stato individuato un "diaframma" che distingue ciò che può essere determinato in un "tempo finito" da un calcolatore da ciò che invece non può esserlo: la complessità polinomiale. Hanno complessità polinomiale tutti e soli i problemi decisionali che possono essere risolti da una macchina di Turing deterministica usando una quantità polinomiale di tempo di computazione.

Primalità e fattorizzazione

Nel 2002 è stato dimostrato da Agrawal, Kayal e Saxena che

il problema di verificare se un numero intero è primo

è di complessità polinomiale.

Quindi la determinazione di due grandi numeri primi p e q che forniscano $n = pq$ è un processo possibile perché richiede una quantità polinomiale di tempo di computazione.

Al contrario, ad oggi non si conosce alcun algoritmo con grado di complessità polinomiale che sia in grado, a partire da $n = pq$, di determinarne i grandi fattori primi p e q.

Primalità e fattorizzazione

Nel 1994 Peter Shor ha dimostrato che in linea di principio sarebbe possibile risolvere il problema della fattorizzazione in tempo polinomiale se si potesse disporre di un computer quantistico, attraverso il metodo della trasformata di Fourier quantistica.
Nel giugno 2013 Google e Nasa presentano il D-Wave Two, nel Quantum Artificial Intelligence Lab, in California: questo è il primo computer quantistico mai prodotto. Possiede un processore a 512 qubit, ognuno dei quali è un circuito superconduttore mantenuto a temperature bassissime (2 o 3 K, -271 Celsius). È costato circa 10 milioni di dollari. La sua reale efficienza è ancora un argomento molto controverso tra gli addetti del settore.

Il metodo più efficiente oggi noto per risolvere in modo completamente deterministico la fattorizzazione $n = pq$ di grandi numeri non è polinomiale: questo metodo è basato sulla teoria delle curve ellittiche, ed è dovuto principalmente a Pollard, Strassen e Lenstra.

Che cosa ha reso possibile la crittografia moderna?

- 1601 - 1665 in Francia, Pierre de Fermat, magistrato e matematico, fonda la teoria dei numeri: sarà uno dei primi matematici ad occuparsi di aritmetica modulare.
- 1707 - 1783 in Svizzera, Leonhard Euler, è il più importante e prolifico matematico e fisico illuminista. Nei suoi studi sulla aritmetica modulare generalizza e dimostra un risultato congetturato da Fermat, quello che oggi è noto come il teorema di Eulero-Fermat, che vedremo nel V incontro, e che è alla base del metodo crittografico RSA.
- 1978, tre ricercatori de Massachusetts Institute of Technology, Ronald Rivest, Adi Shamir e Leonard Adleman, utilizzando in modo fondamentale i risultati prettamente teorici di aritmetica modulare sviluppati 250 anni prima da Leonhard Euler, fondano il metodo crittografico a chiave asimmetrica RSA, che così diviene una formidabile applicazione di risultati di matematica pura alla crittografia attuale, vastamente impiegata in tutto il mondo.

Perché la crittografia moderna è irrinunciabile?

Dal 1980 ad oggi, la tecnologia elettronica ed informatica, ha reso possibile la realizzazione industriale di computer con una potenza di calcolo sempre crescente, inimmaginabile ai tempi di Turing.
Questa tecnologia ha rivoluzionato i tempi ed i metodi di comunicazione nel mondo, ed ha visto la nascita del web.
Contestualmente si è presentato il problema della confidenzialità e della autenticità dei dati memorizzati e di quelli in transito.
Questo è ciò che ha generato la crittografia a chiave pubblica, che entra in gioco ogniqualvolta vi è carattere di confidenzialità nei messaggi e nei file presenti su supporti di memorizzazione, nelle comunicazioni wireless (Wi-Fi e reti cellulari), in web per oscurare la comunicazione dati in transito tra client e server (protocolli SSH, SSL/TSL, HTTPS, IPsec), nelle transazioni finanziarie-bancarie (home banking), nella pay per view per impedire la visione di contenuti audiovisivi a pagamento ai non abbonati ecc...
Ed è proprio sulle attuali capacità/incapacità di calcolo dei super-computer che si fonda la sicurezza della crittografia moderna.