CRITTOGRAFIA

G. Travaglini
Dipartimento di Matematica e Applicazioni
Università di Milano Bicocca

1 Crittare e decrittare

Svetonio riporta[1] l'abitudine di Giulio Cesare ad usare per le sue corrispondenze riservate un codice di sostituzione molto semplice, nel quale ogni lettera doveva essere sostituita dalla lettera che la segue di tre posti nell'alfabeto: la lettera A era sostituita dalla D, la B dalla E e così via fino alle ultime lettere dell'alfabeto, che erano sostituite con le prime, come nella tabella seguente, riferita all'alfabeto di 26 lettere

Chiaro	A	B	C	D	E	F	G	...	T	U	V	W	X	Y	Z
Cifrato	D	E	F	G	H	I	J	...	W	X	Y	Z	A	B	C

.

Ad esempio, la frase

PROVA TU STESSO IL CIFRARIO DI CESARE

sarebbe diventata

SURYD WX VWHVVR LO FLIUDULR GL FHVDUH .

Il Cifrario di Cesare contiene già i due elementi caratteristici di un codice di cifratura: l'*algoritmo* e la *chiave*. Il primo è la regola secondo cui si

[1] Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Restano quelle [le lettere] a Cicerone, così come quelle ai familiari sugli affari domestici, nelle quali, se doveva fare delle comunicazioni segrete, le scriveva in codice, cioè con l'ordine delle lettere così disposto che nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D per A e così via per le rimanenti.

(Vita di Cesare §56)

modifica il messaggio originario (in questo caso il fatto di spostare in avanti le lettere), la seconda è il parametro che viene applicato (in questo caso è 3, cioè il numero di passi in avanti, ma poteva anche essere 4, o 11, ...). Nel caso del Cifrario di Cesare la chiave appare poco importante, poichè, una volta saputo che le lettere sono state spostate in avanti, basta qualche tentativo per stabilire di quanto, e quindi essere in grado di decifrare il messaggio. Tuttavia è bene avere subito chiara la distinzione tra algoritmo e chiave, poichè in sistemi crittografici più raffinati l'algoritmo può essere noto a tutti, mentre la sicurezza della cifratura sta nella mancata divulgazione della chiave.

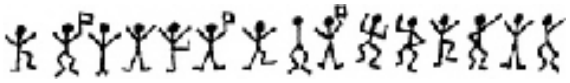
Per quanto sappiamo, il Cifrario di Cesare era per la sua epoca sufficientemente sicuro. Tuttavia non è difficile migliorarlo: se è vero che esistono pochi modi di spostare in avanti tutte le lettere di uno stesso passo, esistono però moltissimi modi di mescolarle, come ad esempio

Chiaro	A	B	C	D	E	F	G	...	T	U	V	W	X	Y	Z
Cifrato	P	A	J	T	B	V	M	...	X	N	E	H	W	Q	C

e diventa così impossibile provare tutte le chiavi. Questo nuovo modo di crittare i messaggi, apparso in India, divenne a sua volta insicuro quando la civiltà araba iniziò ad usare la statistica, e più precisamente la frequenza con cui le lettere dell'alfabeto appaiono nella lingua in cui si ritiene sia scritto il messaggio da decrittare.

Era iniziata la guerra tra i crittografi, che inventavano nuovi algoritmi, e i crittoanalisti, che dedicavano il loro ingegno alla ricerca dei punti deboli di questi algoritmi (e della loro messa in opera).

Per capire in cosa consiste il contributo dei crittoanalisti arabi riportiamo le parole di Sherlock Holmes che nel racconto *L'Avventura degli omini danzanti* è posto di fronte al mistero costituito da alcuni disegni apparentemente infantili, come il seguente,



che l'investigatore immediatamente riconosce come messaggi cifrati, in cui ogni omino rappresenta una lettera dell'alfabeto. Spiega quindi al Dr. Watson che il messaggio precedente *"era talmente breve che non ho potuto fare altro che decidere, con una certa sicurezza, che il simbolo*

indicava la lettera E. *Come sapete,* E *è la lettera più usata dell'alfabeto inglese, a un punto tale che si è quasi certi di trovarla ripetuta spesso anche*

in una frase breve. Dei quindici simboli nel primo messaggio, quattro erano uguali, quindi era regionevole pensare che stessero per la lettera E. *E' vero che in alcuni casi il pupazzetto aveva una bandierina e in altri no ma,dal modo in cui queste bandierine erano distribuite, appariva probabile che indicassero lo stacco tra una parola e l'altra della frase. Partendo da questa ipotesi, notai che la lettera* E *era simboleggiata da*  . *Ora però arrivava il difficile. L'ordine di frequenza delle lettere inglesi, dopo quello della* E*, non è molto marcato ... la frequenza delle lettere* T, A, O ed I *è molto ravvicinata e ci vorrebbe un'eternità a provare tutte le combinazioni per arrivare a un qualche risultato. Aspettai quindi di avere altro materiale a disposizione."*

L'analisi di Holmes prosegue coniugando statistica e linguistica, utilizzando l'apparente struttura delle frasi e il contesto dell'indagine. Questo richiede pazienza e molto tempo, troppo per evitare il tragico finale della storia.

Chi desidera mettersi alla prova può cercare di decifrare il seguente messaggio, liberamente tratto dalla pagina economica di un quotidiano italiano. Ad ogni lettera dell'alfabeto italiano è stata sostituita una lettera greca:

$$\lambda\epsilon \quad \chi\psi\omega\varphi\gamma\pi\psi\eta\kappa \quad \mu\kappa\epsilon \quad \alpha\psi\theta\mu\psi \quad \mu\lambda \quad \lambda\theta\pi\kappa\xi\varphi\lambda\tau\kappa\theta\varphi\psi \quad \xi\psi\xi\varphi\lambda\kappa\theta\kappa$$
$$\mu\lambda \quad \gamma\pi\kappa\omega\kappa \quad \alpha\gamma\varphi\varphi\psi \quad \epsilon\kappa \quad \theta\kappa\eta\kappa\xi\xi\gamma\omega\lambda\kappa \quad \gamma\theta\gamma\epsilon\lambda\xi\lambda \quad \kappa \quad \mu\lambda \quad \gamma\pi\kappa\omega\kappa$$
$$\eta\psi\theta\eta\epsilon\zeta\xi\psi \quad \eta\rho\kappa \quad \epsilon\kappa \quad \gamma\sigma\lambda\psi\theta\lambda \quad \mu\lambda \quad \zeta\theta\gamma \quad \lambda\tau\chi\psi\omega\varphi\gamma\theta\varphi\kappa \quad \eta\psi\tau\chi\gamma\beta\theta\lambda\gamma$$
$$\lambda\varphi\gamma\epsilon\lambda\gamma\theta\gamma \quad \xi\psi\theta\psi \quad \zeta\theta \quad \varepsilon\zeta\psi\theta \quad \gamma\eta\delta\zeta\lambda\xi\varphi\psi$$

Per la frequenza delle lettere nella lingua italiana riportiamo quella ricavata dai primi 15 capitoli dei *Promessi Sposi:*

$$A = 11,1\%, \quad B = 1\%, \quad C = 4,8\%, \quad D = 3,7\%, \quad E = 11,9\%,$$
$$F = 1.1\%, \quad G = 1,8\%, \quad H = 1,3\%, \quad I = 9,7\%, \quad L = 5,5\%,$$
$$M = 2,4\%, \quad N = 7,3\%, \quad O = 10\%, \quad P = 2,9\%, \quad Q = 0,7\%,$$
$$R = 6,6\%, \quad S = 5,4\%, \quad T = 6,1\%, \quad U = 3,5\%, \quad V = 2,2\%,$$
$$Z = 0,8\% \ .$$

L'analisi delle frequenze, nata in Arabia, aveva definitivamente messo in crisi le cifrature basate sulla semplice sostituzione di ogni lettera dell'alfabeto con un'altra lettera o simbolo. Questo fatto determinò la creazione di cifrature più complesse, come la *Gran Cifra*, basata sulla sostituzione sia di lettere singole sia di sillabe e usata da Luigi XIV per la sua corrispondenza riservata, rimasta; nonostante il grande interesse degli storici, un mistero fino al termine del XIX secolo.

L'evoluzione della crittografia era destinata a subire una brusca accelerazione nel XX secolo, soprattutto perchè stava cambiando la *trasmissione dell'informazione*. La radio e gli altri sistemi di comunicazione rendevano estremamente semplice trasmettere i messaggi. E spesso anche intercettarli. Nell'Agosto del 1914 i russi subirono a Tannenberg la sconfitta decisiva per le sorti del fronte russo-tedesco anche perchè non disponevano di un servizio crittografico: i messaggi russi viaggiavano attraverso la radio "in chiaro"! La cifratura dei messaggi riservati era dunque diventata assolutamente necessaria, ma gli strumenti a disposizione erano vecchi algoritmi non proporzionati all'importanza che il problema stava assumendo. Sempre nella prima guerra mondiale, fu clamorosa la decifrazione, ad opera del servizio segreto inglese, del telegramma in cui il ministro degli esteri tedesco Zimmermann proponeva al Messico una alleanza contro gli Stati Uniti, nel caso di una loro entrata in guerra. L'effetto di questa rivelazione fu enorme e convinse gli Stati Uniti ad entrare nel conflitto, in tempo per influire sul corso della storia.

I tedeschi, che all'inizio della prima guerra mondiale erano privi di un servizio crittoanalitico militare, erano invece destinati a creare nell'immediato dopoguerra la più famosa cifratrice della storia: *Enigma.* Si trattava di un apparecchio elettromeccanico, all'apparenza simile ad una grossa macchina da scrivere. Mentre si batteva un messaggio, la regola di sostituzione delle lettere cambiava continuamente in base a parametri iniziali scelti tra decine di migliaia possibili. Un'altra macchina Enigma e la conoscenza dell'assetto iniziale permettevano poi di decrittare automaticamente il messaggio cifrato. L'esistenza di Enigma era ben nota, e anche la sua struttura, ma la macchina era considerata dai francesi e dagli inglesi inviolabile. Furono i polacchi, forse resi più previdenti dalla loro storia, ad attaccare Enigma con maggiore convinzione. Nel fare questo introdussero una svolta fondamentale nella storia della crittografia: l'utilizzo di significativi strumenti matematici. Nel suo libro *Codici & Segreti* Simon Singh descrive così questo passaggio. *"Per secoli si era partiti dal presupposto che le persone più adatte a volgere in chiaro una scrittura segreta fossero i conoscitori del linguaggio e delle sue leggi - i linguisti e gli umanisti; ma il nuovo sistema tedesco di protezione delle comunicazioni spinse i polacchi ad adottare un'altra strategia di reclutamento ... organizzarono un corso di crittografia al quale invitarono venti matematici dell'Università di Poznan ... Il più brillante era Marian Rejewski ... Cercò di tradurre in termini numerici ogni aspetto del funzionamento della macchina, ... come sempre in matematica, il suo lavoro richiedeva ispirazione oltre che logica."* Rejewski riusci ad entrare nel segreto di Enigma, ma si arrese di fronte ad una nuova più complessa versione, usata dai tedeschi a partire dal 1938. Il successo parziale dei polacchi fu però fondamentale per

gli inglesi che allo scoppio della guerra si trovarono di fronte alle nuove versioni di Enigma, continuamente migliorate dai tedeschi lungo tutto l'arco del conflitto. Il centro di crittoanalisi inglese, che arrivò a contare 7000 operatori, riuscì nell'impresa grazie al genio di Alan Turing, uno dei più celebri matematici del XX secolo, che seguendo l'esperienza dei polacchi fu in grado di spezzare il procedimento logico di Enigma in problemi più semplici, creare un'opportuna macchina elettromeccanica e individuare alcune debolezze di Enigma e degli operatori che la utilizzavano. Già all'inizio del 1940 gli inglesi erano in grado di decrittare i messaggi prodotti da Enigma, con decisive conseguenze per lo sviluppo della guerra.

Enigma

Alan Turing

Le macchine elettromeccaniche avevano così soppiantato la carta e la penna nelle mani dei crittografi e dei crittoanalisti, ma nella seconda metà del secolo avrebbero a loro volta ceduto il passo ai computer, che per la velocità e la possibilità di programmare sono particolarmente adatti ai problemi della crittografia. All'introduzione degli elaboratori elettronici si accompagnò un fondamentale passo in avanti: l'eliminazione della necessità di trasmettere la chiave.

In molti casi questo era un punto debole delle cifrature e diventava particolarmente grave con l'aumentare dei destinatari. La novità consiste nell'uso di due chiavi, una *chiave pubblica*, che tutti conoscono e con cui chiunque può inviare un messaggio cifrato, e una *chiave privata*, che solo il destinatario conosce e che è indispensabile per decifrare. Questo significa che è facile passare dal testo chiaro a quello cifrato, ma che non si è in grado di passare da

un testo cifrato a uno chiaro. Viene così a cadere una delle caratteristiche dei tradizionali sistemi di cifratura, la *simmetria*. Cifrare e decifrare non sono più la stessa cosa. In realtà i sistemi simmetrici continuano ad essere usati quando la trasmissione della chiave non è un problema, dato che, a parità di sicurezza, possono richiedere chiavi molto più corte rispetto ad un sistema a chiave pubblica. Si può ad esempio utilizzare un sistema a chiave pubblica per trasmettere la chiave di un sistema simmetrico, attraverso il quale trasmettere poi il messaggio vero e proprio.

Il più famoso e il più usato dei sistemi a chiave pubblica è stato proposto nel 1978 da tre ricercatori del M.I.T., R. Rivest, A. Shamir e L. Adleman e prende dalle loro iniziali il nome di sistema RSA. La sicurezza dei segreti militari, industriali o bancari (come i pagamenti attraverso carte di credito) si basa oggi su sistemi come questo.

Rivest, Shamir e Adleman

Ovviamente l'introduzione del metodo RSA non fu solo un fatto accademico. Diventando una scienza, la crittografia non poneva più di fronte i governi e alcuni geniali inventori isolati, ma le agenzie governative (come la NSA - National Security Agency) e le università; due mondi non pregiudizialmente ostili, ma abituati a seguire regole diverse. La divulgazione dei risultati della ricerca poteva rientrare nella legislazione sull'esportazione delle armi e ci furono pressioni perchè questi non fossero resi pubblici. Negli anni successivi le relazioni tra la NSA e la comunità dei crittografi migliorarono e divenne chiara la distinzione tra la *ricerca crittografica*, che, in quanto opera dell'ingegno, poteva diventare di pubblico dominio, e i *prodotti crittografici*, cioè software e hardware, che non potevano essere distribuiti indiscriminatamente ed erano soggetti ai controlli sull'esportazione.

2 Il sistema RSA

Per leggere questo capitolo occorre munirsi di carta e matita. La fatica sarà però ricompensata, perchè la matematica del sistema RSA sta in poco più di una pagina, e non è frequente poter comprendere così facilmente una delle numerose spettacolari applicazioni moderne della matematica.

Siano a e b due numeri interi (positivi, nulli o negativi) e sia s un intero positivo. Diciamo che a è congruo a b modulo s, e scriviamo

$$a \equiv b \pmod{s}$$

se s divide la differenza $a - b$. Ad esempio

$3 \equiv 59 \pmod{7}$	poichè $3 - 59 = (-8) \times 7$
$17 \equiv 1 \pmod{8}$	poichè $17 - 1 = 2 \times 8$
$5 \equiv -7 \pmod{3}$	poichè $5 - (-7) = 4 \times 3$.
$51 \equiv 0 \pmod{17}$	poichè $51 - 0 = 3 \times 17$
33 non è congruo a 7 $\pmod{5}$	poichè $33 - 7$ non è un multiplo di 5

In altre parole, $a \equiv b \pmod{s}$ significa che dividendo a e b per s otteniamo lo stesso resto (che per sua definizione è compreso tra 0 e $s - 1$).

Nel sistema RSA si scelgono due numeri primi p e q (un numero primo è un intero maggiore di 1, divisibile solo per se stesso e per 1) grandi (rispetto alle capacità di calcolo) e distinti. Si considera quindi il loro prodotto $n = pq$. Sia

$$\phi(n) = (p-1)\,(q-1) \ . \tag{1}$$

Scegliamo poi un numero h che non abbia divisori comuni con $\phi(n)$. Un teorema sulle congruenze ci dice che esiste allora un numero d tale che

$$dh \equiv 1 \pmod{\phi(n)} \ ,$$

cioè che esiste un intero ℓ tale che

$$dh = 1 + \ell\phi(n) \ . \tag{2}$$

Ora prendiamo il messaggio da cifrare e scriviamolo in modo ovvio come un grosso numero, ad esempio ponendo $A = 01$, $B = 02$, $C = 03$, etc.. I cento numeri da 00 a 99 sono in genere sufficienti per rappresentare lettere, numeri e simboli (l'alfabeto Braille classico funziona abbastanza bene con solo 64 simboli). Spezziamo il grosso numero in blocchi di uguale lunghezza, in modo che ciascun blocco sia un numero inferiore ad n. Sia P uno di questi

blocchi, dunque $0 \leq P < n$. Sostituiamo P con il numero "cifrato" C definito da

$$\begin{cases} C \equiv P^h \pmod{n} \\ 0 \leq C < n \end{cases} ,$$

cioè C è il resto della divisione di P^h per n. Mostriamo che per riottenere P da C basta calcolare C^d. Cioè mostriamo che

$$C^d \equiv P \pmod{n} . \tag{3}$$

Infatti $C^d \equiv \left(P^h\right)^d \pmod{n}$ e, per (1) e (2),

$$\left(P^h\right)^d = P^{hd} = P^{1+\ell(p-1)(q-1)}$$

Supponiamo ora per semplicità che p non divida P, allora esiste un importante teorema, noto come Piccolo Teorema di Fermat, che assicura che $P^{p-1} \equiv 1 \pmod{p}$ e quindi

$$C^d \equiv P \left(P^{p-1}\right)^{\ell(q-1)} \equiv P \pmod{p} ,$$

Poichè p e q entrano in modo simmetrico nel nostro problema abbiamo anche $C^d \equiv P \pmod{q}$ e allora, essendo p e q primi distinti, $C^d - P$ è un multiplo di $pq = n$ e dunque (3) è dimostrata.

Possiamo ora comunicare a qualsiasi persona i numeri h ed n, conoscendo i quali chiunque può scriverci un messaggio. Solo noi, però, siamo in grado di decifrare, perchè, per farlo, usiamo d e per calcolare d dobbiamo conoscere $\phi(n) = (p-1)(q-1)$. Conoscere $\phi(n)$ è "equivalente" a conoscere p e q: in un senso è ovvio, nell'altro senso osserviamo che, supponendo $p > q$, (1) implica

$$\begin{aligned} p + q &= n + 1 - \phi(n) \\ p - q &= \sqrt{(p+q)^2 - 4pq} = \sqrt{(n+1-\phi(n))^2 - 4n} . \end{aligned}$$

In poche parole, conoscere $\phi(n)$ (e quindi d) richiede la stessa fatica che conoscere p e q, cioè fattorizzare n, e questo, se n è grande, può richiedere un tempo di calcolo troppo lungo. Per comprendere la grandezza dei numeri coinvolti è interessante visitare la pagina

http://www.rsasecurity.com/rsalabs/challenges/factoring/

dove la società RSASecurity, fondata dagli inventori del metodo RSA, oggi (maggio 2004) offre da \$20.000 a \$200.000 per scomporre numeri di varia grandezza che sono prodotto di due numeri primi. Non è ovviamente una iniziativa promozionale, ma un aspetto vitale della secolare competizione tra crittografi e crittoanalisti.

Ora applichiamo il sistema RSA in un esempio.

Consideriamo le lettere dell'alfabeto (nell'esempio che segue, a parte lo "spazio", non ci servono altri simboli) e associamo a ciascuna di esse un numero di due cifre:

$$A = 01,\ B = 02,\ C = 03,\ D = 04,\ E = 05,\ F = 06,\ G = 07,\ H = 08,$$
$$I = 09,\ J = 10,\ K = 11,\ L = 12,\ M = 13,\ N = 14,\ O = 15,\ P = 16,$$
$$Q = 17,\ R = 18,\ S = 19,\ T = 20,\ U = 21,\ V = 22,\ W = 23,\ X = 24,$$
$$Y = 25,\ Z = 26,\ \text{spazio} = 00.$$

Consideriamo la frase

$$\text{UN TEMPO TROPPO LUNGO} \tag{4}$$

che così diventa

$$21140020051316150020181516161500122114 0715$$

Fissiamo ora $n = 2867 = 47 \times 61$ (47 e 61 sono numeri primi) e separiamo la sequenza precedente in blocchi di un numero pari di cifre (per non spezzare le lettere) in modo che ciascun blocco sia costituito da un numero inferiore a 2867 (poichè nessun blocco di due cifre supera 26, ogni blocco di 4 cifre è un numero inferiore a 2867). Scriviamo

$$\begin{array}{cccccccccccc} 2114 & 0020 & 0513 & 1615 & 0020 & 1815 & 1616 & 1500 & 1221 & 1407 & 1500 \\ P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 & P_9 & P_{10} & P_{11} \end{array} \tag{5}$$

(abbiamo aggiunto 2 zeri in fondo in modo da avere blocchi di 4 cifre). Poichè $n = 47 \times 61$ (con 47 e 61 numeri primi) abbiamo

$$\phi\,(2867) = 46 \times 60 = 2760\ .$$

Poichè $2760 = 2^3 \times 3 \times 5 \times 23$, il numero $h = 7$ non ha divisori comuni con 2760. Trasformiamo ora ciascun P_j tra gli 11 blocchi in (5) nel numero $C_j \equiv P_j^h \pmod{2867}$, con $0 \leq C_j < 2867$. Otteniamo così

$$P_1^h = 2114^7 \equiv 1973 \pmod{2867}\ ,$$
$$\vdots$$
$$P_{11}^h = 1500^7 \equiv 1147 \pmod{2867}\ .$$

Quindi il messaggio cifrato è

$$1973 \quad \cdots \quad 1147\,. \tag{6}$$

Ricordiamo che tutti conoscono $n = 2867$ e $h = 7$, ma per ricostruire (5) (e quindi (4)) partendo da (6) occorre conoscere d, che è definito da $dh \equiv 1 \pmod{\phi(n)}$, cioè da

$$7d \equiv 1 \pmod{2760}$$

(ricordiamo che $\phi(n) = \phi(2867) = 2760$ non è noto ad estranei, poichè proviene dalla scomposizione di $n = 2867$, che per n opportunamente grande è apparentemente impossibile da determinare in tempi ragionevoli). Noi però conosciamo $\phi(n)$ e quindi possiamo calcolare $d = 1183$. A questo punto possiamo ricostruire il messaggio iniziale:

$$\begin{aligned} 1973^{1183} &\equiv 2114 \pmod{2867}\ , \\ &\vdots \\ 1147^{1183} &\equiv 1500 \pmod{2867}\ . \end{aligned}$$