LA CRITTOGRAFIA DA SPARTA AL BANCOMAT

di Emanuele Bottazzi

COS'È LA CRITTOGRAFIA?

Cara lettrice, caro lettore, ti presento Alice e Bob. Alice e Bob hanno diversi problemi. Innanzitutto desiderano comunicare, ma non si possono vedere di persona. Di conseguenza sono costretti a scambiarsi messaggi con dei mezzi che non sono sicuri, come le e-mail. Inoltre Alice e Bob temono che la loro nemica giurata, Eva, intercetti la loro corrispondenza per leggerla di nascosto. Di fronte a queste dicoltà, Alice e Bob non si sono lasciati scoraggiare, ma hanno ideato diversi metodi per poter comunicare in modo che nessuno riesca a capirli. In altre parole, hanno inventato la crittografia.

LA CRITTOGRAFIA ANTICA

La scitala. Secondo Plutarco, i primi Alice e Bob della storia dell'Occidente sono stati i generali spartani. La loro tecnica per inviare messaggi segreti si chiama scitala, ed è descritta nella *Vita di Lisandro*.

Prima di partire per una campagna militare, il generale spartano Alice prendeva un bastone di legno di diametro costante e lo tagliava a metà. Una delle due parti rimaneva a Sparta, nelle mani del magistrato Bob, mentre l'altra metà veniva custodita da Alice. Per comunicare con la madrepatria, il generale arrotolava una sottile striscia di stoffa al bastone, dopo di che la fissava alle estremità e scriveva il messaggio in verticale, senza indicare la punteggiatura né gli spazi tra le parole. In questo modo, quando la striscia veniva srotolata, le lettere del testo originale si trovavano tutte mescolate tra loro.

Figura **1** – L'inizio di un messaggio in lingua inglese cifrato con la scitala

La striscia di stoffa veniva poi affidata a uno schiavo, che se ne cingeva i fianchi come se fosse stata una cintura e partiva alla volta della madrepatria. Qui, Bob poteva arrotolare la striscia attorno al bastone dello stesso diametro di quello utilizzato da Alice, in modo da decifrare il messaggio.

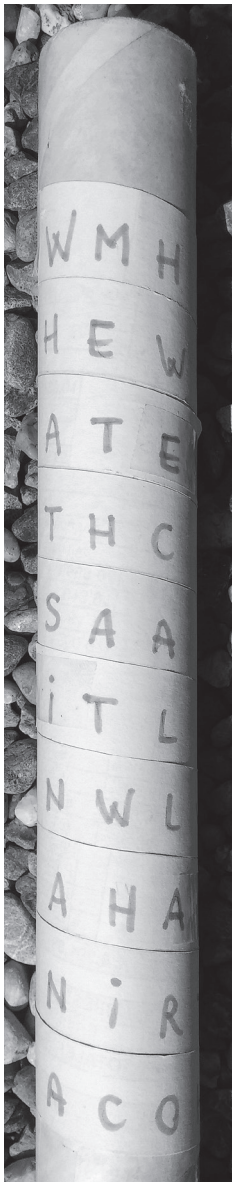


Figura **2** – Un famoso passo di Shakespeare decifrato

Cosa sarebbe successo se lo schiavo fosse stato catturato da Eva, nemica di Sparta? Innanzitutto Eva avrebbe dovuto scoprire che il testo era nascosto nella cintura del prigioniero. Questa tecnica che prevede di nascondere il messaggio non fa parte della crittografia propriamente detta, bensì della steganografia, l'arte di occultare i messaggi. Se anche Eva avesse scoperto la finta cintura con la missiva del generale, si sarebbe trovata di fronte a un'accozzaglia di lettere senza significato. Per ricostruire il testo originale avrebbe dovuto innanzitutto scoprire che era stato cifrato con il metodo della scitala, ma anche questa informazione non le sarebbe bastata. Infatti il messaggio sarebbe rimasto illeggibile finche Eva non avesse scoperto il diametro del bastone di Alice.

Per quanto primitiva, la scitala è la prima forma di crittografia della nostra storia. Il suo studio ci può aiutare a identificare gli elementi fondamentali di un cifrario. Innanzitutto c'è il messaggio che Alice vuole trasmettere a Bob. In secondo luogo c'è la tecnica di cifratura, che nel caso della scitala consiste nello scrivere il testo in verticale sulla striscia di stoffa arrotolata al bastone. Infine in ogni cifrario c'è sempre un segreto, che in questo caso è il diametro del bastone.

A questo punto sorge spontanea una domanda: per decifrare la scitala Eva deve davvero arrotolare la striscia di stoffa che contiene il messaggio su tanti bastoni di diametri diversi finché non trova quello con il diametro giusto? In realtà, Eva può anche ragionare così: due lettere consecutive del testo originale si trovano sempre alla stessa distanza anche nel testo cifrato. Grazie a questa idea, Eva può decifrare la scitala senza utilizzare i bastoni!

Il cifrario di Giulio Cesare. Anche nell'antica Roma non mancano Alice, Bob ed Eva. Una delle Alice più famose è Giulio Cesare. Questo imperatore ha ideato uno dei cifrari più longevi della storia, che ancora oggi è ricordato con il suo nome. Il cifrario di Giulio Cesare consiste nel sostituire ciascuna lettera del messaggio con quella che lo segue di un numero fissato di posizioni.

Vediamo insieme un esempio: supponiamo che Alice voglia sostituire ogni lettera con quella otto posti più avanti nell'alfabeto. Se desidera trasmettere il messaggio «Alan Turing», effettua le seguenti trasposizioni:

A	*L*	*A*	*N*	*T*	*U*	*R*	*I*	*N*	*G*
$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$	$\downarrow +8$
I	*T*	*I*	*V*	*B*	*C*	*Z*	*Q*	*V*	*O*

Il testo cifrato sarà dunque «Itiv Bczqvo». Per decifrarlo, Bob sostituirà a ogni lettera quella che la precede di otto posizioni nell'alfabeto. Il segreto che garantisce la sicurezza del cifrario di Giulio Cesare è il numero di posizioni delle quali ciascuna lettera viene spostata.

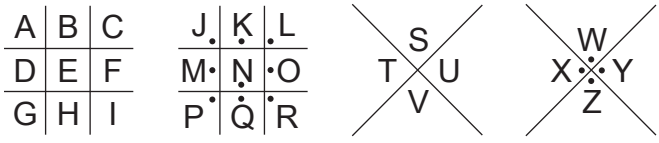
Il cifrario di Giulio Cesare non è molto sicuro: Eva lo può decifrare anche a mano. Non è nemmeno necessario effettuare tutte le trasposizioni possibili: si possono sfruttare le caratteristiche della lingua nella quale Alice e Bob comunicano. Per esempio, nella lingua italiana la lettera «e» è la lettera più frequente. Di conseguenza, se il messaggio cifrato è lungo a sufficienza, uno dei primi tentativi di Eva è quello di provare con lo spostamento che manda la lettera «e» nella lettera che nel testo cifrato compare più spesso. Altri suggerimenti per decifrare il cifrario di Giulio Cesare si possono trovare in Rete.

Provate a mettervi nei panni di Eva: avete intercettato il messaggio seguente e desiderate decifrarlo.

Le tzwirizf jlttvjjzmf r hlvccf uz Xzlczf Tvjriv v zc tzwirizf uz Mzxveviv. Hlvjkf tzwirizf v jkrkf r clexf izkvelkf zerkkrttrszcv, dr ze ivrckr jfwwiv uvccv jkvjjv uvsfcvqqv uvc tzwirizf uz Xzlczf Tvjriv.

Per verificare se avete decifrato correttamente il messaggio, potete usare gli strumenti disponibili alla pagina **https://www.dcode.fr/caesar-cipher**.

Pigpen: il cifrario degli alieni. Una variante del cifrario di Giulio Cesare è il cifrario pigpen. In questo caso, Alice sostituisce ogni lettera dell'alfabeto secondo lo schema seguente.



I messaggi cifrati in questo modo sembrano quasi scritti dagli alieni, ma si possono decifrare con tecniche simili a quelle usate per il cifrario di Giulio Cesare.

LA CRITTOGRAFIA MODERNA

Fino alla seconda guerra mondiale gli Alice e Bob della storia sono stati condottieri, generali, monarchi e rivoluzionari. Chi sono invece gli Alice e Bob della nostra societa? Sei tu, cara lettrice, quando prelevi dal bancomat del tuo quartiere. Sei tu, caro lettore, quando accedi all'area riservata di un sito internet utilizzando una password. E siamo tutti noi quando comunichiamo con le ultime app di messaggistica. Il pin del bancomat e le password per accedere ai servizi online sono le chiavi d'accesso ai nostri risparmi e ai nostri documenti personali: neanche uno di essi deve cadere nelle mani di Eva!

Questi esempi ci mostrano che la crittografia moderna svolge due ruoli. Il primo è analogo a quello della crittografia antica: permette ad Alice e Bob di comunicare senza che Eva possa leggere i loro messaggi. Le tecniche di cifratura che si usano in questi casi sono molto lontane dal cifrario di Giulio Cesare o dalle sue varianti: non si basano più sulla sostituzione delle lettere secondo algoritmi stabiliti, bensì sull'esistenza di particolari funzioni matematiche che sono facili da calcolare solo se si è in possesso della chiave segreta. Un esempio di cifrario basato su questa idea è il protocollo RSA, descritto nel numero di giugno di Archimede.

Il secondo ruolo della crittografia moderna è di garantire ad Alice che il suo interlocutore sia effettivamente Bob, e non la sua nemica Eva. L'identificazione tra Alice e Bob avviene per esempio tutte le volte che usiamo il bancomat o ci connettiamo all'area riservata di un sito internet. Di conseguenza, è fondamentale che il sito non tenga una copia della nostra password sui suoi server: in caso contrario, Eva potrebbe rubarla. Purtroppo questa semplice misura di sicurezza non è sempre verificata, e periodicamente si sente dare la notizia di siti ai quali sono state sottratte migliaia di password.

Quindi la banca Alice chiede a Bob di identificarsi mediante il suo codice segreto per autorizzarlo alle operazioni, ma allo stesso tempo non può conoscere il suo pin. Com'è possibile soddisfare queste richieste che a prima vista possono sembrare in contraddizione?

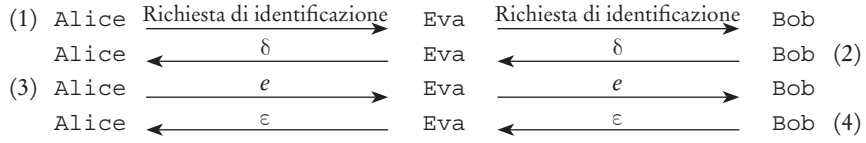
Un semplice protocollo di identificazione a conoscenza zero. Vediamo un esempio di protocollo che permette ad Alice di identificare Bob senza che lui sveli il suo segreto. Per semplicità non lavoriamo con l'aritmetica modulare, ma con le costruzioni geometriche con riga e compasso. Nel 1837 Pierre-Laurent Wantzel ha dimostrato che con questi due strumenti non è possibile dividere in tre parti un angolo qualsiasi. Invece è noto sin dall'antichita che un angolo può essere triplicato senza difficoltà.

Vediamo ora come Alice può identificare Bob utilizzando la trisezione dell'angolo. Per prima cosa, Bob costruisce un angolo arbitrario α e lo tiene segreto. Rende invece pubblicamente disponibile l'angolo $\beta = 3\alpha$. Quando Alice chiede a Bob di identificarsi, lui costruisce un nuovo angolo arbitrario γ e invia ad Alice il suo triplo $\delta = 3\gamma$. Dopo aver ricevuto δ, Alice determina un numero $e \in \{0, 1\}$ a caso, per esempio lanciando una moneta, e lo comunica a Bob. Bob risponde inviando l'angolo $\varepsilon = \gamma + e\alpha$. A questo punto, Alice verifica se vale l'uguaglianza $\delta + e\beta = 3\varepsilon$. Questa procedura viene ripetuta un numero di volte t a scelta di Alice.

Come mai questo protocollo è sicuro? Eva conosce solamente l'angolo β, e a partire da esso non può costruire con riga e compasso l'angolo $\alpha = \frac{\beta}{3}$. Se provasse comunque a impersonare Bob, si troverebbe in difficoltà ogni volta che Alice le comunica il numero $e = 1$: infatti in questi casi Eva non sarebbe in grado di costruire l'angolo $\gamma + \alpha$. Di conseguenza, la probabilità che riesca a superare le t prove che le impone Alice è pari a $\frac{1}{2^t}$. Anche se quest'ultima scegliesse valori bassi di t, come $t = 8$ o $t = 10$, Eva avrebbe scarsissima probabilità di riuscire a spacciarsi per Bob.

I protocolli di identificazione della crittografia moderna si basano sullo stesso schema, ma al posto della trisezione dell'angolo utilizzano funzioni dell'aritmetica modulare facili da calcolare e difficili da invertire. Una di queste funzioni è l'elevamento al quadrato modulo un prodotto di primi, sul quale si basa il protocollo di identificazione Fiat-Shamir. Per una discussione più approfondita, corredata di esempi e dimostrazioni, la lettrice e il lettore interessati possono consultare l'articolo [1], liberamente disponibile in Rete.

Un possibile attacco. In realtà, se Alice e Bob non sono attenti, Eva ha una possibilità di ingannare entrambi: vediamo insieme come può fare. Innanzitutto, il suo attacco deve avvenire in un momento in cui Alice sta cercando di identificare Bob con un protocollo come quello descritto al paragrafo precedente. La prima cosa che Eva deve fare è intercettare il messaggio di Alice: una volta che lo ha ottenuto, lo inoltra a Bob senza modificarlo in alcun modo. Bob, che è ancora convinto di comunicare con Alice, riceve una richiesta di identificazione alla quale fornisce la risposta δ secondo la procedura concordata. Però ricordiamo che Bob non sta davvero rispondendo ad Alice, bensì a Eva! A questo punto, lei può inoltrare ad Alice il messaggio δ. Alice, avendo ricevuto la risposta che si aspetterebbe da Bob, fornisce a Eva il numero e, che lei prontamente gira a Bob. Quando quest'ultimo le risponde con il messaggio finale ε, Eva non fa altro che ripetere il messaggio ad Alice, che ora è convinta di parlare con Bob. Forse questa procedura si descrive meglio mediante uno schema.



Una volta autenticata, Eva può chiedere ad Alice tutte le risorse che dovrebbero essere a disposizione solo di Bob. Siccome per portare a termine questo attacco Eva deve frapporsi tra Bob e Alice, la procedura si chiama «man-in-the-middle», cioè letteralmente «uomo nel mezzo».

A prima vista, può sembrare che non ci si possa difendere da un simile attacco. In realtà, c'è almeno un accorgimento che Alice e Bob possono adottare per mettersi al riparo da Eva: entrambi dovrebbero controllare i tempi di risposta del proprio interlocutore. Se una comunicazione risultasse più lenta rispetto a quelle usuali, i due farebbero meglio a ricominciare la procedura di identificazione da capo.

Intorno al 2012 un team di informatici italiani ha scoperto che il servizio di gestione delle password di Google era suscettibile di un attacco man-in-the-middle. Grazie a un'analisi matematica della vulnerabilità, i ricercatori non hanno solamente identificato la debolezza del protocollo, ma hanno anche avanzato delle proposte concrete che hanno permesso al colosso americano di rendere sicura la sua gestione delle password.

Nella sezione precedente abbiamo visto il livello di sicurezza raggiunto oggi da `Alice` e `Bob`: le loro comunicazioni sono difficili da decifrare in tempi brevi e i loro protocolli di autenticazione danno molto filo da torcere a `Eva`. E pensare che hanno ottenuto questi risultati senza mai trovarsi faccia a faccia! Sorge spontanea la domanda: di cosa sarebbero capaci se potessero incontrarsi anche solo per un breve istante? Riuscirebbero finalmente ad associare un volto a tutti quei messaggi che si sono scambiati nel corso della storia, ma questo non darebbe loro alcun vantaggio nella lotta contro `Eva`. Invece, potrebbero scambiarsi delle informazioni: un'occasione d'oro per concordare una chiave segreta!

Quale può essere la miglior chiave segreta che `Alice` e `Bob` possono ideare? La risposta sorprendente è che per costruire un cifrario inattaccabile è sufficiente un lungo elenco di numeri, che per semplicità assumiamo tutti compresi tra `0` e 25, sorteggiati rigorosamente a caso. Condividendo questa informazione, `Alice` e `Bob` potrebbero scambiarsi messaggi senza timore che `Eva` possa svelarne il contenuto. Il procedimento è analogo a quello del cifrario di Giulio Cesare: supponiamo che l'elenco di numeri inizi con

$$20 \quad 25 \quad 19 \quad 17 \quad 12 \quad 25 \quad 3 \quad 3 \quad 25 \quad 4 \quad 10 \quad 9 \quad \ldots$$

e che `Alice` desideri comunicare a `Bob` il messaggio «One time pad»: la procedura di cifratura consisterà nello spostare la lettera alla posizione n del messaggio di un numero di posizioni indicato dall'n-esimo numero dell'elenco:

O	*N*	*E*	*T*	*I*	*M*	*E*	*P*	*A*	*D*
$\downarrow +20$	$\downarrow +25$	$\downarrow +19$	$\downarrow +17$	$\downarrow +12$	$\downarrow +25$	$\downarrow +3$	$\downarrow +3$	$\downarrow +25$	$\downarrow +4$
J	*M*	*X*	*L*	*U*	*L*	*H*	*S*	*Z*	*H*

Per la decifrazione, `Bob` sostituirà alla lettera n-esima quella che la precede di un numero di posizioni pari all'n-esimo numero.

Qual è l'unica caratteristica che distingue questo cifrario da quello di Giulio Cesare? Non certo i messaggi o la procedura per trasformarli: di conseguenza, la differenza è tutta nella chiave segreta, che nel cifrario antico è un solo numero, mentre per questa variante è un elenco di numeri casuali. Queste differenze possono sembrare minuscole, ma sono due delle tre condizioni che garantiscono la massima sicurezza possibile del protocollo di cifratura. La terza è che nessun pezzo della chiave, cioè della sequenza di numeri, venga utilizzata per cifrare più di un messaggio. Questa richiesta è così importante da dare il nome al cifrario, che viene chiamato «one time pad», cioè «blocco monouso». Ogni volta che queste condizioni sono soddisfatte, se anche `Eva` riuscisse a intercettare una comunicazione, non saprebbe che farsene: siccome la chiave segreta è stata generata con una procedura casuale e non si ripete mai, non esiste alcun modo per ottenere nemmeno un minimo di informazione dal messaggio cifrato.

Al contrario, se Eva intercettasse due messaggi cifrati con la stessa sequenza di numeri, potrebbe ottenere con facilità la somma dei due messaggi originali. Vediamolo con un esempio: cifriamo «Dotish idea» con la stessa porzione di chiave usata in precedenza

D	*O*	*T*	*I*	*S*	*H*	*I*	*D*	*E*	*A*
↓ +20	↓ +25	↓ +19	↓ +17	↓ +12	↓ +25	↓ +3	↓ +3	↓ +25	↓ +4
X	*N*	*N*	*Z*	*F*	*G*	*L*	*G*	*D*	*E*

Mettiamoci ora nei panni di Eva che ha intercettato i due messaggi. Iniziamo a chiamare con x_1 la prima lettera, a noi sconosciuta, del primo messaggio originale; con y_1 la prima lettera, sconosciuta, del secondo messaggio originale; e con k_1 il primo numero, anch'esso sconosciuto, della chiave. Le uniche informazioni che abbiamo sono $x_1 + k_1 = J$ e $y_1 + k_1 = X$, che prese singolarmente non ci aiutano a decifrare i messaggi. Se però sottraiamo entrambe le equazioni membro a membro, otteniamo $x_1 - y_1 = J - X = M$. Nell'ultimo passaggio abbiamo spostato la lettera J di tre posizioni in avanti, cioè l'inverso della trasformazione che manda la lettera A nella lettera X. Procedendo in modo analogo, possiamo ottenere le differenze $x_i - y_i$ di ciascuna lettera dei due messaggi originali. Sembra che, dopo tutto questo lavoro, siamo tornati al punto di partenza, ma in realtà non è così. Infatti, invece di avere la somma di un messaggio con una sequenza di numeri casuali, abbiamo la somma di due messaggi che non sono affatto casuali e che quindi sono vulnerabili a diversi tentativi di decifrazione. Grazie a questo trucco, i servizi segreti britannici e statunitensi sono riusciti a decifrare delle comunicazioni sovietiche e tedesche durante la seconda guerra mondiale.

Quando è utilizzato correttamente, lo one time pad è il cifrario più sicuro della storia, ma anche il più scomodo: infatti richiede di tenere segreta, talvolta per lungo tempo, una lunga sequenza di numeri casuali. Inoltre Alice e Bob devono essere perfettamente sincronizzati: se uno di loro si trovasse anche solo un numero avanti o indietro nell'elenco, nessuno dei due riuscirebbe a decifrare i messaggi dell'altro. Nonostante questo limite, la sicurezza dello one time pad è tale da averlo fatto adottare in diversi momenti critici degli ultimi sessant'anni, come per esempio nel filo diretto tra il Cremlino e il Pentagono a partire dalla crisi dei missili di Cuba del '63.

Emanuele Bottazzi
emanuele.bottazzi@alumni.unitn.it

Bibliografia

[1] O'Donnell, Michael (2002) «Identification Protocols in Cryptography», The ITB Journal: Vol. 3: Iss. 1, Article 3. doi:10.21427/D7WW54 Available at: http://arrow.dit.ie/itbj/vol3/iss1/3.