CAP. 17

LE CHIAVI ALLE MASSE

Diffie, Rsa e Zimmerman. Come in vent'anni la crittografia è divenuta un terreno di libertà, dopo essere stata un affare dei militari e delle spie. Anche la moneta elettronica deve essere anonima e riservata

Crittografia? E' quel gioco che tutti i ragazzini fanno a scuola, per camuffare i loro biglietti, sì che solo chi possiede il codice segreto possa capirli. E' quella tecnica molto importante che fu al centro di una delle battaglie più cruciali e meno note nella seconda guerra mondiale, quando si trattava di decifrare tempestivamente i messaggi che i comandi nazisti mandavano, via radio, alle loro truppe: anche da quelle ricerche nacque il computer.

La parola "crittografia" viene dal greco, ed indica l'arte della scrittura nascosta o, forse e meglio, la scienza del saper costruire e rompere i codici segreti. I sistemi crittografici consentono la trasformazione delle informazioni trasmesse (lettere comuni, conversazioni radio e telefoniche, posta elettronica) in dati cifrati inintellegibili a chiunque non possieda i necessari strumenti per la decodificazione.

Lo scopo è garantire la segretezza del messaggio, che sarà disponibile in chiaro solo a mittente e destinatario.

In realtà ogni sistema di segni, per esempio un alfabeto, è un sistema crittografico: solo chi li possiede può capire che cosa significa quel testo; se non si conosce lo "jezyk" (linguaggio, in polacco), si è esclusi dal codice e dalla comunicazione

Si può usare la crittografia per proteggere i segreti militari di uno stato o quelli commerciali di un'azienda; per difendere la propria privacy o per riscuotere un abbonamento televisivo: così avviene per esempio nelle televisioni a pagamento, per vedere le quali è necessario mettere un apposito apparecchio tra l'antenna e il televisore; esso riceve un segnale strapazzato (come le uova, *scrambled*) e rimette le cose a posto. Per maggiore sicurezza il codice che pilota l'apparecchio viene cambiato ogni tanto e consegnato solo agli abbonati in regola con il canone.

Come è facile immaginare, si è instaurata una gara continua tra i cifratori e i decifratori, tra chi vuole mantenere inaccessibili e segreti i propri messaggi e chi li vuole carpire impunemente.

Dominio incontrastato di spie, diplomatici, militari e agenzie governative fino alla metà degli anni '70, la crittografia (o *encriptazione*) ha infatti oramai un ruolo centrale come strumento pubblico a protezione della trasmissione di informazioni riservate tra singoli individui. E' insomma uno strumento di difesa del cittadino contro i sempre più numerosi spioni al soldo di questa o quella entità che origliano le sue comunicazioni personali o le sue transazioni commerciali.

La metafora è quella della "chiave": c'è una chiave (un numero o un insieme di numeri) con cui crittografare il messaggio di partenza, e solo chi in ricezione

possiede la stessa chiave numerica potrà aprire il segreto: per questo si parla anche di messaggi "cifrati".

I sistemi classici di crittografia si basano su una chiave unica. Può essere un numero, un insieme di numeri, un algoritmo, non importa. Se il mittente A deve mandare un messaggio riservato al destinatario B, prende il testo e lo mette in codice, usando la chiave. Quando B riceve il messaggio, userà la stessa chiave per decodificare (de-crittare) il testo, eseguendo l'operazione inversa. Per esempio in un banale sistema di codici che preveda di sostituire ogni lettera dell'alfabeto con quella che la segue, la parola "addio" diventerebbe "beelp". La chiave è nella regola: "traslare in avanti di uno".

Ovviamente la segretezza è garantita soltanto a due condizioni: che sia A che B non rivelino ad altri la chiave; e che il sistema di codici sia sufficientemente furbo da alterare la frequenza delle lettere. Tutti sanno, infatti, che le lettere dell'alfabeto compaiono con diverse frequenze nelle lingue parlate; per esempio in italiano la lettera 'a' è quella più usata, seguita da 'e', 'i' eccetera. Dunque una spia che non conosca la chiave potrebbe comunque individuarla semplicemente disponendo di molti messaggi e facendo un po' di statistica sul numero di volte con cui i diversi simboli compaiono. Questo è il compito dei *criptoanalisti*. Di questo si occupavano i matematici inglesi che durante la seconda guerra mondiale riuscirono con successo a rivelare i meccanismi su cui si basava *Enigma*, la macchina crittografica usata dai comandi militari nazisti. Tra di loro c'era Alan Turing, il matematico padre dell'informatica teorica. Ma anche Claude Shannon, uno dei costruttori della Teoria dell'Informazione, si dedicò lungamente alla crittografia.

Dunque in un sistema di crittografia perfetto il testo codificato non deve rivelare più alcuna informazione relativamente al testo in chiaro originale. La cosa è teoricamente fattibile, ma così complicata e farraginosa da risultare impraticabile.

Perciò tutti i codici in circolazione sono in qualche modo un compromesso. La loro sicurezza sta soprattutto nel fatto che la chiave resti assolutamente segreta, oppure nel fatto che per scovarla occorra troppo tempo, persino con i moderni e superveloci computer.

Lo standard crittografico adottato ufficialmente nel 1977 dal governo americano (National Bureau of Standards) si chiama DES (*Data Encryption Standard*). E' un sistema di crittografia inventato dai ricercatori della Ibm ed è a chiave unica, basato su una serie di sostituzioni e trasposizioni di lettere. Il metodo è noto e pubblico, ampiamente descritto nei libri: per come è costruito esistono in tutto 2^{56} chiavi, e questo lo rende difficile da rompere.

Ma anche così il DES continua ad avere dei critici. Infatti anche quando il sistema sia robusto, la chiave unica crea molti problemi. In qualche modo A e B devono mettersi d'accordo e passarsela di persona. Ma sulle reti di computer, dove entrano in contatto persone lontanissime che magari non si sono mai incontrate fisicamente, questo può essere impossibile; né conviene spedirsela per via elettronica, dato che potrebbe essere intercettata.

Il suo uso è raccomandato per la protezione dei documenti riservati, ma non viene giudicato invece sufficiente per i documenti "classificati", quelli protetti da segreto ufficiale, infatti chi abbia a disposizione un computer abbastanza potente potrebbe riuscire ad "aprirlo".

Due chiavi meglio di una

La svolta cruciale nella moderna crittografia avviene nel 1976 quando il programmatore trentunenne Whitfield Diffie e il professore d'ingegneria elettrica presso la Stanford University Martin Hellman annunciano al mondo intero l'invenzione della chiave pubblica, il primo passo verso la privacy per le masse.

«Siamo all'inizio di una rivoluzione nella crittografia». Cominciava così, senza modestia alcuna, l'articolo che Whitfield Diffie e Martin Hellman pubblicavano nel novembre del 1976 su una rivista assai specializzata di scienza dei computer[1]. Ma non avevano torto a essere vanagloriosi: il marchingegno matematico da loro escogitato è stato addirittura definito dallo storico David Kahn, «il concetto più rivoluzionario nel settore dopo il Rinascimento». Il rimando al Rinascimento non è un'enfasi eccessiva: quella fu epoca di grandi studi sui cifrari, che impegnarono, tra gli altri, Leon Battista Alberti.

Il primo effetto immediato fu la rottura del ferreo regno che la National Security Agency (NSA) aveva esercitato per decenni, controllando la diffusione dei programmi di crittografia con l'imposizione di complicate procedure per i brevetti e con la loro equiparazione alle armi pesanti, soggette ad approvazioni governative per l'esportazione; questa prassi militare rendeva praticamente impossibile la ricerca da parte dei programmatori di software. Una volta infranto tale schema, a guadagnarci sono stati i diritti civili dei cittadini telematici presenti e futuri: non a caso Whit Diffie è stato definito il "profeta della privacy".

Lui, ora cinquantenne, lavora come consulente alla Sun Microsystems, una delle più affermate aziende americane di computer; è stimatissimo e riverito, un vero santone ascoltato con rispetto da industriali e agenzie del governo. Ma allora, nel 1976, non aveva ancora combinato molto nei suoi 33 anni di vita: un diploma in computer science al Mit, quindi il trasferimento a Stanford per lavorare al laboratorio di intelligenza artificiale di John McCarty. Qui la scoperta del tema della privacy e dei modi per proteggerla; qui una sorta di ossessione mentale che lo porta a girare tutte le biblioteche del paese e, nello stesso tempo, a tenere nascosto il suo interesse perché si trattava comunque di materia classificata, di cui non ci si poteva occupare troppo apertamente.

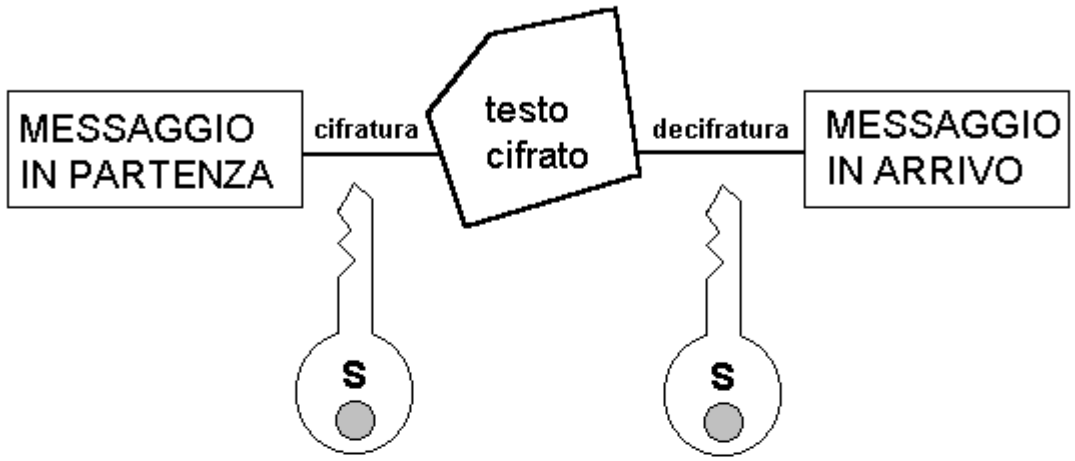
Fino a quella mattina del maggio 1975. Mentre riordinava la casa con una lattina di Coke in mano, tanto rimuginare prese di colpo forma in un'idea precisa: un sistema di codici *a doppia chiave*, con cui garantire insieme tre cose preziose: la riservatezza dei messaggi, la loro autenticità e la loro integrità.

---

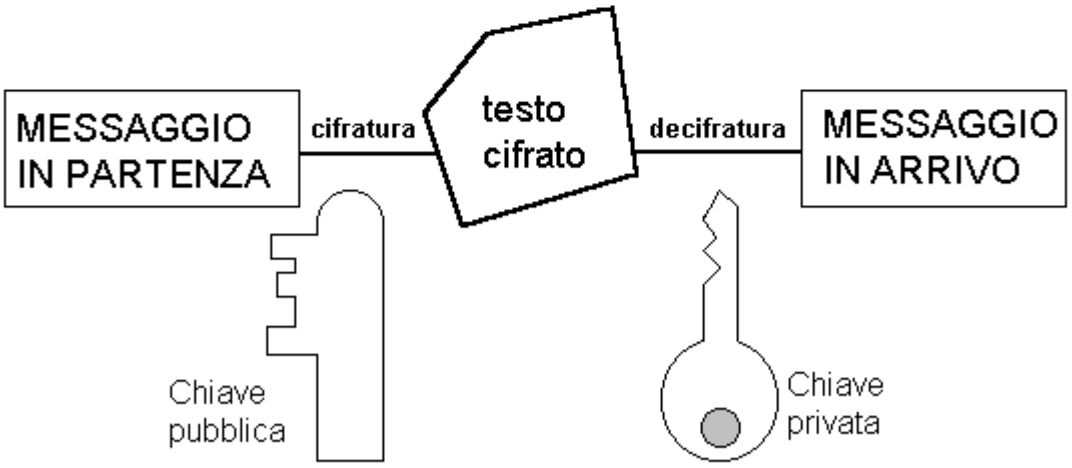
[1] W. Diffie and M. E. Hellman, «New directions in cryptography», I*EEE Transactions on Information Theory*, Vol. IT-22, No. 6, November 1976, pp. 644-654

Il suo capo alla Stanford university era David Hellman. Accolse l'idea con iniziale scetticismo, ma divenne via via più entusiasta, fino al grido di gioia in quella prima frase del loro articolo. Ma dove stava la novità?
Il sistema a doppia chiave escogitato da Diffie risolve il problema in modo ingegnoso: ognuno rende nota a tutti gli altri la sua chiave pubblica (possono anche essere contenute in appositi elenchi simil-telefonici). Se A vuole scrivere a B, userà la chiave pubblica di B per mettere in codice il messaggio. Ma quel testo può essere riportato in chiaro solo disponendo anche della chiave privata, che solo B conosce e che non mette a disposizione di nessuno. La semplice conoscenza della chiave pubblica, invece, non permette di leggere il messaggio. Viceversa, per autenticare un messaggio, A userà la propria chiave privata e B potrà verificare la firma elettronica di A usando la chiave pubblica di A.

SISTEMA DI CRITTOGRAFIA
A CHIAVE UNICA, SEGRETA



SISTEMA DI CRITTOGRAFIA
A DOPPIA CHIAVE



Come è possibile? Il "trucco" escogitato da Diffie consiste nell'uso di alcune funzioni matematiche che sono, per così dire, "a senso unico". E' facile calcolarle in una direzione e molto più difficile calcolarle nella direzione inversa. L'operazione matematica del quadrato, per esempio, è facile in entrambe le direzioni: a^2 = a x a mentre, viceversa, a = $\sqrt{a^2}$. Invece se si lavora con i numeri primi (quelli che non sono divisibili per nessun altro), sarà abbastanza facile moltiplicarne due tra di loro, ma molto più difficile partire dal prodotto e trovare i due numeri primi che lo compongono: certo è immediato scomporre il numero 21 nel prodotto dei numeri primi 7 e 3, ma quando si tratti di numeri con centinaia di cifre l'operazione risulta praticamente irrealizzabile.

Proprio sui numeri primi e su una serie di operazioni matematiche realizzate a partire da essi, si basano i sistemi a doppia chiave.

Detto così sembra assai strano e persino incomprensibile. Eppure è possibile, funziona, ed è effettivamente assai robusto.

La prima applicazione pratica del sistema a doppia chiave, sotto forma di un algoritmo matematico trasferibile nel programma di un computer, arriva subito nel 1978, grazie a Ronald Rivest, Adi Shamir e Leonard Adleman. Per renderlo abbastanza robusto basta usare dei numeri primi molto lunghi. Quando il sistema RSA venne inventato (il nome è composto con le iniziali dei loro cognomi) si valutò che per spaccare in due primi un numero di 129 cifre fossero necessari $40x10^{15}$ anni di lavoro al computer, ben più che l'intera vita dell'universo. Ma nel 1994 un numero RSA da "sole" 129 cifre è stato spezzato in due. L'impresa non è dovuta a un singolo matematico, dotato di un grande calcolatore, ma alla rete Internet. Nell'occasione 600 gruppi di ricerca, sparsi in 25 paesi, che hanno messo a disposizione circa 1600 macchine da calcolo, dai personal ai supercomputer.

L'esperimento di rottura, portato a termine da Arjen Lenstra dei laboratori di ricerca Bellcore, ha richiesto 8 mesi di lavoro. I computer reclutati per lo scopo usarono i loro tempi morti per effettuare ognuno un pezzo dei calcoli. La furbata di Lenstra è consistita nel mettere a punto degli algoritmi di calcolo molto efficienti e nel dividere con intelligenza il compito tra più gruppi. Questo allora vuol dire che il sistema RSA non è poi così sicuro? Affatto: è davvero difficile che un gruppo di malintenzionati possa disporre di una tale potenza di calcolo; occorrerebbe immaginare una rete di delinquenti ben coordinata e matematicamente molto avanzata. Tra l'altro chi utilizza il sistema crittografico RSA già oggi si serve di numeri lunghi almeno due o trecento cifre e ogni cifra in più rende sei volte più difficile (e più lunga) la scomposizione.

Dunque RSA è quasi perfetto, ma proprio per questo viene osteggiato dal governo americano e dai suoi spioni. I software che lo utilizzano possono essere liberamente usati negli Stati uniti, ma non possono essere esportati: è un vero e proprio reato. Il che ha generato diverse proteste da parte dei produttori di software che si vedono privati di un mercato mondiale della crittografia che, senza l'embargo governativo, potrebbero ampiamente dominare.

Il disappunto dei costruttori è ancora maggiore perché il sistema RSA è brevettato. Nel 1982, infatti, Rivest, Shamir e Adleman fondavano la *RSA Data Security Inc*. per utilizzare commercialmente il loro sistema. Forse per la prima volta nella storia delle scienze, un insieme di regole matematiche (un algoritmo) è stato brevettato.

Come se Pitagora avesse brevettato il suo teorema, obbligando tutti quelli che lo usavano a pagargli un tot. In questo caso il Patent Office americano, che da un po' di tempo sembra preso da follia, ha riconosciuto il pieno controllo dell'algoritmo ai tre matematici.

Resta comunque il fatto che le idee matematiche non dovrebbero essere brevettabili: così da tempo diversi programmi ispirati a quell'algoritmo di codifica circolano liberamente fuori degli Stati Uniti, dove non sono coperti da brevetto e dove non arrivano i funzionari dell'amministrazione americana. E' illegale l'atto di esportarli, ma non è illegale possederli e usarli fuori degli Stati Uniti.

Non solo, c'è addirittura chi li diffonde liberamente su Internet: Philip Zimmermann, per esempio, un fervido sostenitore della libera circolazione del software. Zimmermann ha realizzato nel 1991 un suo sistema di codifica, e l'ha chiamato PGP, *Pretty Good Privacy* , cioè una "riservatezza abbastanza buona".

«Volevo rafforzare la democrazia e garantire agli americani la possibilita' di continuare a proteggere la privacy individuale» - ha detto Zimmermann dopo aver ricevuto uno degli *Awards 1995* della Electronic Frontier Foundation (EFF).

Il PGP si può prelevare liberamente dai computer Internet e questa pratica viene incoraggiata da tutti i cybernauti: per dispetto al governo Usa e per avere uno strumento in più, sicuro e affidabile.

Export proibito

Per aver fatto circolare il PGP in America, Zimmermann venne citato in tribunale dalla Rsa, per violazione del brevetto. Va detto che egli si era limitato a distribuirne pochissime copie ad alcuni amici, i quali - preoccupati da una legge allora in discussione al Congresso (poi non approvata) che prevedeva la totale messa fuori-legge dei programmi d'encriptazione - lo inserirono materialmente in vari sistemi telematici californiani.

La causa legale con la Rsa si è protratta per un po' di tempo e poi è finita nel nulla, anzi con una vera e splendida vittoria di Zimmerman e dei libertari. I dettagli delle trattative sono tortuosi assai. Per un certo periodo Phil cercò di ottenere da Jim Bidzos, il presidente della Rsa, una licenza gratuita a usare il brevetto. Ma gli venne risposto di no, perché era già stata attribuita ad altri sub-licenziatari. Poi venne una lettera di intenti, con la quale Rsa rinunciava a ogni causa legale, purché Phil la smettesse di diffondere il suo PGP. Ma quando una nuova versione del programma spuntò di nuovo sulla rete Internet, su computer australiani e olandesi, l'Rsa si sentì ingannata e lo accusò di aver fatto il doppio gioco.

La mossa decisiva che mise fine al litigio legale arrivò dal Massachusetts Institute of Technology. Nell'assurda catena dei brevetti che si incrociano attorno alla doppia chiave, il Mit in realtà è il primo licenziatario, che poi gira il diritto alla Rsa. James Bruce del Mit era dell'idea che «i sistemi crittografici devono essere messi nelle mani del grande pubblico e che PGP corrispondeva perfettamente allo scopo». Fu proprio il Mit a spingere alla collaborazione Zimmerman e l'Rsa per la realizzazione di nuove versioni di PGP, la release 2.5 e quella migliorata 2.6. Le quali hanno subito cominciato a circolare per la rete, in Europa e nel resto del mondo, alla faccia del dipartimento di stato e dei divieti all'esportazione.

"Senza encriptazione, ogni e-mail non è più sicura di una cartolina postale» dice Bruce Schneier, noto esperto ed autore della monumentale opera *Applied Cryptography* oltre che del recente *E-Mail Security*. Si spinge più oltre il movimento crypto-anarchico, nato nell'autunno del 1992 con un Manifesto, presentato da Timothy May che così concludeva: «Come la diffusione della stampa ha alterato e ridotto il potere delle corporazioni medievali e delle strutture sociali, così i metodi d'encriptazione modificheranno profondamente la natura imprenditoriale e l'interferenza statale nelle transazioni economiche. In combinazione con i mercati emergenti dell'informazione, la crypto anarchia creerà un mercato per tutte le cose che possono essere messe in parole e immagini. Proprio come un'invenzione apparentemente minore come il filo spinato ha reso possibile il recintare vasti ranch e fattorie, alterando così per sempre il concetto di terra e di diritti di proprietà, così anche la scoperta apparentemente minore di una branca arcana della matematica diventerà come le cesoie da metallo che smantelleranno il filo spinato attorno alla proprietà intellettuale».

Il quadro della discussione sulla diffusione pubblica della crittografia è molto fluido. Passaggi da una macchina all'altra, vulnerabilità dei sistemi, intrusioni illegali e furti di password sono comunque tutti motivi più che sufficienti per adottare serie precauzioni crittografiche.

I sistemi d'encriptazione sono sempre più diffusi in ambito commerciale, a garanzia di shopping online e transazioni finanziarie via Internet (per non parlare dell'imminente arrivo del contante digitale); sono anche apprezzatissimi dalle decine di milioni di persone che si scambiano quotidianamente messaggi personali di posta elettronica.

Sia le aziende che i singoli abitanti del cyberspazio si aspettano in sostanza che:

1. I messaggi siano *in busta chiusa*, apribile solo dal destinatario.
2. I messaggi siano *autentici*. Cioè che si possa avere la certezza che il mittente è proprio quello indicato, e non altri.
3. I messaggi siano *integri*, ovvero che nessuno possa manipolarli.

Eventualmente si vorrebbe anche che nessuno possa negare la paternità di un messaggio da lui spedito: per esempio che, una volta ordinate 200 tonnellate di semi di soia, un commerciante non possa negare di aver fatto quella commessa. Sono, in fondo, le stesse garanzie che il sistema telex offriva al mondo delle aziende. Ora con i sistemi a doppia chiave possono essere offerte anche dai computer, piuttosto semplicemente e con assoluta sicurezza.

Anonimi e nascosti

Ci sono diversi nodi della rete Internet (di cui una trentina ufficiali) che svolgono il servizio di *anonymous remailer*. Si potrebbe tradurre "ri-speditori anonimi" perché altro non fanno che ricevere dei messaggi di posta elettronica e ri-spedirli a destinazione. Nel farlo, però, provvedono automaticamente a "stripparli", cioè a togliere dalla intestazione tutte quelle indicazioni sulla loro provenienza che i diversi computer della rete altrettanto automaticamente avevano inserito. In tal modo garantiscono che essi arrivino a destinazione come provenienti da un sito anonimo, senza la possibilità di risalire al mittente. Il massimo dell'anonimato si ottiene utilizzando un'intera catena di remailer anonimi.

I motivi per cui i mittenti cercano l'anonimato nei remailer non interessano. Loro svolgono una funzione tecnica: quella di vettori postali. Sì, proprio come le Poste e Telegrafi che - per fortuna - non obbligano nessuno a identificarsi: sono vettori ciechi di un servizio di utilità generale dove possono circolare i messaggi più diversi, dalle lettere d'amore alle fatture commerciali; dalle minacce alle molestie sessuali. Nessuno si è mai sognato (se non negli stati più autoritari) di controllare la posta dei cittadini: perché mai dovrebbe avvenire su Internet?

Si risponde di solito dicendo che un conto è la corrispondenza privata, che ha pieno diritto alla riservatezza, attraverso la crittografia (e magari anche con l'uso dei remailer), ma che altro sono i messaggi destinati alle aree di dibattito. Trattandosi di luoghi pubblici ognuno si assuma la sua responsabilità, con nome e cognome veri, altrimenti taccia (per sempre?). Si contro-risponde che su certi argomenti caldi (politici, sessuali eccetera) l'anonimato può permettere una libertà di espressione che altrimenti andrebbe persa.

Ma la fobia per l'anonimato, la paura di essere chiamati a rispondere dei reati eventualmente commessi dai cybernauti che passano per il proprio nodo, ha già prodotto alcune pessime prassi nel mondo telematico. Non solo i grandi servizi come *Italia On Line* (Olivetti-24 ore) chiedono la fotocopia della carta di identità ai loro utenti, ma lo stesso hanno cominciato a fare molti BBS locali e amatoriali.

La grande rete mondiale Fidonet, poi, vieta il transito di messaggi crittografati, come *policy* da tempo stabilita e di recente ribadita. Su questo tema si è svolta una discussione accesissima: da una parte molti sysOp Fidonettiani che rivendicano il diritto di controllare i messaggi in transito sul loro BBS («è casa mia, e stabilisco io le regole») e dall'altra molti Internettiani fautori della crittografia Pgp.

Il timore di molti è di vedersi arrivare in casa la polizia, che magari sequestra il computer e il modem e blocca tutto, solo perché qualche cretino ha diffamato qualcun altro in quel luogo pubblico. Così in Italia, sempre sull'onda delle perquisizioni selvagge, si sente una gran voglia di autoregolamentazione. Circolano diverse proposte, delle specie di Carte dei Diritti e dei Doveri dei sysOp (i gestori dei nodi). Con la motivazione apparentemente ragionevaole di evitare che leggi più rigide eventualmente arrivino dall'alto, tutte queste proposte vanno nel senso di limitare gli spazi di espressione. Non è un bel vedere quando la gente

si incatena da sola e non ha più voglia di scrivere sui muri delle strade, ma soltanto sulle bacheche affisse nei luoghi consentiti, con licenza comunale e visto del "commissariato".

Un chip troppo curioso

Resta il fatto che il "commissariato", inteso come CIA ed FBI, sostiene che l'aumento esponenziale della crittografia pubblica impedisce alle autorità di prevenire e perseguire le attività criminali condotte via computer e modem, poiché le forze di polizia non sono in grado di verificare il contenuto dei messaggi cifrati in circolazione. «Noi siamo entusiasti sostenitori della crittografia pubblica, ma ritieniamo che non debba esser consentito a terroristi, perversi, dinamitardi, rapitori e criminali vari di muoversi a piacimento in un ambiente privo di apparati repressivi e mandati di perquisizione», dice Jim Kallstrom, agente della Special Operations Division di New York. Già. Terroristi, Pedofili, Riciclatori di denaro sporco e Trafficanti di droga. Ormai queste figure fantastiche sono diventate i Quattro Cavalieri dell'Internet, ha osservato ironico Timothy May.

Il 1994 è stato un altro anno di battaglia in nome della libertà di crittografia: infatti in febbraio l'amministrazione Clinton annunciava di aver adottato, su consiglio della National Security Agency, uno standard crittografico nuovo, destinato a sostituire il DES e a spiazzare RSA e PGP. Il proposito era di renderlo obbligatorio in tutte le apparecchiature vendute allo stato. In questo modo le aziende di alta tecnologia avrebbero finito per adottarlo definitivamente, anche negli apparati "civili".

L'hanno chiamato "Clipper" e mai nome (cesoie) fu più giusto, ha commentato molto polemicamente il *New York Times* . Infatti il piccolo chip voluto dal governo americano, minaccia appunto di «tagliare le ali delle libertà individuali». Sulle stesse colonne William Safire, che non è propriamente uno stinco di progressista, scrisse due colonne di indignata indignazione contro Big Ear, il Grande Orecchio che renderà «il singolo cittadino nudo di fronte a una burocrazia curiosa».
Clipper è un piccolo chip che contiene Skipjack , un algoritmo di codifica dei dati (voci, testi, numeri o quant'altro) che dovrebbe renderli sicuri e non intercettabili da osservatori-ascoltatori indiscreti. E allora che male c'è?

La National Security Agency, progettandolo, aveva sfidato i ricercatori a scassinarne il meccanismo. Nel maggio del 1994 Matt Blaze, un giovane matematico che lavora ai Bell Laboratories della At&t, c'è riuscito. Il difetto stava nella porta sul retro, la *backdoor*, appositamente progettata per consentire agli spioni governativi di intercettare le comunicazioni. Tecnicamente viene chiamata LEAF (*Law Enforcement Acces Field*) ed è protetta da una parola di 16 bit su cui viene effettuata un'operazione matematica (tecnicamente una *checksum*). Per scassinare il Clipper, Blaze ha impiegato soltanto 42 minuti.
Nelle intenzioni del governo la chiave di accesso alla backdoor sarebbe stata a disposizione di tutti i possibili servizi segreti americani, dalla National Security Agency alla Cia e allo stesso Fbi, ma l'accesso consentito solo previa autorizzazione di un magistrato; ciò non è bastato tuttavia ad accontentare i

difensori della riservatezza e della libera circolazione delle idee: «Information must be free», è lo slogan assai efficace del cyberspazio libertario.

E infatti Clipper suscitò, nella primavera del 1994, una vera rivolta nel cyberspazio, guidata da organizzazioni come la EEF (*Electronic Frontier Foundation*), da Cpsr, ovvero dall'associazione dei "Professionisti del computer per la responsabilità sociale", e dalla rivista *Wired*. Centinaia di fax e di messaggi in posta elettronica raggiunsero il vice presidente Al Gore che si era fatto una fama di ecologo e di alto-tecnologo, ma che era scivolato malamente sulla buccia di banana delle libertà.

«Non comprate nulla che contenga il chip Clipper. Non comprate alcun prodotto da alcuna azienda che fabbrichi degli apparecchi che contengono al loro interno il Grande Fratello. E' possibile che il governo vi chieda di usare Clipper per le vostre comunicazioni elettroniche con il servizio fiscale o per i vostri affari con le agenzie federali. Non possono chiedervi di farlo. Just Say No». Questa una delle frasi assai battagliere disseminate su Internet. Un altro appello diceva: «E' una guerra rivoluzionaria quella in cui siamo impegnati. Clipper è l'ultimo tentativo degli Stati uniti, l'ultima grande potenza delle vecchia Era Industriale, di stabilire un controllo imperiale sul cyberspazio. Se loro vinceranno, lo sviluppo più liberatorio nella storia dell'umanità, potrebbe divenire, invece, il sistema di sorveglianza che controllerà la moralità dei nostri nipoti»

Alla fine, dopo mesi di polemiche, Clipper è finito nell'ombra, nella sostanza abbandonato dal vicepresidente Gore[2]. La sconfitta di Clipper, però, non è stata opera soltanto dei libertari. Le case di computer americane hanno esercitato una potente azione di lobby contro il chip malcapitato. E questo per un motivo molto banale: i sistemi di crittografia sono molto richiesti dalle aziende che vogliono garantirsi comunicazione sicure. Ma sarebbe davvero difficile vendere fuori degli Stati uniti dei computer o dei telefoni che le agenzie di spionaggio americane possono ascoltare quando vogliono (che la CIA si dedichi largamente allo spionaggio industriale oltre che a quello militare è vero da sempre, ma questa tendenza è aumentata dopo il crollo dell'impero sovietico).

Dunque oramai i sistemi crittografici sono largamente diffusi, ma, eliminato Clipper, c'è ancora da fare chiarezza sullo standard: Rsa, PGP o qualche loro nuova fantasiosa variante? Nell'aprile 1995, un gruppo di grosse aziende ha deciso di investire molti dollari in una piccola casa di Menlo Park, in California, sconosciuta ai più. Si tratta della *Terisa Systems Inc*., a sua volta controllata dalla Rsa. Gli investitori sono grossi nomi come Ibm, America On Line, Compuserve e Netscape. L'obbiettivo sembra che sia proprio quello di costruire lo standard crittografico vincente per l'Internet di domani, armonizzando e rendendo compatibili quelli adottati separatamente da Netscape e Rsa.

---

[2] E' stato però approvato, nell'autunno 1994, il *Digital Telephony Bill*, che impone comunque ad aziende e produttori nel campo della telecomunicazione di organizzare i propri sistemi in modo da consentire rapide intercettazioni governative.

E-MONEY

Sembra che ci sia un insopprimibile bisogno di moneta elettronica sull'Internet. Moneta sicura, garantita, esente da rischi di falsificazioni e di rapine. Solo così la grande rete, finora organizzazione spontanea e *nonprofit*, sarà pienamente praticabile dai venditori e dagli acquirenti. I primi potranno offrire due cose: a) la merce-informazione sotto forma di bit agevolmente trasferibili dal produttore al consumatore; b) la merce-merce, fatta di atomi, che sui Web colorati appare solo come immagine e simulacro, ma che verrà inviata a casa in seguito, dopo aver premuto sullo schermo gli appositi pulsanti. In quest'ultimo caso potrebbe anche funzionare il pagamento alla consegna, ma è una forma desueta, da quando le case sono meno abitate e i portinai esistono solo nelle residenze dei ricchi (ma anche in quelle spesso sono sostituiti da vigilantes).

Serve insomma l'accredito automatico, il trasferimento elettronico dei fondi.

Questa è un'attività che le banche già compiono da decenni, reciprocamente riconoscendosi il dare e l'avere; sono soltanto i loro utenti che vengono penalizzati con i giorni di valuta, come se gli assegni da Milano a Pavia («fuori piazza») viaggiassero a dorso di mulo. Per non dire dei trilioni (migliaia di miliardi) di dollari che vorticano tra le piazze finanziarie del mondo: apparentemente immateriali, ma tali comunque da determinare le politiche, i livelli di vita, le pensioni e i salari delle persone. Per tutte queste attività esistono da tempo super computer e reti specializzate, a prova di scasso e di crash.

Qui si sta parlando invece delle minute transazioni (ma globali, milioni di volte al giorno) che su Internet e affini potrebbero svolgersi e che richiedono che quei 9.99 dollari siano immediatamente versati al destinatario a colpo di clic. «A meno che Internet non abbracci il commercio, corre il rischio di fare la stessa fine della radio CB. Se le aziende non fanno soldi, non aggiungeranno valori ai servizi e il tutto non funzionerà», ha dichiarato Lee Stein, l'avvocato californiano che ha fondato la *First Virtual Bank*, con l'ambizione di farne una vera banca elettronica.

Dunque avverrà, non c'è dubbio che avverrà, anche se nella fase iniziale i servizi *online* che vendono merci sulla rete (AOL, Compuserve, per non dire della nostrana Italia Online) hanno fatto affari assai magri: il popolo telematico per ora preferisce chiacchiere e interazioni anziché shopping. Forse a ragione. Ma come avverrà e con quali sistemi universalmente diffusi e accettati nessuno lo sa.

Emergono tuttavia due tendenze, *filosoficamente* contrapposte. Val la pena di capirle.

Come il Bancomat

La prima ipotesi, favorita dalle banche e dai governi, non è altro che un'estensione alle reti di computer del sistema attuale delle carte di credito. In sostanza basterebbe stabilire una volta per tutte un bell'accordo internazionale, con il quale si sceglie un sistema di crittografia sicuro e robusto che tutti adotteranno, i venditori come i compratori. Allora ci si potrà fidare a immettere il numero della propria carta sul terminale, sapendo che esso viaggerà sicuro fino a destinazione.

Va in questa direzione l'accordo del 9 novembre 1994 tra Microsoft e Visa.

Lo svantaggio è che soltanto chi ha una carta plastificata può comprare, gli altri no.

E poi c'è un'altra perplessità di fondo: in questo modo si dilata a dismisura quella gigantesca schedatura dei gusti e dei consumi delle persone che le grandi aziende di televendita già stanno realizzando. Si è già descritto come l'incrocio infinito dei più svariati database elettronici consenta ormai di spogliare ogni singolo cittadino di ogni riservatezza.

Nell'attesa dello standard universale, la *First Virtual Bank* ha messo a punto e sta sperimentando il suo sistema: sia venditore che compratore hanno un conto in banca. Quando il compratore sceglie un prodotto, dà il suo numero di codice al venditore, autorizzandolo a farsi accreditare l'importo. La banca, a sua volta, manda un messaggio elettronico al compratore chiedendogli conferma dell'acquisto effettuato; in caso positivo la somma viene trasferita. Non c'è dubbio che, per quanto rapida sia la messaggeria elettronica, questo resti un modo complicato e tortuoso di far la spesa.

Come le banconote

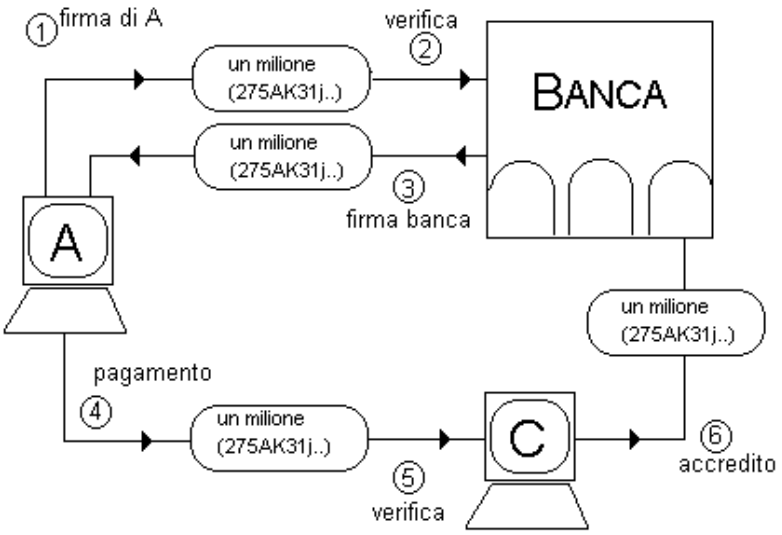
Il bello della moneta fisica invece è la sua praticità: ogni biglietto è coperto dalla banca nazionale di emissione e perciò accettato da tutti. Non solo: si può usarlo senza dover dichiarare a nessuno nome, cognome e residenza. Meno che mai il numero del conto corrente bancario. Come mantenere queste innegabili virtù dell'anonimato anche nella grande rete?

Lo schema proposto dalla *Digicash* di Amsterdam va in questa direzione e utilizza il sistema della doppia chiave pubblica-privata. Il fondatore e proprietario di questa piccola azienda è David Chaum, professore di informatica a Stanford.

Il modello di Chaum è di tutti il più avveniristico e interessante: si basa infatti su di una vera e propria circolazione di moneta elettronica, dove ogni banconota altro non è che un numero opportunamente generato e unico (così come unica è ogni banconota emessa da una banca centrale). Il sistema della doppia chiave permette, nella versione più semplice, di controllare l'autenticità della banconota, ed è descritto nella figura a fianco. Nella formulazione più spinta, attraverso una serie di passaggi tecnici qui troppo complicati da descrivere, garantisce anche il totale

anonimato: in questo modo né gli uffici di marketing, né i governi intriganti possono sapere se uno ha acquistato condom o bibbie.

Un tentativo di truffa può consistere nel cercare di spendere due volte la stessa banconota. Solo in questo caso l'anonimato viene rotto: si aprono gli archivi della banca e si va a vedere chi ha "spacciato" quella banconota.



*1) **A**ndrea ha un conto corrente presso la **B**anca. **A** ha bisogno di moneta elettronica da spendere sulla rete. Il suo computer genera un numero di serie di una banconota, per esempio da un milione, lungo 100 cifre. Lo codifica (lo firma) con la sua chiave privata e lo spedisce alla **B**anca.*
*2) La **B**anca usa la chiave pubblica di **A**ndrea per decodificarlo e verifica così che proviene proprio da lui.*
*3) La **B**anca defalca un milione dal conto di **A**ndrea e gli rispedisce il biglietto, controfirmato da lei stessa per convalida.*
*4) **A**ndrea decide di comprare libri per un valore di un milione dalla **C**ooperativa del manifesto: conferma l'ordine telematico e spedisce a **C** la sua banconota.*
*5) La **C**ooperativa decodifica la banconota ricevuta da **A**ndrea, usando la chiave pubblica della **B**anca; se il biglietto è legittimo la decodifica riesce e la transazione è completata.*
*6) La **C**ooperativa potrà riusare quella banconota oppure versarla alla **B**anca.*

Naturalmente tutte queste operazioni avvengono automaticamente dentro il computer; Ogni soggetto coinvolto deve soltanto puntare alcuni simboli sullo schermo, che rappresentano la banca, le banconote a sua disposizione, eccetera.

I problemi della moneta elettronica, su rete, non finiscono però con la sicurezza e la riservatezza. Risolti quelli, ne emergeranno altri più di fondo, magari più drammatici. Alcuni sono già ben identificabili, altri sono del tutto avveniristici, ma potrebbero tuttavia essere dietro l'angolo.

Se la rete è globale, altrettanto senza confini sarà il denaro che vi circola: allora come far pagare le tasse per gli incassi su Internet, e dove, in quale paese? Nello schema "carta di credito", con transazioni sempre registrate, tutto è regolare; anzi, nessun pagamento sfuggirà agli uffici delle imposte. Ma nel caso della moneta

elettronica tipo Digicash (che garantisce la privacy dei cittadini - e questo è un valore) rintracciare gli scambi e riscuotere l'Iva sarà un bel problema.

Non solo: si ripropone la vecchia questione delle monete, nella sua forma più pura e astratta. La moneta da un lato serve come mezzo di scambio, al posto del baratto tra le merci. E da questo punto di vista la e-money offre il massimo dei vantaggi, quanto a facilità e rapidità di circolazione. Dall'altro canto però le monete sono depositarie di un valore. O perché valgono esse stesse, essendo fatte di materiali preziosi, o perché un istituto di emissione ne garantisce la convertibilità e, grazie ad essa, ognuno è disposto a fornire beni materiali in cambio di pezzi di carta.

Dunque anche l'e-money - elettronica e impalpabile - dovrà verosimilmente avere un corrispettivo in un qualche deposito di moneta fisica, presso qualche banca. O, viceversa: a ogni unità di moneta reale corrisponde un "alias" nel mondo digitale.

In questo caso un attivo in e-money non potrà fruttare interessi perché quelli che guadagnerebbe sono persi dal contante reale che la sostiene, che è immobilizzato.

Non dovrebbe essere possibile però il prestito solo digitale, perché questo aumenterebbe il circolante di moneta elettronica senza però incrementare, in corrispondenza, la quantità di moneta reale; in tal caso andrebbe a pallino la convertibilità.

Non è detto che alle banche faccia tanto piacere. Rischiano di essere costrette a accreditare e validare la moneta elettronica senza poterci guadagnare sopra. Certo potrebbero sempre caricare sui clienti una certa quota di servizio per la conversione carta-bit e viceversa, ma sarebbe inevitabilmente poca cosa, vista la rapidità e l'automatismo delle operazioni, tutte fatte dai computer, e la concorrenza relativa tra istituti bancari.

Ma ci si può spingere ancora più in là: magari il dogma della convertibilità potrebbe essere definitivamente abbandonato, anche a opera di privati cittadini o di organizzazioni. Per esempio John Blutarsky potrebbe decidere, insieme a una sottopopolazione di softwaristi di Internet, di commerciare in una moneta convenzionale di rete, chiamata l'*hacker*. Vuoi il mio ultimo programma per leggere e smistare la posta elettronica? Vale 27 hacker, cioè tre volte il tuo giochino da 9 hacker che è l'ennesima variante di Tetris. Sarebbe un e-cash senza uno stato di appartenenza (o, se si preferisce, una moneta di tutti gli stati), infinitamente scambiabile senza le spese e gli inconvenienti legati al passaggio da una valuta all'altra. Perché no? In fondo non sarebbe come le conchiglie con cui si fanno gli acquisti in certi villaggi turistici? Molte comunità virtuali potrebbero finire per battere la loro moneta. Allora per i commerci tra una comunità e un'altra si dovrebbero stabilire dei fattori di scambio. Magari la comunità Blutarsky vale di più di quella di Joe Condor. Oppure i valori fluttuano, come fluttuavano nel secolo scorso in America le diverse monete emesse dalle diverse banche. Una bella confusione. Ma forse anche un vantaggio: Chaum della Digicash, violentemente proiettato nel futuro cyber, vede con favore l'emergere della moneta elettronica di rete. Finché uno la utilizza dentro Internet non deve ricorrere a tutte le fastidiose e costose conversioni nelle valute dei diversi stati, a seconda di dove fa acquisti. Solo quando ha bisogno di contante fisico la cambierà. Ma potrebbe succedere di rado, o anche mai, se le attività commerciali sui network continueranno a crescere.