Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Nuno Crato

Codici indecifrabili, messaggi sicuri; Alice, Roberto e il ficcanaso; Crittografia quantistica

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **7-A**—*La Matematica nella Società e nella Cultura* (2004), n.2, p. 275–289.

Unione Mastematica Italiana

<http://www.bdim.eu/item?id=BUMI_2004_8_7A_2_275_0>

Bollettino dell'Unione Matematica Italiana, Unione Mastematica Italiana, 2004.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. VII-A, Agosto 2004, 275-289

L'EMS, European Mathematical Society, per mezzo del suo comitato Raising Public Awareness of Mathematics *ha assegnato il primo premio per il migliore articolo di divulgazione della matematica al Professor Nuno Crato del Dipartimento di Matematica dell'Instituto Superior de Economia e Gestão, Universidade Técnica de Lisboa per l'articolo, diviso in tre parti* Cibersegredos invioláveis *pubblicato sul settimanale portoghese* Expresso-Revista, *nelle date 8, 22, 29 settembre 2001. Il premio era riservato ad autori di articoli apparsi entro il 31 dicembre 2002 su giornali o riviste di largo richiamo.*

Il nostro Bollettino La Matematica nella Società e nella Cultura *provvede, in questo numero, a tradurre ed a pubblicare il lavoro di Nuno Crato, come esempio interessante di divulgazione della Matematica al grande pubblico. Al fine di inquadrare e trattare più ampiamente il problema della divulgazione matematica, in specie quella rivolta al grande pubblico, il Bollettino pubblica in questo stesso numero l' articolo* Matematica e Cultura: la via maestra della divulgazione *del nostro Michele Emmer. I lettori troveranno, tra l' altro, nel contributo di Emmer, membro del Comitato* Raising Public Awareness of Mathematics, *altri dati e considerazioni relativi ai tre articoli di Crato. (N.d.D.)*

NUNO CRATO

Codici indecifrabili, messaggi sicuri (*).

La sicurezza del commercio elettronico è garantita da un metodo matematico innovativo: un codice che permette di chiudere delle cifre in una cassaforte che può essere riaperta solo da una chiave segreta.

Vi sentite a disagio nel digitare il numero della vostra carta di credito per acquisti in Internet? Avete mai rinunciato a comprare un disco o un libro perché il commesso vi ha chiesto di usare la carta di

(*) L'articolo è apparso su «Expresso-revista» nel numero dell'8 settembre 2001, sotto il titolo: *Cibersegredos invioláveis.*

Esso è reperibile attualmente sulla pagina web dell'European Mathematical Society: *http://pascal.iseg.utl.pt/~ncrato/EMS/Crypto1.htm* nell'edizione inglese dal titolo *Unbreakable ciber-secrets*; da quest'ultima abbiamo tratto la presente traduzione a opera di Pierluigi Contucci.

credito? Sappiate che non siete i soli a non firdarvi! Ci sono molte persone in tutto il mondo che non prendono parte al cosiddetto «e-commerce» perché pensano che non sia sicuro. Ciò nonostante la circolazione di dati confidenziali attraverso la rete Internet è basata su uno dei più sicuri sistemi informatici attualmente a disposizione. Semplicemente seguendo delle regole elementari,quali evitare siti commerciali sconosciuti oppure spedire informazioni confidenziali via e-mail standard (non cifrata), il mondo dell'e-commerce è alla portata di tutti, in tutta sicurezza.

Internet ha aperto delle possibilità e fornito molte opportunità che sarebbero state impensabili solo alcuni anni fa. Esso è diventato una specie di biblioteca pubblica e ha permesso alla gente comune l'accesso al commercio internazionale in modo sicuro e veloce. Volete acquistare quel manuale tecnico che non trovate in libreria e di cui non ricordate neppure il titolo esatto? Cercate invano un disco di Bob Dylan? Siete dei collezionisti e non trovate la bussola del secolo scorso che vi interessa? Con Internet ora potete! E grazie all'accesso a moltissime reti internazionali vi potrebbe anche capitare di trovare, ad un ottimo prezzo, l'autobiografia di Max Planck che avete sempre desiderato e che da anni è fuori stampa. Forse, come è accaduto a chi scrive, c'è una libreria in Nuova Zelanda che ve la vende via Internet.

Ma siamo certi che è sicuro spedire i numeri delle nostre carte di credito in pezzetti e bocconcini che circolano Dio solo sa dove? Come possono Amazon e gli altri gestori di e-commerce garantire che le nostre informazioni non raggiungano mani meno affidabili che maneggia-

no tastiere in qualche altro angolo del mondo? Possiamo essere d'accordo col fatto che l'informazione è cifrata, ma anche se il messaggio è codificato attraverso una chiave che è spedita al mio computer, siamo certi che non sia possibile che qualcuno scopra la chiave stessa?

Questa domanda ha ovviamente una solida ragion d'essere. Per lungo tempo le comunicazioni segrete si state basate su sistemi di codifica a chiave simmetrica che permette di cifrare e de-cifrare i messaggi. Supponiamo per esempio la chiave assegna al simbolo A l'apparenza B al simbolo C l'apparenza D e cosi via. In tal modo il saluto BUONGIORNO apparirà CVPOHLPSOP. Lo stesso tipo di chiave che serve per la codifica è usata per la decodifica. La sicurezza del sistema di comunicazione è ovviamente basata sul fatto che la chiave sia segreta.

Il metodo di cifraggio usato in Internet è invece basato su un principio innovativo detto «*della chiave asimmetrica*». È una vera a propria rivoluzione in crittografia, forse la più importante di tutte. Il metodo, incorporato in tutti i browser (Netscape, Explorer, Mozilla), nei sistemi di posta elettronica e, naturalmente, nelle comunicazioni bancarie, è basato su quello proposto da Ronald Rivest, Adi Shamir e Leonard Adleman. Nel 1977 questi ricercatori del MIT proposero il metodo di codifica che ora è conosciuto col nome delle loro iniziali: RSA.

Ronald Rivest

Adi Shamir

Leonard Adleman

I ricercatori del MIT Ronald Rivest, Adi Shamir e Leonard Adleman concepirono il codice RSA nel 1977. Come è stato scoperto di recente due ricercatori della British Intelligence James Ellis e Clifford Cocks avevano trovato in precedenza un sistema di codifica basato sugli stessi principi. Tuttavia avevano tenuto segreto il risultato della loro scoperta.

Usando questo metodo il destinatario (venditore Internet) costruisce una chiave costituita da due grandi numeri naturali (N, e) che vengono spediti al computer del cliente senza preoccuparsi della sicurezza di tale spedizione, se lo desidera può persino pubblicarli nel giornale. Il computer del cliente riscrive il messaggio in forma numerica (di solito nella forma standard ASCII), ottiene un terzo numero (M) e applica una formula elementare: eleva M alla e, divide il risultato per N e calcola il resto, ottenendo il numero C che viene spedito attraverso Internet.

La cosa impressionante è che il numero C, che costituisce il messaggio codificato, (per esempio un numero di carta di credito) può essere visto da tutti. Anche conoscendo la chiave (N, e) il messaggio non è decodificabile.

E allora come lo decodifica il destinatario? Ebbene... poiché egli ha prodotto la chiave egli sa come è stata creata: scegliendo N come il prodotto di due numeri primi (quei numeri naturali più grandi di 1 che si lasciano dividere solo da 1 e da loro stessi) p e q. Conoscendoli egli produce un altro numero d tale che $(ed - 1)$ è divisibile per $(p - 1)(q - 1)$. Egli quindi eleva il numero C alla d, lo divide per N e ottiene un resto. Questo resto è il messaggio originale M! Sembra un miracolo ma non lo è. È il semplice risultato di una ingegnosa applicazione di un importante risultato della teoria dei numeri conosciuto come il teorema di Eulero.

Ciò che rende questo sistema virtualmente inattaccabile è un fatto semplicissimo: la fattorizzazione di un intero nel prodotto di primi richiede un tempo straordinariamente grande quando i numeri in questione sono abbastanza grandi. Ottenere il prodotto di due primi è facile e velocissimo. Tuttavia anche se si sa che il numero intero è il prodotto di due soli (grandi) numeri primi il trovarli rappresenta una impresa praticamente impossibile. E senza di essi il messaggio non è decifrabile.

Come spesso accade un qualsiasi progresso in tecniche crittografiche è subito seguito da un progresso in tecniche di decodifica. Il sistema RSA è stato minacciato da diversi matematici che cercano algoritmi per decifrare la chiave privata d senza conoscere la fattorizzazione in primi della chiave pubblica N. Nonostante qualche parzia-

le successo di tali tentativi, essi hanno avuto il solo risultato di convincere gli esperti a qualche sforzo ulteriore per assicurare la sicurezza del sistema. Ad oggi i matematici non hanno ancora trovato un metodo di decodifica che possa «scassinare» il sistema RSA. Il commercio online è di fatto il metodo piu sicuro per i trasferimenti di denaro.

Alice, Roberto e il ficcanaso (*).

La comunicazione via internet è basata su un meccanismo di codifica che garantisce la privacy. La matematica rende possibile tutto ciò senza che gli utenti debbano comunicarsi e neppure conoscere le chiavi di codifica.

Alice e Roberto vivono lontani e possono comunicare solo per posta. Sanno però che il postino è molto curioso e legge le loro lettere. Alice ha un messaggio per Roberto e non gradisce che venga letto da nessun altro. Che cosa può fare? Lei ha pensato di spedire il messaggio in una cassaforte chiusa da un lucchetto, ma come spedirà la chiave per aprirlo? Dopo averci pensato a lungo decide di spedire la cassaforte chiusa senza la chiave. Lei sa che Roberto è molto acuto e capirà la sua idea.

La lettera segue il suo corso e dopo qualche viaggio di andata e ritorno senza spedizione di chiavi Roberto legge il messaggio. Come può essere possibile tutto ciò? Se vi appassionano i quiz logici fermatevi qui per un po' e pensateci.

La cosa è elementare... col senno del poi. Roberto riceve la cassaforte chiusa e invece di aprirla aggiunge ad essa un suo lucchetto. Spedisce quindi la cassaforte ad Alice chiusa coi due lucchetti. Quando Alice la riceve toglie il proprio lucchetto e rispedisce la cassaforte a Roberto il quale può finalmente aprirla con la sua chiave e leggere l'atteso messaggio. Nessuna chiave è mai stata spedita e il postino non ha avuto nessuna possibilità di leggere il messaggio.

(*) L'articolo è apparso su «Expresso-revista» nel numero del 22 settembre 2001, sotto il titolo: *Alice e Bob.* Le illustrazioni sono di Fernando Gurreiro Martins.

Esso è reperibile attualmente sulla pagina web dell'European Mathematical Society: *http://pascal.iseg.utl.pt/~ncrato/EMS/Crypto2.htm* nell'edizione inglese dal titolo *Alice e Bob*; da quest'ultima abbiamo tratto la presente traduzione a opera di Pierluigi Contucci.

Come posso dire a Roberto che lo amo?

Questa storia è la riformulazione di un antico quiz logico e di una delle sue soluzioni. Essa ha ispirato i giovani americani, Whitefield Diffie, Martin Hellman e Ralph Merkle, a creare un metodo crittografico secondo il quale la segretezza della comunicazione è assicurata dall'uso di due chiavi che le due parti non si scambiano mai. Questa fu l'invenzione da cui scaturì il sistema RSA discusso nel precedente articolo.

Alice e Roberto sono personaggi fittizi ma i criptologi li usano sistematicamente. Essi rendono la storia più pittoresca di quella in cui si parla di un mittente e un destinatario o peggio ancora di generici e impersonali A e B. E anche il terzo personaggio, il postino Fick (ficcanaso), gioca un suo ruolo colorito oltre ai due protagonisti.

Prima che Diffie, Hellman e Merkle inventassero il sistema a due chiavi la trasmissione di messaggi cifrati richiedeva lo scambio di una chiave. Sarebbe stato necessario per i due protagonisti incontrarsi prima dello scambio di messaggi e duplicare la chiave da usare per aprire il lucchetto assicurandosi che nessun altro ne avesse una ulteriore copia. Solo così avrebbero potuto scambiarsi messaggi in totale privacy senza che Fick li potesse intercettare. Questo è infatti il modo in cui hanno funzionato i messaggi segreti dal tempo dei Romani all'era moderna, per le spie e gli agenti segreti, per i generali dell'esercito e per gli amanti.

Non riesco proprio ad aspettare la lettera di Alice.

L'idea di Diffie, Hellman e Merkle è veramente rivoluzionaria. La loro strategia permette ad Alice e Roberto di cominciare mettendosi d'accordo pubblicamente su due numeri e non importa che Fick ne venga a conoscenza. Poi ciascuno di loro sceglie un numero che non rivelerà a nessuno. In seguito, dopo qualche calcolo, essi ottengono lo stesso risultato: un numero che nessun altro conosce e che rappresenta la chiave per decodificare i loro messaggi. Nonostante sia molto ingegnoso tale procedimento è molto semplice (è spiegato nel riquadro). Tutto funziona come nella storia dei due lucchetti. Non c'è nessuno scambio di chiavi e ciò nonostante, sia Alice che Roberto possono aprire la cassaforte mentre Fick non può.

Utilizzando una analogia persino più calzante Simon Singh nel suo libro «The Code Book» racconta la storia di Alice e Roberto che vogliono dipingere un quadro segreto con colori che solo loro conoscono. Iniziano quindi scegliendo pubblicamente un colore di base e portandosene ciascuno a casa un litro. Alice mescola il suo litro con un altro litro di un colore segreto che non rivela a nessuno, neppure al suo ragazzo. Roberto fa la stessa cosa con un colore segreto che solo lui sa. Ognuno spedisce all'altro il proprio secchio di colore incurante che Fick lo veda. Alice aggiunge nel secchio ricevuto un litro del proprio colore segreto e Roberto fa la stessa cosa. Il colore finale che ottengono è esattamente lo stesso perché contiene una parte del colore di base, un parte del colore segreto di Alice e una

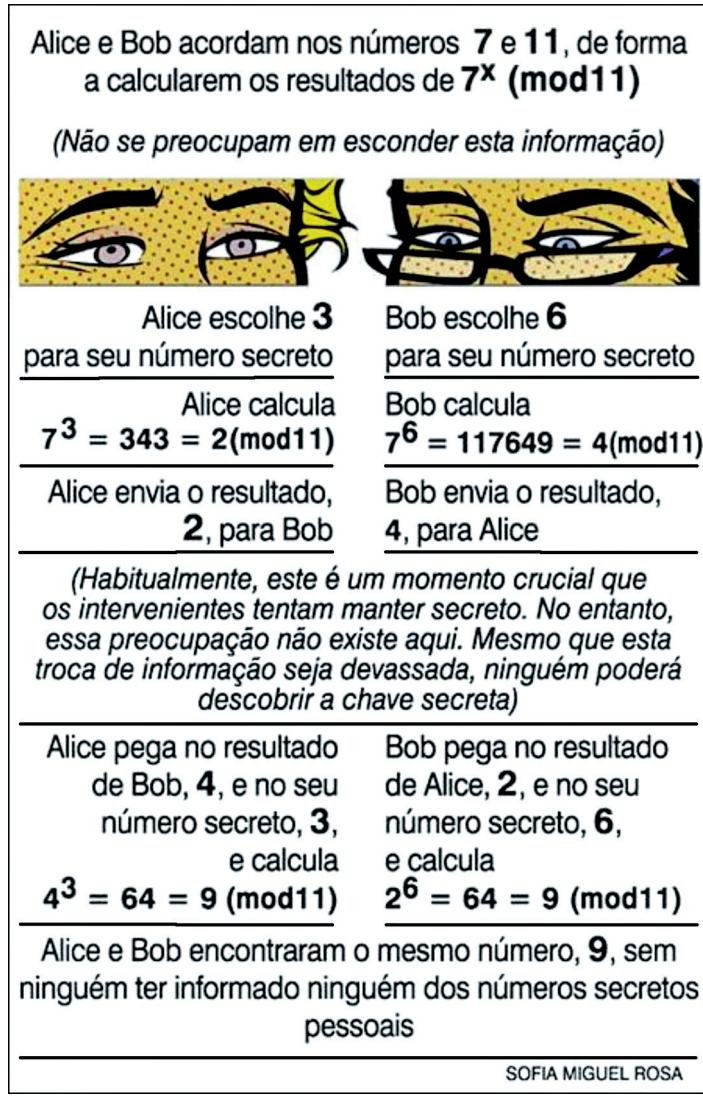
parte del colore segreto di Roberto. Ciascuno di loro non ha mai rivelato il colore segreto a nessuno, neppure all'altro e ciò nonostante ottengono alla fine lo stesso colore che nessun altro può ottenere, neppure Fick che ha che non si è mai trattenuto dal ficcare il naso nei secchi che recapitava dall'uno all'altro.

Nel sistema di trasmissione digitale ci sono i numeri naturali al posto dei colori e invece del mescolamento dei liquidi c'è il prodotto algebrico (N.d.T.: la sicurezza del codice si basa sul fatto che è in generale praticamente impossibile riconoscere i due colori componenti osservando il colore mescolato tanto quanto trovare i due primi che moltiplicati danno un certo numero naturale). Senza i risultati della crittografia il commercio e le comunicazioni via Internet non sarebbero sicure come di fatto sono.

Riquadro: Chiavi pubbliche e segrete.

La procedura inventata da Diffie, Hellman e Merkle segna la data di nascita delle chiavi pubbliche in crittografia usata in congiunzione con le chiavi segrete che non sono scambiate coi messaggi. Essa è basata sull'aritmetica modulare che essenzialmente consiste nel lavorare coi resti delle divisioni per un numero, il modulo. Un buon esempio è costituito dal nostro sistema a 12 ore. Se un orologio segna le 10 che ora segnerà 5 ore più tardi? Il risultato è ovviamente le 3, che è il resto della divisione dell'intero $10 + 5 = 15$ per il numero 12. In matematica si scrive $10 + 5 = 3 \pmod{12}$. Con questa notazione descriviamo come segue la procedura seguita da Alice e Roberto come suggerito da Simon Singh. I nostri due amici sono capaci di accordarsi su una comune chiave crittografica senza peraltro doversela mai scambiare e senza che nessuno abbia la possibilità di scoprirla.

Alice e Roberto si mettono d'accordo sui numeri 7 e 11 e si preparano a eseguire l'operazione $7^{\times} \pmod{11}$. Questa informazione è pubblicamente nota. Alice sceglie il 3 come suo numero segreto e Roberto il 6. La prima esegue il calcolo $7^3 = 343 = 2 \pmod{11}$, il secondo $7^6 = 117649 = 4 \pmod{11}$. Alice spedisce il suo risultato (il numero 2) a Roberto e questo spedisce il numero 4 ad Alice. Fick può



osservare sia il 2 che il 4. Alice prende il numero avuto da Roberto e calcola $4^3 = 64 = 9 \pmod{11}$ e Roberto similmente $2^6 = 64 = 9 \pmod{11}$. Entrambi ottengono lo stesso risultato senza essersi rivelati i numeri segreti.

Crittografia quantistica (*).

Sembra fantascienza ma è realtà: le proprietà più bizzarre delle particelle subatomiche ci permettono di creare codici crittografici sicuri.

La sicurezza delle transazioni bancarie, del commercio on line e delle trasmissioni di posta elettronica è basata sui più sicuri metodi crittografici esistenti; «più sicuri» ovviamente non significa «infallibili». La sicurezza di uno dei più affidabili sistemi moderni di crittorgrafia, il cosiddetto RSA che abbiamo discusso nei due precedenti articoli, è basato sulla difficoltà di trovare i fattori primi di numeri molto grandi. Non si conoscono algoritmi in grado di eseguire questa operazione in un tempo ragionevole neppure utilizzando i più potenti calcolatori a nostra disposizione. Tuttavia se un matematico scoprisse un processo in grado di accelerare la fattorizzazione in primi o se una nuova generazione di calcolatori quali quelli quantistici venisse commercializzata ([1]) il mondo delle comunicazioni cosi come lo conosciamo oggi sarebbe seriamente minacciato. Nel caso in cui una di queste rivoluzioni scientifiche o tecnologiche divenisse reale il commercio elettronico cesserebbe di essere sicuro, le forze

(*) L'articolo è apparso su «Expresso-revista» nel numero del 29 settembre 2001, sotto il titolo: *Criptografia quântica*. Esso è reperebile attualmente sulla pagina web dell' European Mathematical Society:
http://pascal.iseg.utl.pt/~ncrato/EMS/Crypto3.htm
nell' edizione inglese dal titolo *Quantum Cryptography*; da quest'ultima abbiamo tratto la presente traduzione a opera di Pierluigi Contucci.

([1]) Il fatto che un computer quantistico possa decomporre velocemente in primi un intero è una conseguenza di risultati di Peter Shor che ha ricevuto per essi il Premio Nevanlinna nel 1998. Sul calcolo quantistico e le sue applicazioni anche al problema della decomposizione di un intero in fattori primi, il lettore può utilmente leggere l'articolo di Mario Rasetti, *Il calcolo quantistico: una sfida per la matematica del 2000*, su questa rivista, Serie VIII, Vol. III-A, Agosto 2000, 201-222 (N.d.T.).

armate dovrebbero inventarsi nuovi sistemi di comunicazione e le istituzioni bancarie tornerebbero a fare transazioni di denaro secondo gli antichi e lenti metodi. Tutto ciò significherebbe il collasso della tecnologia dell'informazione nella società di oggi.

Non sorprende quindi che si stia cercando un nuovo sistema criptologico che possa essere sicuro anche nell'eventualità considerate e i matematici, i fisici e gli informatici ci stanno lavorando già da tempo. La possibilità teorica di sviluppare un tale sistema è basata sulle più profonde leggi a cui è sottoposta la struttura della materia, quelle che governano la cosiddetta «indeterminazione» della realtà quantistica. L'impossibilità concettuale e non solo sperimentale di conoscere a priori le proprietà delle particelle elementari costituirà la garanzia di sicurezza della comunicazione.

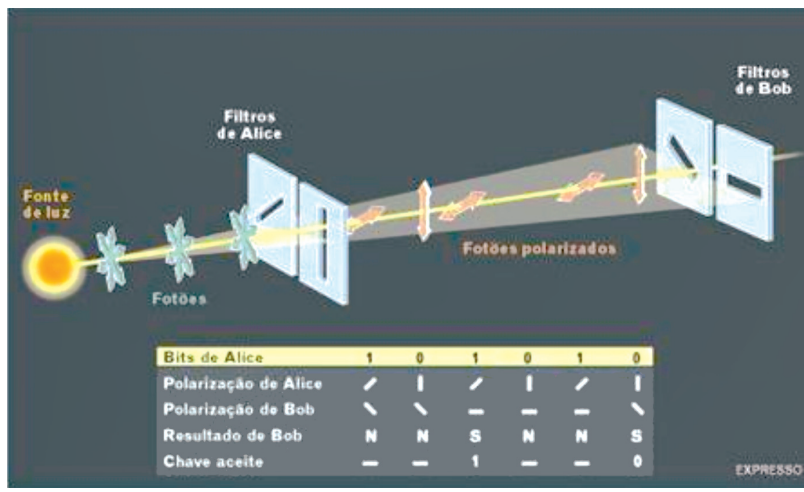
Una simile idea è maturata nelle menti degli scienziati ormai da tempo. Charles Bennet, un informatico del Centro Ricerche Watson della IBM è stato uno di quelli che hanno cercato a lungo una soluzione di questo problema. Finalmente negli anni 80 lui e il suo collega Gilles Brassard sono riusciti a concepire un sistema crittografico quantistico. Le loro idee sono rimaste pure speculazioni per un tempo molto lungo ma negli ultimi due anni i progressi tecnologici e scientifici hanno reso possibile la costruzione di prototipi di sistemi quantistici la cui sicurezza sembra essere assolutamente a prova di scasso.

Nel discutere le questioni legate ai messaggi cifrati gli esperti usano i tre personaggi di Alice, Roberto e Fick. La prima è il mittente, il secondo il destinatario e il terzo l'intruso ficcanaso che cerca con ogni mezzo di violare la segretezza della comunicazione. Nel cuore del processo proposto da Charles Bennet e i suoi collaboratori c'è la chiave di un codice casuale che viene aggiunto al messaggio stesso. Questa chiave è un numero in rappresentazione binaria, cioè una sequenza di 0 e di 1 che inizia con un 1. Alice comincia col trasformare il testo letterale che vuole spedire a Roberto traducendolo in un numero in forma binaria. Quindi somma il numero chiave al suo numero e spedisce il risultato a Roberto che possiede la chiave usata da Alice. Sottraendo il numero chiave dal numero ricevuto egli è in grado di ottenere il messaggio originale semplicemente ristra-

sformando in lettere la stringa binaria ottenuta, una procedura che ogni computer è perfettamente in grado di eseguire.

La sicurezza di questo sistema è completamente basata sul fatto che la chiave è una sequenza casuale di zeri e uni e che viene utilizzate una sola volta. Di solito questo significa che quelle cifre devono essere generate in anticipo e che Alice deve spedirle a Roberto. E questo è il punto in cui sorgono problemi. Ma se Alice e Roberto non si incontrano mai, come accade nel commercio on line, devono scambiarsi la chiave attraverso il canale di comunicazione. E come possono fare? Certo potrebbero mettersi d'accordo su un'altra chiave ma questo non risolve ancora il problema perché per farlo dovrebbero incontrarsi o fidarsi del messaggero... ma Fick col suo modo di ficcare il naso ovunque rende la fiducia impossibile.

A questo punto entra in scena il mondo quantistico per mano di Charles Bennet ed altri informatici. Questo è uno strano mondo le cui regole sono difficili da capire se ci basiamo troppo sulla nostra esperienza quotidiana. Una di queste regole è l'indeterminazione ed essa non dipende dalla nostra scarsa conoscenza ma è una proprietà intrinseca delle particelle. Come può essere usato tutto questo al fine di produrre comunicazioni sicure?



Per creare il codice random Alice comincia con lo spedire a Roberto una sequenza di particelle di luce, dei fotoni. Lei ha due polarizzatori nel suo sistema, uno orientato verticalmente e l'altro inclinato di 45 gradi, come rappresentato in figura. Per produrre la chiave lei alterna in modo random i polarizzatori e, per esempio, fa corrispondere lo zero a un fotone polarizzato verticalmente a l'uno a quello polarizzato a 45 gradi. Roberto ha a sua volta due polarizzatori: uno orizzontale e l'altro inclinato a 45 gradi. Quando egli riceve i fotoni di Alice li fa passare attraverso i suoi polarizzatori scegliendone di volta in volta uno in modo del tutto casuale. I fotoni che Alice spedisce arrivano o meno a Roberto a seconda della scelta di orientamento dei polarizzatori. Se Alice spedisce un fotone polarizzato verticalmente e Roberto sceglie il polarizzatore orizzontale la particella non passa. Lo stesso accade se Alice spedisce a Roberto un fotone polarizzato a 45 gradi e Roberto sceglie il polarizzatore a -45 gradi. In generale due polarizzatori perpendicolari in successione fermano la paticella.

La sorpresa sorge quando Alice spedisce un fotone polarizzato verticalmente e Roberto sceglie il polarizzatore diagonale oppure quando Alice spedisce un fotone polarizzato diagonalmente e Roberto sceglie un polarizzatore orizzontale, cioè quando i polarizzatori dei due formano un angolo di 45 gradi. In questo caso infatti il principio di indeterminazione della meccanica quantistica entra in gioco: la metà delle particelle raggiunge Roberto mentre l'altra metà non passa. E ciò accade senza che ci sia nessun modo di sapere a priori quali particelle arriveranno al destinatario e quali no. In tale circostanza solo Alice conosce la polarizzazione dei fotoni che ha spedito. E solo Roberto conosce quali di essi sono giunti sino a lui. In questo modo Roberto scopre la polarizzazione scelta da Alice per i fotoni che sono passati. Se infatti un fotone gli arriva attraverso il filtro diagonale significa che Alice aveva il filtro verticale che significa 0. Se tuttavia un fotone arriva attraverso il filtro orizzontale Alice deve aver usato il polarizzatore diagonale che significa 1. I fotoni che non sono passati rimangono invece un mistero per Roberto. A questo punto Alice deve sapere quali fotoni hanno raggiunto Roberto. Per acquisire questa conoscenza i due possono comunicare attraverso

canali convenzionali e possono persino permettersi di essere ascoltati da Fick. Infatti anche se questo scopre quali particelle hanno raggiuinto Roberto non avrà nessun modo di sapere quali filtri sono stati usati. La chiave quindi è stabilita dai soli fotoni che sono giunti a destinazione. I due pertanto stanno comunicando in completa sicurezza e privacy. L'indeterminazione del mondo quantistico fornisce loro la certezza che il loro codice non può essere violato.

Forse non siamo lontani dall'implementare un sistema crittografico siffatto. Solo alcuni anni fa tutto ciò sembrava fantascienza ma alcuni progressi tecnologici recenti hanno reso possibile la creazione di prototipi di modelli computazionali le cui applicazioni a tali idee risultano accessibili. Possiamo subito anticipare che le difficoltà tecnologiche da superare sono enormi. Come trasmettiamo la luce un fotone alla volta? Come possiamo essere sicuri che ciascun fotone polarizzato raggiunge il secondo filtro? Questi problemi sono affrontati passo dopo passo e lentamente risolti. Siamo già in grado di utilizzare la crittografia quantistica attraverso fibre ottiche e persino attraverso l'atmosfera per qualche chilometro. Il tutto fa sperare che potremmo non essere lontani dal riuscire a proteggere i nostri segreti semplicemente facendoli viaggiare, una particella alla volta, alla velocità della luce.