

LA MODERNA CRITTOGRAFIA
può mettere al sicuro i dati sensibili delle persone anche se si espongono ai pericoli di Internet.

Kenn Brown Mondolithic Studios

COME MANTENERE UN SEGRETO

Numerose tecniche di calcolo possono proteggere la privacy delle nostre informazioni e attività su Internet con il grado di accuratezza che vogliamo

di Anna Lysyanskaya

Paolo ha deciso di provare il servizio di appuntamenti *on line* Chix-n-Studz.com. Per ottenere un *account* sul sito web compila diversi moduli, fornendo i dettagli personali e le caratteristiche che cerca in un potenziale partner. In breve tempo il servizio gli offre una gamma di possibili cuori solitari compatibili, e tra questi un profilo molto promettente, quello di Vanessa. Così Paolo le spedisce il suo indirizzo di posta elettronica, sperando di aver scritto un messaggio accattivante. Lei risponde, e comincia un turbinoso epistolario digitale.

Povero Paolo. Presto riceve anche numerose telefonate non richieste da parte di gruppi politici e venditori che sembrano sapere tutto su di lui, mentre la sua assicurazione sanitaria lo interroga sulle vacanze estremamente avventurose. È facile intuire che i proprietari poco scrupolosi della Chix-n-Studz vendono informazioni che riguardano i loro clienti. In più c'è Ivan, un collega dispettoso, al quale Paolo mostra una delle e-mail di Vanessa. Paolo non sa che molti messaggi con Vanessa come mittente sono, in realtà, scherzi di Ivan.

Alice, invece, è felice di avere un nuovo amico, Bruno. I due si sono incontrati grazie a SophistiCats.com, un servizio di incontri on line che offre tutti i più recenti strumenti crittografici. Alice entra nel suo sito web protetto da autorizzazione anonima, cioè un sistema grazie a cui non si può tracciare la persona che accede al sito. SophistiCats usa un programma che fa combaciare il profilo e i criteri di Alice per la scelta del partner con quelli di Bruno, in modo che nessuno all'interno del servizio possa conoscere le informazioni che li riguardano o sapere se i due sono compatibili. È difficile immaginare un sistema di appuntamenti così efficace, che non sa praticamente nulla dei suoi clienti!

Alice ha contattato Bruno usando un'opzione conosciuta come «canale anonimo», e lui ha risposto in modo simile: neanche l'Internet Service Provider (ISP) di Alice, ovvero l'azienda che le fornisce l'accesso alla rete, sa che Bruno è il suo contatto e che cosa si dicono. E l'ISP di Bruno non è certo meglio informato. Tuttavia la coinquilina di Alice, Eva, sa di Bruno, ma solo perché Alice ne ha parlato e ha stampato alcuni suoi messaggi, attaccandoli sul computer. Eva potrebbe essere un problema, perché, essendo un'esperta di computer e reti, è in grado di intercettare e modificare dati che entrano ed escono dal computer di Alice (in pratica Eva controlla la rete che connette entrambe a Internet). Niente paura: la crittazione assicura che Eva conosca solo le informazioni comunicatele da Alice, e le «firme digitali» codificate nelle e-mail di Bruno e Alice riescono facilmente a rivelare e ignorare i messaggi ingannevoli di Eva.

Tutto criptato

Come Alice e Paolo, molti di noi conducono per via telematica numerose attività che riguardano la loro vita personale e lavorativa. Facciamo tante cose on line che ottenere informazioni dettagliate sulla maggior parte delle persone è facile quanto raccogliere, o registrare, le loro attività in rete.

IN SINTESI

- La moderna crittografia offre un'ampia gamma di strumenti matematici per proteggere privacy e sicurezza, che vanno ben oltre l'antica arte di criptare i messaggi.
- È possibile impedire ad altri di conoscere quello che stiamo dicendo e a chi.
- È possibile restare anonimi anche nelle attività on line che richiedono una sottoscrizione e informazioni personali.
- I gruppi possono calcolare praticamente ogni cosa partendo da dati dei loro membri (come il vincitore di un'elezione per cui votano) senza rivelare nulla dei dati individuali.

E per varie ragioni, gli ISP stanno già registrando dati sulle nostre attività, quali siti abbiamo visitato e quando. Ma non sono soli. Anche molti soggetti con cui interagiamo virtualmente - negozi, giornali, siti di appuntamenti e così via - mantengono schede accurate su di noi. Quindi, se riteniamo che la privacy sia un bene prezioso, dobbiamo affrontare la sfida di come trarre vantaggio da quello che ci offre Internet ma senza rinunciare alla nostra privacy.

Una scoperta sbalorditiva della moderna crittografia è che praticamente tutte le attività che coinvolgono la comunicazione elettronica si possono svolgere in forma anonima. Molte persone, compresi diversi editori di dizionari, pensano erroneamente che «crittografia» sia sinonimo di «studio della crittazione». Ma la moderna crittografia è molto di più: fornisce metodi matematici che consentono di proteggere comunicazioni e calcolo da qualsiasi comportamento fraudolento, fornendo quindi anche strumenti per proteggere la nostra privacy e la nostra sicurezza.

Si supponga, per esempio, che tutti i membri di un gruppo che comunicano usando Internet vogliano fare un calcolo basato su dati che provengono da ciascuno di loro e che devono rimanere riservati. I dati potrebbero essere i voti di un'elezione, e il risultato l'esito della votazione, che però non riveli i voti individuali. Una procedura nota come calcolo *multiparty* o valutazione della funzione di sicurezza, *secure function evaluation* (SFE), consente di registrare i voti in modo che ciascun partecipante apprenda il risultato esatto senza conoscere il voto di un altro membro del gruppo. Questa stessa procedura impedisce anche a eventuali intrusi di intercettare e manipolare i voti dei membri. Inoltre il protocollo SFE può fornire a ogni individuo un risultato personale, come nel caso del servizio di SophistiCats.

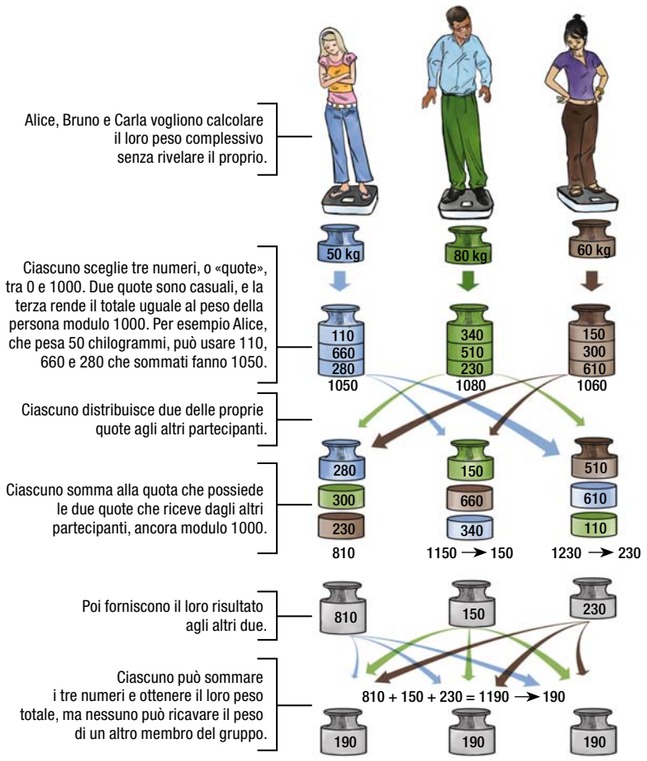
L'idea alla base della SFE è che il dato proveniente da ciascun membro è diviso in parti, o quote, e distribuito tra gli altri membri del gruppo. Ogni membro quindi elabora le quote (sommandole, ridistribuendole e così via) sotto il suo controllo. Infine il gruppo rimette insieme i pezzi per ottenere il risultato. In questo modo nessuno è mai in possesso delle informazioni necessarie per ricostruire i dati immessi da un'altra persona (*si veda il box in questa pagina*).

Potrebbe non sorprendere che una funzione così semplice come la somma di voti sia considerata sicura, ma ricordiamo quello che ha fatto SophistiCats per Alice: scegliendo tra migliaia di utenti, ha individuato quali potessero andare bene ad Alice, dandole scarne informazioni sulle affinità, il tutto senza sapere nulla sul suo profilo o su quello di qualsiasi altro utente. Anche un'organizzazione tipo Grande Fratello che intercettasse il traffico della rete o combinasse i dati dei dischi rigidi della SophistiCats non ricaverebbe alcuna informazione.

SophistiCats è un servizio immaginario, ma gli specialisti di crittografia hanno già mostrato come metterlo in pratica. Nel gennaio di quest'anno il protocollo SFE è stato usato in Danimarca per un problema pratico: fissare il prezzo per gli scambi della barbabietola da zucchero con un accordo tra circa 1200 agricoltori danesi, basandosi sulle offerte fatte da ciascun agricoltore. Con SFE è possibile che tutti abbiano i servizi che desiderano senza sacrificare la privacy.

Calcolare insieme

La valutazione della funzione di sicurezza consente a un gruppo di fare calcoli partendo dai dati dei singoli, ma impedendo ai singoli di conoscere i dati altrui.



Una procedura più complicata consente ai gruppi di moltiplicare tra loro i numeri privati. Sommando e moltiplicando bit, è possibile calcolare qualunque cosa si possa valutare dai loro dati grazie all'uso del computer. L'intero sistema salvaguarda anche le persone dalla deviazione dalle regole.

LA STORIA IN PILLOLE (I)

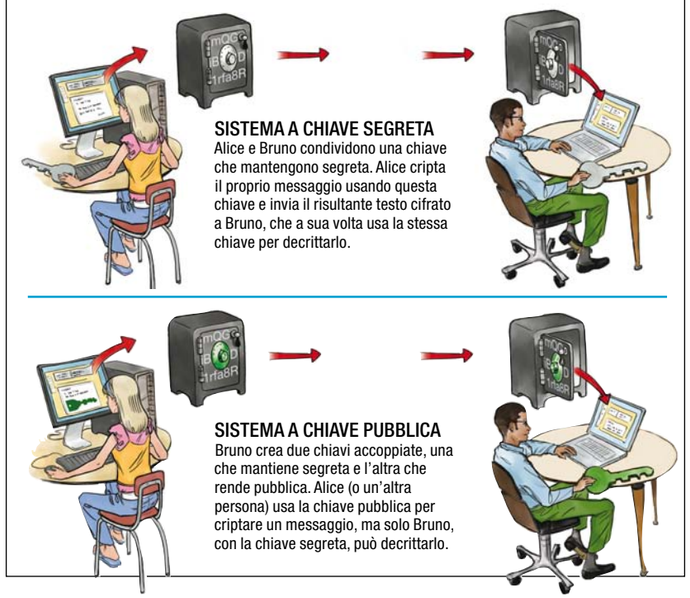
800 d.C.: al-Kindi, studioso e matematico arabo che vive a Baghdad, scrive il *Manoscritto sulla decifrazione dei messaggi criptati*. Si tratta della prima descrizione nota dell'analisi della frequenza e di altre tecniche di crittoanalisi.

1586: Thomas Phelippes usa l'analisi della frequenza per decrittare messaggi tra Maria I di Scozia e i cospiratori contro Elisabetta I d'Inghilterra. Maria e i cospiratori vengono giustiziati.

Matt Collins

Nascondere il contenuto

Le moderne tecniche di crittazione dell'informazione sono di due tipi: a chiave segreta e a chiave pubblica.



Anche se il protocollo SFE rende possibile un'ampia gamma di funzionalità, la sua potenza e universalità ha un prezzo: richiede un'enorme quantità di calcolo e comunicazione. Il protocollo è efficiente per compiti speciali come le elezioni, ma è troppo ingombrante per essere inserito in un servizio ogni volta che si clicca su un link a una pagina sicura. Per questo gli studiosi di informatica hanno sviluppato protocolli più efficienti, per i compiti comuni. Tra questi ricordiamo:

Crittazione. L'ISP di Alice e quello di Eva non possono decifrare i messaggi che Alice invia a Bruno. Anche il traffico tra il computer di Alice e la SophistiCats è sicuro.

Autenticazione. Alice può essere sicura che i messaggi arrivino da Bruno e non da Eva.

Canali anonimi. L'ISP di Alice non può conoscere il destinatario dei suoi messaggi o se Alice ha visitato il sito SophistiCats.

Dimostrazione a conoscenza zero. Alice può dimostrare a un'altra persona che una cosa è vera senza rivelare nulla delle prove che ha.

Autorizzazione anonima. La SophistiCats sa che Alice è iscritta quando accede al sito Web, ma non è in grado di dire chi sia. Questo protocollo è un caso speciale della prova a conoscenza zero.

Matt Collins

LA STORIA IN PILLOLE (II)

1918: Il maggiore dell'Esercito degli Stati Uniti Joseph O. Mauborgne e Gilbert Vernam, degli AT&T Bell Laboratories, inventano il *one-time pad*, un sistema crittografico in cui una chiave segreta casuale è lunga quanto lo stesso messaggio e viene usata una sola volta.

1944: A Bletchley Park, in Inghilterra, il Colossus (la prima macchina di calcolo programmabile) decritta i messaggi dell'Alto comando tedesco fornendo preziose informazioni prima dello sbarco in Normandia.

1948: Claude Shannon degli AT&T Bell Laboratories dimostra che il one-time pad è inviolabile anche per chi ha potenza di calcolo illimitata. Ma la definizione di segretezza è così stretta che Shannon dimostra anche che il one-time-pad è l'unico sistema crittografico in grado di soddisfarla.

Messaggi segreti

Il problema più vecchio e tra i più fondamentali studiati in crittografia è la crittazione: come comunicare in modo sicuro su un canale insicuro, cioè che può essere spiato. Alice vuole inviare un messaggio a Bruno ma Eva controlla parte del canale usato da Alice, cioè la rete della casa. Alice vuole che Bruno possa leggere il messaggio, ma non Eva.

Nell'analizzare questo problema si noti, in primo luogo, che Bruno deve sapere qualcosa che Eva non sa, altrimenti Eva sarebbe in grado di fare tutto ciò che è in grado di fare Bruno. L'elemento riservato di Bruno è la sua chiave segreta (CS). In seconda battuta, occorre notare che Alice deve conoscere qualcosa della CS di Bruno in modo da creare un messaggio criptato per Bruno. Se Alice conosce la CS, il protocollo è chiamato crittazione a chiave segreta, un tipo di crittazione usato da secoli.

Nel 1976 Whitfield Diffie e Martin E. Hellman, entrambi alla Stanford University, intuirono un'altra possibilità, chiamata crittazione a chiave pubblica, in cui Alice non deve necessariamente conoscere la CS. Tutto ciò che le occorre è un valore pubblico collegato alla CS chiamato chiave pubblica (CP) di Bruno. Alice usa la CP di Bruno per criptare il messaggio, e solo Bruno, con la sua CS, può decrittare il testo cifrato (*si veda il box in questa pagina*). Non importa che anche Eva conosca la CP di Bruno, poiché non può usarla per decifrare il testo. Diffie e Hellman proposero l'idea della CP, ma non sapevano come produrla. Un anno dopo Ronald L. Rivest, Adi Shamir e Leonard M. Adleman, tutti del Massachusetts Institute of Technology, pubblicarono la prima costruzione di un sistema di crittazione a chiave pubblica: l'algoritmo RSA.

Il loro algoritmo funziona per la crittazione pubblica perché coinvolge la cosiddetta funzione *trapdoor* (letteralmente «botola» o «trabocchetto», N.d.t.). Questa funzione è facile da calcolare per produrre il testo cifrato, ma difficile da invertire per recuperare il testo in chiaro, a meno che non venga usata una trapdoor speciale. La trapdoor serve da chiave segreta. L'algoritmo RSA è stato il primo esempio di funzione con proprietà di tipo trapdoor. Per questo risultato, nel 2002 gli studiosi hanno vinto il premio Turing, il riconoscimento più prestigioso nel campo dell'informatica.

La scoperta di Rivest, Shamir e Adleman, salutata come un progresso fondamentale per la crittografia, stimolò negli anni successivi la ricerca in questo campo. Sono ancora molti gli obiettivi da raggiungere: trovare nuove funzioni trapdoor,

studiare i postulati matematici su cui è basata la sicurezza di una specifica funzione, definire precisamente ciò che è richiesto per considerare sicuro ogni sistema di crittazione.

La crittazione a chiave pubblica permette l'acquisto on line di prodotti senza inviare informazioni sensibili come i numeri della carta di credito in chiaro. Il *browser* del cliente riveste il ruolo di Bruno. Più in generale, il protocollo HTTPS, che la maggior parte dei browser ora supporta, usa la crittazione a chiave pubblica per fornire ai browser web un canale criptato. Molte persone usano la crittazione a chiave pubblica anche per messaggi di posta elettronica. Sono numerosi i programmi dedicati a questo scopo. Se non si cripta l'e-mail, il messaggio viaggia su Internet in una forma facile da leggere e che potrebbe rimanere tale in vari dischi rigidi lungo il percorso per un certo periodo di tempo.

Ciao, sono io!

Il problema dell'autenticazione è strettamente collegato a quello della crittazione. Si supponga che Alice riceva il messaggio: «Alice, per favore invia 100 dollari a Eva. Con amore, Bruno». In che modo potrebbe sapere se proviene effettivamente dal suo fidanzato Bruno e non da Eva?

Come nel caso della crittazione, Bruno deve sapere qualcosa che Eva non sa, in modo che Bruno, e non Eva, possa produrre un messaggio che Alice accetterà. Anche in questo caso Bruno ha bisogno di una chiave segreta. Inoltre Alice deve sapere qualcosa della CS di Bruno per verificare se un messaggio provenga effettivamente da lui. Ancora una volta ci sono due tipi di protocolli: l'autenticazione a chiave segreta, nota come codice di autenticazione del messaggio, e l'autenticazione a chiave pubblica, spesso indicata come schema di firma digitale. Diffie e Hellman per primi hanno immaginato gli schemi di firma digitale nel periodo in cui hanno proposto la crittazione a chiave pubblica, e lo schema che usa l'algoritmo RSA è stato il primo a essere costruito.

L'idea è che Bruno usi la CS per calcolare una «firma» che allega al suo messaggio e che Alice, o altri destinatari, si serva della sua CS per verificare che vada bene per il messaggio (*si veda il box in questa pagina*). Alice sa che il messaggio deve provenire da Bruno, perché nessun altro ha la CS necessaria per produrre una firma valida.

Oggi è facile indurre un programma di posta elettronica a «credere» che un messaggio provenga da Bruno quando in effetti proviene da Eva. Una e-mail fraudolenta può contenere notizie false e quotazioni di borsa non corrette, inducendo le persone ad agire contro il proprio interesse. Ma se tutta la comunicazione via e-mail fosse autenticata un simile attacco sarebbe impossibile: il vostro programma di posta elettronica firmerebbe tutti i messaggi in uscita e verificherebbe le firme digitali di tutti i messaggi in entrata.

L'autenticazione potrebbe anche combattere lo *spam*, grazie a server che rifiutano e-mail in arrivo non autenticate dal mittente. I protocolli di autenticazione non esistevano negli anni settanta, quando sono state sviluppate le e-mail, e molte convenzioni di quell'epoca sono ancora in uso, anche se sono disponibili gratuitamente programmi che tutti possono usare per firmare le proprie mail e verificare le firme.

L'ispirazione della cipolla

Criptando i propri messaggi, è possibile impedire che l'ISP (o qualunque altra spia) scopra che cosa si invia e si riceve, ma non chi si sta comunicando. Per esempio l'ISP di Alice sa perfettamente se frequenta un sito web di alcolisti anonimi. Si immagini che cosa accadrebbe se l'ISP vendesse l'informazione alle compagnie di assicurazione per auto. Le persone cercherebbero meno polizze on line perché sarebbero preoccupate del rischio di pagare premi più alti.

Questo problema si potrebbe risolvere con SFE: il dato privato in ingresso di Alice sarebbe l'indirizzo del sito a cui vorrebbe collegarsi e i dati privati in entrata sarebbero i contenuti della pagina Web. L'uso di SFE, tuttavia, sarebbe estremamente inefficiente. Nel 1981 David Chaum, allora all'Università della California a Berkeley, propose una soluzione più semplice, i canali anonimi, ora nota come instradamento a cipolla (*onion routing*).

Come suggerisce il nome, Alice struttura il proprio messaggio in una successione di strati. Ogni strato, e ogni elemento al suo interno, viene criptato da Alice con le differenti chiavi pubbliche di diverse persone. Poi Alice aggiunge l'indirizzo di ciascuna persona all'esterno di ogni strato. Un messaggio da Alice a Bruno potrebbe viaggiare così: Alice invia la cipolla a Marco, il quale può levarne lo strato più esterno decrittando la cipolla con la propria chiave segreta. All'interno, Marco trova una cipolla più piccola e l'indirizzo di Lisa. Marco inoltra questa cipolla a Lisa, che può decrittare con la propria chiave e così via. Alla fine della catena Bruno riceve il «cuore» della cipolla e lo decifra per trovare il messaggio di Alice.

In pratica gli intermediari sono parte di una rete di computer realizzata per gestire la decrittazione e inoltrarla in automatico. Idealmente, ogni intermediario riceve di continuo diverse cipolle e le inoltra in ordine sparso. A patto che nella rete ci sia traffico sufficiente, un ISP che intercetta senza sosta gli intermediari non può conoscere la destinazione del messaggio di Alice o la provenienza di quello di Bruno.

Lo stesso Bruno non sa chi ha spedito il messaggio, a meno che Alice non scelga di rivelare la propria identità. Ma anche se Alice resta anonima Bruno può inviarle una risposta anonima, basta che Alice includa una «cipolla di risposta» con gli strati di indirizzi e le chiavi pubbliche necessarie per instradare un messaggio di risposta.

I messaggi di Alice e Bruno possono rima-

LA STORIA IN PILLOLE (III)

1976: Whitfield Diffie e Martin E. Hellman, entrambi della Stanford University, propongono la crittazione e l'autenticazione a chiave pubblica.

1977: Ronald L. Rivest, Adi Shamir e Leonard M. Adleman, del Massachusetts Institute of Technology, costruiscono il primo sistema di crittografia a chiave pubblica: nasce l'algoritmo RSA.

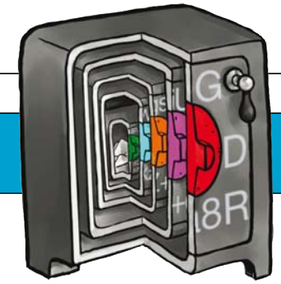
Agosto 1977: In una rubrica di Martin Gardner su «Scientific American», Rivest e collaboratori sfidano i lettori a decifrare un messaggio criptato con l'algoritmo RSA con una chiave a 129 cifre. Gli stessi autori stimano in 40 milioni di miliardi di anni il tempo necessario per l'operazione.

LA STORIA IN PILLOLE (IV)

1982: Shafi Goldwasser dell'Università della California a Berkeley e Silvio Micali del MIT sviluppano le definizioni fondamentali della moderna crittografia, inclusa una definizione pratica di sicurezza.

1985: Goldwasser, Micali e Charles Rackoff, dell'Università di Toronto, inventano la dimostrazione a conoscenza zero. Un anno dopo gli israeliani Oded Goldreich e Avi Wigderson, la applicano alla tricolorabilità dei grafi.

1987: Goldreich, Micali e Wigderson elaborano i protocolli per la *multiparty computation*, costruendo un protocollo in due parti sviluppato da Andrew C. Yao della Princeton University.

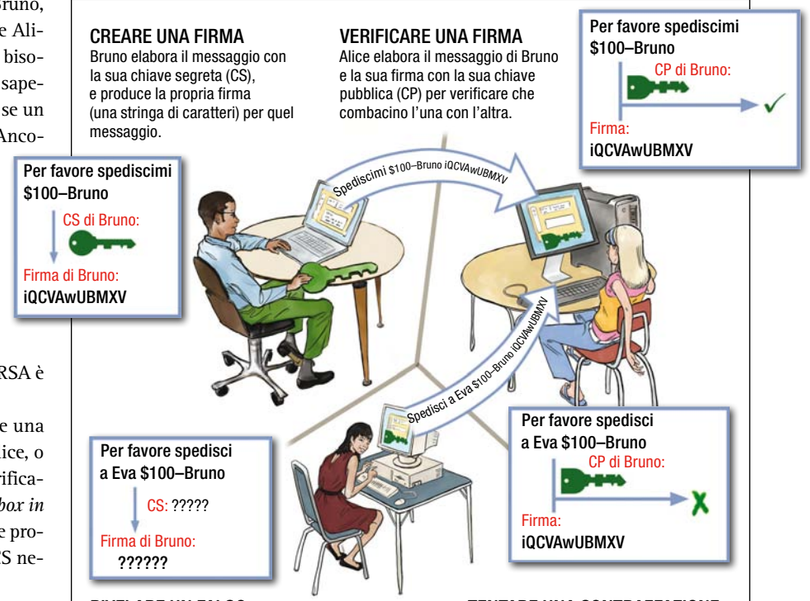


Firmare un messaggio

Una firma digitale garantisce che un messaggio provenga da una specifica persona e sia inalterato.

CREARE UNA FIRMA
Bruno elabora il messaggio con la sua chiave segreta (CS), e produce la propria firma (una stringa di caratteri) per quel messaggio.

VERIFICARE UNA FIRMA
Alice elabora il messaggio di Bruno e la sua firma con la sua chiave pubblica (CP) per verificare che combacino l'una con l'altra.



RIVELARE UN FALSO
Eva non può produrre la firma corretta «Bruno» da apporre al suo messaggio contraffatto senza la chiave segreta di Bruno.

TENTARE UNA CONTRAFFAZIONE
Alice sa di ricevere un messaggio falso quando usa la CP di Bruno per far combaciare il messaggio con la firma.

Matt Collins

Nascondere le connessioni

I dati si possono inviare in forma anonima usando un «instradamento a cipolla» (*onion routing*), in cui i dati stessi e il percorso che prenderanno sono strutturati in strati di crittazione multipli.

INVIARE UNA «CIPOLLA»
Alice prepara il suo messaggio criptandolo con una serie di chiavi pubbliche che producono una cipolla con molti strati di crittazione. Oltre a ciò, inserisce le istruzioni di instradamento negli strati.

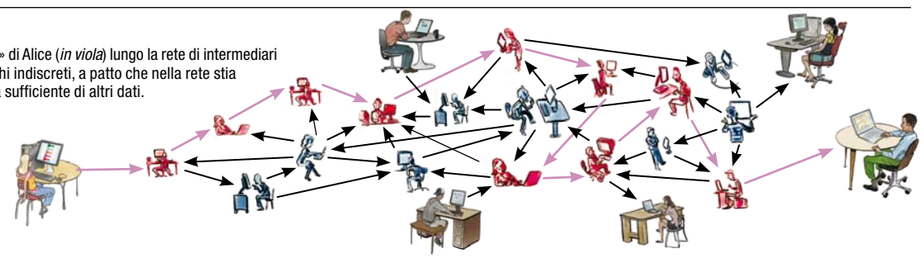


Poi invia la cipolla a Marco, la cui chiave segreta decifra lo strato più esterno della crittazione. All'«interno», Marco trova una cipolla indirizzata a Lisa, alla quale inoltra la cipolla.

La chiave segreta di Lisa rimuove lo strato successivo della cipolla, e all'interno Lisa trova un altro indirizzo per la cipolla, a cui quest'ultima viene inoltrata, e così via.

Infine, Tommaso scopre il nucleo della cipolla e lo invia a Bruno, che lo apre con la sua chiave segreta per trovare il messaggio. Nessuno tranne Alice conosce il cammino completo della cipolla.

LA RETE
Il cammino della «cipolla» di Alice (*in viola*) lungo la rete di intermediari (*in blu*) è nascosto a occhi indiscreti, a patto che nella rete stia transitando una quantità sufficiente di altri dati.



Matt Collins

L'AUTORE



ANNA LYSYANSKAYA è professore associato di informatica alla Brown University ed è membro della Sloan Foundation. Ha conseguito il PhD al Massachusetts Institute of Technology, con la supervisione di Ronald I. Rivest, dal quale deriva la «R» della crittazione RSA. Gli schemi di firme e i protocolli di autorizzazione anonima della sua tesi fanno parte del Trusted Computing Group Standard. Se negli ultimi due anni avete acquistato un computer nuovo, allora è probabile che questi schemi e protocolli siano integrati nel suo microprocessore.

LA STORIA IN PILLOLE

1994: La Netscape Communications pubblica il protocollo Secure Sockets Layer, che impiega la crittazione a chiave pubblica per assicurare la sicurezza delle transazioni sul World Wide Web.

1994: Arjen K. Lenstra della Bell Communications Research e oltre 600 volontari su Internet, usando circa 1600 computer, sviluppano algoritmi di fattorizzazione impiegando otto mesi per fattorizzare la chiave RSA a 129 cifre di Gardner, rivelando il messaggio «THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE», ovvero «Le parole magiche sono avvoltoio schizzinoso».

2008: Occorrerebbe più di un milione di miliardi di anni per violare una chiave RSA di lunghezza raccomandata (2048 bit) su un moderno PC.

nere non tracciabili anche se alcuni intermediari lasciano trapelare informazioni su quello che stanno facendo. Più persone usano questo sistema, offrendo volontariamente i loro computer come intermediari, più diventa difficile sapere chi sta comunicando e con chi.

Per quanto riguarda crittazione e firme digitali per la posta elettronica, sono disponibili gratis programmi per comunicare su canali anonimi o per partecipare come intermediario. Per esempio sul sito di The Onion Router Project, www.torproject.org.

Anonime autorizzazioni

Supponiamo che Alice abbia sottoscritto un abbonamento alla rivista on line SophistiCat American. Si connette alla pubblicazione tramite un canale anonimo, entra con ID utente e password e si accerta che ogni messaggio in entrata o in uscita sia criptato. Ma in questo modo è sicura che nessuno possa venire al corrente di quello che sta facendo? Certamente no: la rivista sa esattamente che cosa sta facendo Alice.

Alice potrebbe coprire le proprie tracce usando uno pseudonimo, ma le abitudini di lettura dello pseudonimo potrebbero presto smascherare la sua vera identità. Alice potrebbe rivelare il proprio codice di avviamento postale per consultare le previsioni del tempo, inserire la propria data di nascita per leggere l'oroscopo e suggerire il sesso di appartenenza leggendo notizie su specifici argomenti, per esempio la mammografia. Queste tre informazioni – codice postale, data di nascita e sesso – bastano a identificare l'87 per cento della popolazione degli Stati Uniti (si veda l'articolo *Informazioni del mondo, unitevi!*, di Simson L. Garfinkel, a p. 94).

Il problema di Alice ha una soluzione crittografica chiamata «autorizzazione anonima». Alice può provare di essere un abbonato ogni volta che accede alla pagina web della rivista. Ma questa prova non rivela alcun elemento dell'identità dell'abbonato, per esempio non rivela che è la stessa persona che ha avuto accesso al sito poco tempo prima. Questo protocollo è un caso particolare del più generale protocollo di dimostrazione a conoscenza zero.

Con la dimostrazione a conoscenza zero, Alice convince Bruno che un'affermazione è vera senza rivelare perché debba esserlo o, in pratica, senza rivelare alcuna ulteriore informazione. Per provare l'affermazione «Sono un utente autorizzato di SophistiCat American», la rivista, o un servizio a essa collegato, rilascia ad Alice un'unica credenziale, simile a chiave segreta, all'atto dell'iscrizione. In seguito Alice usa la chiave per provare di avere una credenziale valida, senza rivelare la credenziale stessa. E grazie a diverse credenziali Alice fornisce una prova a conoscenza zero di affermazioni più complesse come: «Sono un utente autorizzato e maggiorenne».

Un'idea di base su come funziona una prova a conoscenza zero è illustrata nel box a fronte, in cui Alice prova a Bruno di aver colorato il diagramma in un certo modo (tecnicamente, ha «tri-colorato» un grafo) senza mostrargli in che modo. Tri-colorare un grafo è un cosiddetto problema NP-completo (si veda l'articolo *I limiti del computer quantistico*, di Scott Aaronson, in «Le Scienze» n. 477, maggio 2008). Ai fini della nostra discussione, quello che importa della NP-completezza è che si può considerare qualsiasi affermazione per cui si abbia un prova ragionevolmente breve, e mettere insieme una versione del gioco di Alice e Bruno per fornire una prova a conoscenza zero.

Il protocollo della tri-colorabilità dimostra il principio secondo cui è possibile fornire prove a conoscenza zero, anche se non è una soluzione pratica. Per fortuna gli studiosi di crittografia hanno sviluppato protocolli per specifici tipi di credenziali che possono servire per l'autorizzazione anonima efficiente.

Violare i codici

Quanto è sicura la sicurezza? Quando Alice cripta un messaggio per Bruno, quanto sarà difficile per Eva decifrare il messaggio? E se Eva conosce qualcosa può ingannare il sistema? Eva potrebbe già conoscere qualche dettaglio del messaggio criptato, per esempio il nome di un caffè in cui Alice e Bruno stanno andando per conoscersi di persona. Oppure, se «Bruno» è un server web sicuro, Eva potrebbe inviargli un testo senza senso accuratamente scelto invece di un testo cifrato e carpire dalle sue risposte alcuni indizi sulla sua chiave segreta. Una definizione ampiamente accettata di sicurezza per la crittazione a chiave pubblica contempla tutti questi casi e richiede che Eva sia in grado di acquisire solo informazioni che risultano poco utili.

L'analisi della sicurezza dei sistemi crittografici è una scienza molto sviluppata. Contrariamente alla percezione comune, non si presume che un sistema sia sicuro semplicemente perché nessuno ha mostrato di poterlo violare. Molti «mattoni elementari», invece, si basano su problemi matematici studiati in modo approfondito. I crittografi non possono provare con assoluta certezza che un sistema crittografico sia inviolabile, ma provano che ogni algoritmo in grado di violarlo risponderebbe anche alla questione fondamentale che ha impegnato i migliori matematici ed esperti di informatica.

Alcuni protocolli dipendono solo dall'esistenza di un particolare tipo di funzione matematica. Per esempio gli esperti di crittografia sanno come costruire un sistema crittografico a chiave pubblica da qualunque funzione trapdoor. Così se qualcuno viola le funzioni usate nell'algoritmo RSA le altre ancora valide si possono sostituire.

Solo di rado uno schema è considerato sicuro su una base più specifica. Ma questo viene fatto solo dopo che centinaia tra i ricercatori più bravi di tutto il mondo hanno studiato l'algoritmo per molti anni. La comunità della crittografia può permettersi di svolgere questo processo solo per pochi elementi fondamentali ritenuti critici. Per quanto riguarda i sistemi più complessi, i crittografi ne dimostrano la sicurezza considerando la sicurezza dei singoli blocchi con cui sono costruiti.

I protocolli crittografici possono dare soluzioni sorprendentemente versatili a problemi di privacy che sembrano insormontabili, come l'autorizzazione anonima. Ma molti problemi di privacy esulano dall'ambito della crittografia. Se Alice fosse sotto costante sorveglianza nel mondo fisico, sarebbe una magra consolazione sapere che le sue attività su Internet sono sicure. Attualmente a Londra le telecamere sorvegliano gli spazi pubblici per esigenze di sicurezza. Forse per proteggere la privacy i proprietari degli edifici potrebbero gestire direttamente i dati delle videocamere puntati sulle loro proprietà, e il protocollo SFE potrebbe elaborare i dati, per esempio per seguire persone sospette che lasciano una scena del crimine senza memorizzare le attività di tutti gli altri in una banca dati centralizzata.

Più in generale, quando la privacy è minacciata da un sistema come la sorveglianza pubblica, dovremmo chiederci: quali problemi cerca di risolvere quel sistema? E soprattutto: possiamo risolvere quei problemi preservando la nostra privacy grazie all'uso della crittografia? ■

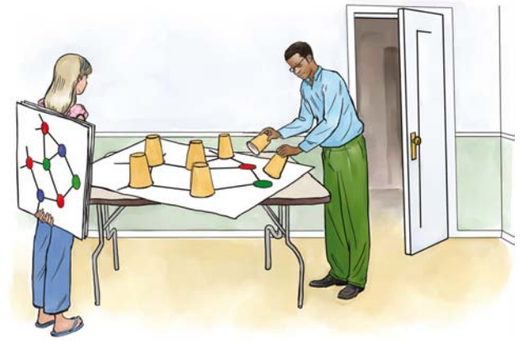
Avere le credenziali senza rivelare l'identità

Un abbonato a un sito Web può firmare come utente legittimo e registrato senza rivelare alcuna informazione utile alla sua identificazione grazie a un'autorizzazione anonima. Questo protocollo è un esempio della dimostrazione a conoscenza zero, in cui un soggetto prova un fatto senza rivelare nulla riguardo la prova tranne la sua validità.

Alice e Bruno giocano con un grafo, tre pennarelli e alcuni bicchieri. Il grafo è una collezione di vertici connessi da linee. Due vertici connessi da una linea sono detti adiacenti. Solo alcuni grafi sono tri-colorabili, cioè tre colori sono sufficienti per colorare i vertici senza averne due adiacenti con lo stesso colore. Alice proverà a Bruno di aver tri-colorato il grafo senza dargli alcun indizio su come ha fatto.

Il gioco inizia con Bruno fuori dalla stanza. Alice traccia sei copie diverse del grafo. Dopo aver tri-colorato la prima copia, completa le altre cinque usando le sei permutazioni dei tre colori. Così le sei copie del grafo sono tri-colorate in modi differenti. Poi sceglie una delle sei copie in modo casuale e copre i vertice con i bicchieri. Bruno rientra, deve scegliere due vertici adiacenti e rimuovere i bicchieri che li nascondono. Se i vertici sono dello stesso colore Bruno sa che Alice sta mentendo e non ha tri-colorato il grafo in modo valido. I due ripetono la procedura: Bruno lascia la stanza ogni volta che Alice sceglie a caso una delle sei copie da coprire con i bicchieri. Dal punto di vista di Bruno, se Alice lo sta ingannando potrebbe mostrargli differenti colorazioni non valide e l'identica colorazione di due vertici adiacenti potrebbe non essere nella stessa parte su ciascun grafo. Ma se Bruno fa un numero sufficiente di tentativi la probabilità di scoprire due vertici uguali si avvicina al 100 per cento. In ogni caso, alla fine non sa come Alice ha colorato il grafo: per ciascuno di essi, i due colori che vede sui vertici scelti sono casuali e potrebbero essere stati scelti da lui stesso.

Per qualsiasi affermazione che abbia una prova ragionevolmente breve («Ho le credenziali che dimostrano che sono un utente autorizzato e maggiorenne»), si può elaborare una versione di questo gioco che provi l'affermazione senza comunicare altre informazioni («Io sono Alice»).



Matt Collins



Kathleen Dooher

Letture

Zero-Knowledge Sudoku. Fortnow L. (come dimostrare di avere la soluzione di un Sudoku senza rivelare qual è). Disponibile alla pagina web http://weblog.fortnow.com/2006/08/zero-knowledge-sudoku.html.

Introduction to Modern Cryptography. Katz J. e Lindell Y., Chapman & Hall/CRC, 2007. Il primo capitolo è disponibile alla pagina web www.cs.umd.edu/~jkatz/imc.html.

Multiparty Computation Goes Live. Bogetoft P. e altri, febbraio 2008. Disponibile alla pagina web http://eprint.iacr.org/2008/068.