La crittografia tra arte e scienza

di Biagio Tampanella

Abstract

Se fino ad alcuni decenni fa la crittografia è stata appannaggio esclusivo di governi e forze militari nel garantire la confidenzialità delle comunicazioni, la crittografia contemporanea cerca di soddisfare anche delle esigenze che si estendono ad un pubblico più ampio (si pensi all'autenticazione, alla firma digitale, alla navigazione sicura in internet). Partendo dalla crittografia simmetrica fino ad arrivare alla crittografia asimmetrica (o a chiave pubblica), l'autore offre una panoramica storica e tecnica dei principali algoritmi di crittografia, correlandoli agli aspetti concreti relativi alla loro implementazione.

Profilo dell'autore

Biagio Tampanella è un Ufficiale della Marina Militare che attualmente presta servizio presso lo Stato Maggiore della Difesa - VI Reparto Sistemi C4I e Trasformazione, dove si occupa di sistemi di telecomunicazioni e di reti. Appassionato di intelligence e di sicurezza informatica, nel 2014 è diventato collaboratore dell'Istituto di Ricerca Eurispes. È l'autore del capitolo intitolato *L'Italia e il Cyberspazio* nel *Rapporto Italia 2015*. Ha inoltre scritto articoli legati al mondo della sicurezza e delle nuove tecnologie per Eurispes Magazine.

Keyword

crittoanalisi, comunicazioni

Scenario strategico dell'era dell'informazione

Nella dottrina militare, la *warfare* è stata definita, fino a pochi decenni fa, all'interno di tre 'domini operativi', denominati anche 'ambienti operativi'. Gli ambienti operativi tradizionali sono stati quello terrestre, quello marittimo e quello aereo. Negli odierni scenari la maggior parte delle operazioni coinvolge solitamente più di una forza armata, per cui è corretto definire la dottrina facendo riferimento all'ambiente nel quale si trovi ad operare una forza militare, che può essere composta da elementi della Marina, dell'Esercito e dell'Aeronautica. Si tratta quindi di un ambiente 'multidimensionale'.

Dopo la terra, il mare e l'aria, la dottrina si è arricchita di due nuovi ambienti operativi: quello dello spazio e quello del cyberspazio. Entrambi i due nuovi ambienti hanno esteso i confini classici della dottrina allargandoli in un contesto più globale e non più esclusivamente militare.

Concentrandoci sul cyberspazio, con questo termine s'intende l'insieme delle reti di telecomunicazioni, tutti i dispositivi (fissi e mobili) connessi ad Internet, nonché i dati e le informazioni che transitano o sono conservate all'interno della rete o dei singoli dispositivi (server, computer, smartphone, ecc.).

Sebbene il cyberspazio sia l'ultimo ambiente operativo ad essere nato, si sta affermando sempre più velocemente come quello più pervasivo di tutti. Proprio per questo motivo l'infrastruttura digitale di un Paese è ormai diventata un asset nazionale strategico.

Nel variegato mondo del Cyberspazio, un'esigenza da assicurare è anche la più antica, ossia quella di proteggere le proprie informazioni e le proprie comunicazioni.

In questo contesto rientra lo studio di una scienza che, da secoli, ha cercato di soddisfare tale esigenza: stiamo parlando della crittografia.

Nel corso dei secoli, la scienza e le tecniche associate alla crittografia sono state appannaggio esclusivo di governi e capi di Stato, nonché di forze militari. Negli ultimi decenni, invece, la vasta diffusione dei computer e delle reti di calcolatori ha generalizzato la richiesta di tecnologie adeguate a proteggere le comunicazioni estendendola al livello dei singoli cittadini o di entità private quali ad esempio aziende o enti di ricerca.

In un'era dove le informazioni in formato digitale sono cresciute in maniera esponenziale, dove l'esigenza di archiviazione sicura si è evoluta in un'esigenza di condivisione sicura dei dati, uno degli Interessi Nazionali è proprio quello di offrire una strategia in grado di garantire la protezione di queste informazioni vitali.

Cosa è la crittografia?

La parola crittografia deriva dal greco e significa scrittura segreta. Storicamente, la crittografia è stata utilizzata per proteggere le informazioni da accessi non autorizzati, in particolare durante le comunicazioni esposte ad un'intercettazione di qualsiasi genere. La crittografia ha svolto un ruolo molto importante nel corso dei secoli nelle questioni militari e nazionali.

Iniziamo il nostro studio operando la definizione dei principali 'ingredienti' della crittografia. Un messaggio in partenza è noto come testo in chiaro, mentre il messaggio codificato è chiamato testo cifrato. Il processo di conversione da testo in chiaro a testo cifrato è conosciuto come cifratura o crittografia; il processo di conversione del testo cifrato nell'originario testo in chiaro è conosciuto come decifratura o decrittazione.

Le tecniche utilizzate per decifrare un messaggio senza alcuna conoscenza dei dettagli di cifratura rientrano nell'ambito della crittoanalisi. La crittoanalisi è ciò che il profano chiama 'rompere il codice'. La crittografia e la crittoanalisi insieme definiscono la più ampia scienza della crittologia. Il nostro studio, sebbene opererà dei cenni riguardo la crittoanalisi, si concentrerà essenzialmente sulla crittografia.

La crittografia simmetrica o a chiave segreta

Nell'uso classico della crittografia, è necessario che sia il mittente che il destinatario abbiano una conoscenza comune del processo di crittografia (l'algoritmo crittografico) e che entrambi condividano un elemento comune segreto, di norma la chiave crittografica.

Secondo il noto principio di Kerckhoffs: «la sicurezza di un sistema crittografico deve basarsi esclusivamente sulla segretezza della chiave e non sulla segretezza dell'algoritmo di cifratura impiegato».

Nel processo di cifratura, l'algoritmo trasforma il testo in chiaro in testo cifrato usando una determinata chiave; l'uso di una chiave differente conduce a un differente testo cifrato. Nel processo di decifratura, l'algoritmo trasforma il testo cifrato in chiaro, utilizzando la medesima chiave che è stata utilizzata per cifrare il testo in chiaro di partenza. Tale schema, in cui entrambe le parti comunicanti devono possedere una chiave comune, è definita crittografia simmetrica o crittografia a chiave segreta: è il tipo di crittografia che è stata usata per secoli.

Fra i più famosi moderni algoritmi di cifratura simmetrica, che sono diventati anche degli standard definiti dal *National Institute of Standards and Technology* (NIST) troviamo, in ordine cronologico, il *Data Encryption Standard* (DES), il Triple DES, l'*Advanced Encryption Standard* (AES).

Questa forma di crittografia ha la caratteristica, che di solito si rivela anche uno svantaggio operativo, di esigere un metodo sicuro per la distribuzione delle chiavi fra le parti interessate.

Può essere infatti difficile organizzare la distribuzione delle chiavi simmetriche e segrete a tutti i soggetti con i quali si potrebbe desiderare di comunicare, soprattutto quando il numero dei soggetti è elevato.

La crittografia asimmetrica o a chiave pubblica

Un sistema denominato crittografia asimmetrica (o, equivalentemente, crittografia a chiave pubblica), sviluppato a metà degli anni '70 da due crittologi americani, Whitfield Diffie e Martin Hellman, aiuta a mitigare molte delle difficoltà della crittografia simmetrica (legate al bisogno di distribuire in maniera sicura una comune chiave segreta) attraverso l'utilizzo di chiavi diverse per l'operazione di cifratura e di decifratura. Negli algoritmi asimmetrici, ogni soggetto ha di fatto due chiavi. La chiave pubblica viene pubblicata, è liberamente disponibile a chiunque, ed è usata tipicamente per crittografare; la chiave privata viene conservata in segreto dal ricevente e viene utilizzata tipicamente per la decifratura.

Se l'utente A vuole trasmettere in maniera sicura un messaggio all'utente B, non deve far altro che cercare la chiave pubblica di B (che, appunto, è pubblica), cifrare il proprio messaggio utilizzando tale chiave e inviare il testo cifrato a B. Quando B riceve il testo cifrato, potrà procedere alla decifratura del messaggio, utilizzando la propria chiave privata. Solo B potrà decifrare il messaggio ricevuto, in quanto la chiave pubblica non può essere impiegata per decifrare il messaggio.

Sebbene le due chiavi siano ovviamente legate tra di loro, tuttavia dal punto di vista matematico è computazionalmente molto difficile, in un qualsiasi periodo di tempo ragionevole, ricavare la chiave privata dalla conoscenza della corrispettiva chiave pubblica.

Per aiutare ulteriormente la comprensione di questo brillante algoritmo, immaginate di avere una cassaforte aperta. Inserite il vostro messaggio all'interno della cassaforte e chiudetela. Voi non potrete più riaprire la cassaforte e solo il proprietario della chiave che apre la cassaforte potrà aprirla e leggere quindi il contenuto del vostro messaggio.

In realtà, come vedremo più avanti, la crittografia asimmetrica consente anche un altro tipo di utilizzo che permette di garantire l'autenticità del mittente. In questo caso il processo seguito è inverso al precedente: il mittente usa la propria chiave privata per codificare il messaggio e il destinatario usa la chiave pubblica del mittente per decifrare il messaggio. In tal modo non si garantisce la confidenzialità del messaggio, ma si ha garanzia su chi lo ha scritto e cifrato.

Fra i più famosi algoritmi di cifratura asimmetrica o a chiave pubblica abbiamo:

- RSA (dal nome dei tre ideatori, Rivest-Shamir-Adleman), basato sull'elevata complessità computazionale della fattorizzazione in numeri primi
- EEC (Elliptic Curve Cryptography), basato sulla difficoltà di risolvere il problema del logaritmo discreto su curva ellittica. Tale difficoltà è ritenuta, ad oggi, più onerosa dal punto di vista computazionale rispetto a quella della fattorizzazione in numeri primi.

Differenza fra crittografia simmetrica ed asimmetrica

Una significativa differenza operativa tra crittografia simmetrica e asimmetrica è che con la crittografia asimmetrica chi conosce la chiave pubblica di una determinata persona può inviare un messaggio sicuro a quella persona. Con la crittografia simmetrica, invece, solo un insieme selezionato di persone (che conoscono la chiave segreta comune) è in grado di comunicare.

Anche se non è matematicamente dimostrabile, tutti i sistemi crittografici asimmetrici noti sono più lenti rispetto ai loro omologhi sistemi di crittografia simmetrica. In genere, la crittografia simmetrica viene utilizzata quando una grande quantità di dati deve essere criptata, o quando la crittografia deve essere effettuata entro un dato periodo di tempo; la crittografia asimmetrica è utilizzata per messaggi brevi, per esempio per proteggere la distribuzione delle chiavi di un sistema di crittografia simmetrica.

Le tre dimensioni degli algoritmi crittografici

I sistemi crittografici sono caratterizzati da tre dimensioni indipendenti:

- gli algoritmi di cifratura: ossia il tipo di operazioni utilizzate per trasformare il testo in chiaro in testo cifrato. A loro volta, tutti gli algoritmi di cifratura si basano su due principi generali: la sostituzione, con la quale ogni elemento del testo in chiaro (che può essere una lettera, un bit, oppure un gruppo di bit o un gruppo di lettere) è sostituito con un altro elemento; la trasposizione, con la quale gli elementi del testo in chiaro sono riorganizzati attraverso degli spostamenti. Il requisito fondamentale comune è che nessuna informazione venga persa (il che implica che tutte le operazioni siano reversibili). La maggior parte degli algoritmi crittografici contempla più fasi di sostituzioni e trasposizioni
- il numero di chiavi utilizzate: come detto, se sia il mittente che il destinatario utilizzano la stessa chiave, l'algoritmo è indicato come simmetrico, a chiave singola o a chiave segreta.

Se il mittente e il destinatario utilizzano chiavi diverse, l'algoritmo viene definito come asimmetrico, a due chiavi, o a chiave pubblica

- la modalità operativa con la quale il testo in chiaro viene elaborato: un cifrario a blocchi processa come input un blocco di elementi alla volta (aventi tutti una certa dimensione predefinita), producendo in uscita un blocco di output cifrato. Un cifrario a flusso elabora gli elementi di input continuamente, producendo in uscita un elemento alla volta, man mano che il flusso prosegue. Senza entrare troppo nello specifico, per il cifrario a flusso è anche importante la lunghezza del cosiddetto vettore d'inizializzazione (IV) e il grado di entropia ad esso associato.

La confidenzialità

È un servizio che fornisce la garanzia che le informazioni siano protette da una visualizzazione non autorizzata, sia mentre sono in transito durante le comunicazioni, sia mentre sono conservate in un sistema informativo.

Si consideri il problema generale di inviare un messaggio privato da A a B. Secoli fa, un tale processo poteva essere compiuto con A che scriveva una lettera contenente la sua firma. La lettera veniva sigillata all'interno di una busta per impedire la divulgazione accidentale. Se B riceveva la busta con un sigillo rotto, voleva dire che la lettera era stata aperta o alterata e B prendeva le azioni appropriate. In caso contrario, B verificava la firma di A e quindi leggeva il messaggio.

Nell'era dell'informazione, ciascuna delle fasi rimane essenzialmente la stessa, ad esclusione del fatto che ora strumenti automatizzati eseguono la maggior parte del lavoro. Per garantire la confidenzialità delle comunicazioni si può agire in tre modi:

- attraverso la sicurezza fisica del percorso: ad esempio, la fibra ottica è un mezzo trasmissivo dal quale è intrinsecamente difficile estrapolare le informazioni che in esso transitano
- attraverso l'offuscamento, basato sul fatto che l'utente A trasmette le informazioni dopo averle adeguatamente nascoste all'interno di un qualche contenitore circostante in modo che un eventuale malintenzionato trovi molta difficoltà nel riconoscere l'informazione e, di conseguenza, nel recuperarla. Un esempio di questo metodo è la steganografia, con la quale i dati possono essere nascosti, ad esempio, all'interno di immagini
- attraverso la crittografia, che abbiamo finora descritto. Quando la confidenzialità viene assicurata dalla crittografia, le informazioni cifrate possono anche cadere nelle mani di qualcuno non autorizzato a visionarle, senza però venire compromesse. L'impiego della crittografia solleva quindi A e B dallo sforzo di garantire la sicurezza fisica del percorso o di ricorrere all'offuscamento. Poiché i mezzi di comunicazione odierni più semplici ed economici sono anche i più insicuri (ad esempio le comunicazioni wireless) l'indipendenza della sicurezza fisica del mezzo utilizzato dalla sicurezza del messaggio (indipendenza offerta dalla crittografia) ha i suoi evidenti vantaggi.

Altri servizi offerti dalla crittografia

Indipendentemente dal particolare approccio adottato, le applicazioni della crittografia sono andate ben oltre le sue radici storiche di scrittura segreta. Queste altre funzionalità possono essere considerate collettivamente come impieghi collaterali della crittografia, in quanto non legati all'esigenza di confidenzialità. Vediamo quali sono le principali applicazioni.

Autenticazione

È la garanzia che l'identità dichiarata è valida per un determinato individuo o sistema in generale. Questo significa verificare che gli utenti sono quelli che dicono di essere e che ogni input che giunge a un sistema proviene da una fonte sicura e fidata. Mentre ci muoviamo verso un'economia ed una condivisione delle informazioni basate sempre di più su sistemi digitali, il tutto condotto su reti di comunicazione su larga scala (dove chi eroga un servizio è quasi sempre fisicamente lontano da chi usufruisce di tale servizio), diventa sempre più impellente sviluppare forti meccanismi di autenticazione che impediscano a qualsiasi malintenzionato di essere in grado di accedere alle risorse remote senza la necessaria autorizzazione.

La crittografia interviene nel soddisfare il requisito di autenticazione, ad esempio, mediante la cosiddetta firma digitale (la quale, a sua volta, garantisce anche l'integrità, di seguito descritta).

Controllo d'integrità

È la garanzia che un messaggio o un'informazione in generale non sia stata manomessa o alterata. Con tale certezza, è difficile per un utente non autorizzato modificare i dati. I possibili problemi che richiedono il ricorso al controllo d'integrità sono due:

- un problema tecnico (come ad esempio un disturbo nella comunicazione) può inavvertitamente modificare uno o più bit dell'informazione trasmessa
- una terza parte può deliberatamente modificare uno o più bit dell'informazione trasmessa, rendendo le informazioni ricevute illeggibili o, peggio, modificate nei loro contenuti.

È quindi auspicabile assicurare che qualsiasi modifica, sia accidentale che intenzionale, possa essere rilevata allorché si verifica.

La crittografia interviene nel soddisfare il requisito di controllo di integrità, ad esempio, mediante una funzione di hash. La funzione di hash è una funzione pseudocasuale che fornisce un output, di lunghezza predefinita, che è più breve rispetto alla lunghezza dell'input. La funzione di hash è detta a senso unico in quanto, se è abbastanza facile calcolare l'hash (o impronta) di un messaggio, è computazionalmente impossibile, dato un hash, ricostruirne la stringa di input.

Firma digitale

È la garanzia che un messaggio o un documento sia stato inviato o creato da una determinata persona (e che tale messaggio sia integro). Una firma digitale lega, crittograficamente, l'identità di una persona con il contenuto di un messaggio o di un documento in generale. Come funziona? L'utente che vuole trasmettere un documento firmandolo digitalmente, calcola innanzitutto l'hash del testo e quindi provvede a cifrare l'hash con la propria chiave privata. Invia infine il documento insieme all'hash cifrato. Il ricevente decifra con la chiave pubblica del mittente l'hash cifrato che ha ricevuto. Calcola l'hash del documento ricevuto in maniera indipendente e quindi verifica che tale hash sia identico a quello ricavato con la decifratura dell'hash cifrato che era stato ricevuto. Se ciò accade, egli ha la conferma che il documento (che, ricordiamo, è in chiaro) ricevuto ha ottenuto la firma digitale del mittente. Con questo meccanismo il ricevente ha anche modo di verificare non solo l'autenticità, ma anche l'integrità del messaggio: se infatti il documento ricevuto fosse una

distorsione di quello trasmesso, il ricevente se ne accorgerebbe in quanto riscontrerebbe hash differenti nella sua verifica. È interessante notare come, in questa circostanza, il mittente usa, come chiave di cifratura, la propria chiave privata (e non quella pubblica come nel caso di trasmissione confidenziale di messaggi), in quanto il suo obiettivo è differente.

Non ripudio

L'autenticazione di un utente e l'integrità di un messaggio, visti nella descrizione della firma digitale, introducono un'ulteriore capacità offerta dalla crittografia, ossia il 'non ripudio'.

Il 'non ripudio' è una capacità crittografica che unisce tecniche per garantire l'autenticazione degli utenti e il controllo di integrità al fine di assicurare che il firmatario di un messaggio non possa plausibilmente negare che sia stato lui a creare quel messaggio e a trasmetterlo.

Il concetto di 'non ripudio' comprende spesso anche una dimensione temporale: per esempio, si deve essere in grado di dimostrare non solo che una determinata persona abbia firmato un certo ordine di acquisto ma anche che tale ordine sia stato effettuato in una determinata data e in un determinato orario (*time stamp*).

Public key infrastructure (infrastruttura a chiave pubblica)

Nel servizio di 'non ripudio' sopra descritto, vi sono due aspetti significativi da evidenziare: il primo è che, a voler essere precisi, la firma digitale (così come descritta) in realtà associa un documento ad una determinata chiave privata. Il secondo è che il cosiddetto *time stamp* non può essere apposto, per ovvi motivi, dal mittente stesso.

È sorta quindi la necessità di creare i certificati digitali e le relative strutture organizzative deputate a gestire tali certificati. L'Ente certificatore, ossia la *Certification Authority* (CA), soddisfa la necessità di associare una persona (o più in un generale una determinata entità) alla sua chiave pubblica, ovvero identificare la persona come il possessore della corrispondente chiave privata. Per farlo, la CA produce un certificato digitale pubblico contenente la chiave pubblica della persona e i suoi dati identificativi, infine cifra il certificato con la propria chiave privata. Tornando quindi all'esempio della firma digitale, il ricevente verifica l'associazione 'chiave pubblica/identità' di una persona mediante il certificato digitale. Per farlo, decifra il certificato digitale mediante la chiave pubblica dell'Ente Certificatore e verifica l'associazione. Qui sorge la domanda: «ma chi ci assicura che la chiave pubblica della CA in possesso del ricevente sia effettivamente quella vera?» La chiave pubblica di una CA, riferendoci ad una comunicazione che avviene tramite Internet, è conservata nel browser. In questo caso l'utente ricevente deve quindi fidarsi:

- della correttezza della CA (che non si metta per oscuri motivi a creare certificati digitali falsi)
- della sicurezza del browser, il quale come visto decide quali chiavi pubbliche di quali CA inserire nel proprio codice
- del fatto che nessuno possa modificare il browser inserendo in maniera nascosta chiavi pubbliche di CA fittizie.

Non è obiettivo del presente studio entrare nel dettaglio di possibili scenari di attacchi, tra l'altro in passato accaduti realmente ad alcune CA, ma un gruppo di hacker che riuscisse a violare una CA

(potendo quindi creare certificati digitali falsi ma allo stesso tempo riconosciuti dalla CA stessa, quindi ritenuti 'veri'), operando al contempo un attacco ad un server *Domain Name System* (DNS), potrebbe causare problemi molto seri, dirottando gli utenti su siti web raggiungibili con lo stesso indirizzo "reale" e che continuerebbero a essere riconosciuti come affidabili per via dei certificati digitali a loro volta contraffatti. Come si vede, alla fine del processo, o meglio a monte di qualsiasi organizzazione di questo genere, si finisce sempre con il ricondursi ad un concetto di 'fiducia', il che include inevitabilmente il fattore umano, che risulta cruciale in ogni questione di sicurezza.

La serie di processi e di standard impiegati per assicurare la trasmissione sicura di informazioni digitali è chiamata *Public Key Infrastructure* (PKI). La PKI, o Infrastruttura a Chiave Pubblica, è quindi un ambiente che gestisce la cifratura a chiave asimmetrica e le firme digitali per garantire in maniera profonda i servizi di autenticazione, cifratura e 'non ripudio'.

Sintetizzando e ricapitolando, una PKI comprende:

- la CA
- i Digital Certificates (DC)
- le coppie di chiavi pubbliche e private.

L'Infrastruttura deve inoltre comprendere dei server dove poter installare i servizi della CA, delle procedure per gestire richieste di nuovi certificati, meccanismi per permettere agli utenti un semplice utilizzo dei certificati e delle chiavi, meccanismi per aggiornare automaticamente le liste di certificati e di chiavi quando queste scadono, un sistema solido di backup.

Analisi degli ostacoli che hanno influenzato o che influenzano la domanda di crittografia

Anche quando un utente è consapevole del fatto che la sicurezza delle comunicazioni è minacciata e intende agire per prevenire questa minaccia, si trova a dover affrontare degli ostacoli pratici che rendono i suoi obiettivi più difficili da raggiungere. Alcuni di questi ostacoli permangono tuttora, altri invece, come si vedrà, sono stati superati. Esaminiamoli insieme.

La mancanza di massa critica

Un telefono sicuro non è di grande utilità se è solo una persona a possederlo. Garantire che le comunicazioni siano sicure richiede un'azione collettiva, una massa critica di dispositivi interoperabili che stimolino l'utilizzo di comunicazioni sicure. Questa massa critica generalmente esiste per organizzazioni di tipo militari, ma nel mondo privato è ancora lontana dall'essere raggiunta.

Questo ostacolo è ancora esistente, in quanto sono poche le persone che ricorrono alla crittografia per soddisfare le varie funzionalità sopra descritte.

La mancanza di una Infrastruttura di supporto

La semplice disponibilità di dispositivi non è necessariamente sufficiente. Come detto anche nei paragrafi precedenti, è necessaria una Infrastruttura Nazionale o Internazionale per gestire le chiavi. Senza una PKI pubblica, la crittografia può rimanere un'attività di nicchia utilizzabile solo mediante

procedure ad hoc che simulano alcune delle funzioni che una Infrastruttura pubblica organizzata fornirebbe.

Questo ostacolo è stato superato in numerosi Paesi. In Italia, la PKI nazionale è gestita dall'AGID, Agenzia per l'Italia Digitale (la quale è subentrata alla DigitPa, che un tempo era denominata CNIPA).

Costi elevati

La sicurezza crittografica, storicamente basata sull'hardware, è molto costosa, in parte a causa dei costi elevati da sostenere per produrre dispositivi stand alone realizzati in quantità ridotte.

Questo ostacolo è stato superato, in quanto da diversi anni la crittografia si può realizzare efficacemente anche in modalità software, il che richiede costi decisamente minori.

Riduzione delle prestazioni

L'implementazione di funzioni crittografiche in passato consumava ingenti risorse computazionali. In alcuni casi, il consumo eccessivo di risorse rendeva la crittografia troppo lenta e costringeva l'utente ad acquistare memoria aggiuntiva.

Questo ostacolo è stato superato, in quanto i computer moderni, anche quelli privati, sono talmente potenti da non rallentare la crittografia. Anche per questo motivo, ad esempio, Google si può permettere di usare *https* per servizi non particolarmente critici, quali ad esempio la ricerca.

Considerazioni

Se, quindi, tutti i motivi precedenti per non utilizzare la crittografia non sono in gran parte più validi, perché la crittografia si utilizza ancora "poco"?

È un problema di usabilità unito, spesso, ad un problema di pigrizia o di mancata conoscenza della materia. Molti utenti, anche se dispongono di competenze e conoscenze professionali di un certo livello, non vogliono complicazioni, nel senso che non vogliono inserire una password in più o non vogliono usare un servizio differente da quello a loro familiare e noto (e che dispone di 'massa critica'), che è così tanto comodo quanto magari insicuro. Altri utenti, peggio, ignorano totalmente il problema, non solo per carenze di conoscenze tecniche, quanto per carenze culturali: essi sono mossi da un forte desiderio di condivisione pubblica della propria vita, desiderio assolutamente privo della consapevolezza dei rischi che si corrono nel non proteggere i propri dati e le proprie informazioni, che siano personali o di lavoro.

Dicotomia nell'impiego della crittografia

Nel contesto della confidenzialità, l'essenza della sicurezza delle informazioni non è che un riflesso della perenne battaglia fra chi vuole proteggere le informazioni e chi invece vuole intercettarle e violarle.

I primi attori, ossia chi vuole cifrare, possono essere motivati da buone ragioni (se sono organizzazioni legittime) o da cattive ragioni (se sono criminali) nel limitare l'accesso alle informazioni esclusivamente a un gruppo selezionato.

Ma anche i secondi attori, ossia chi vuole intercettare, possono essere animati sia da buone ragioni (ad esempio forze dell'ordine che indagano gravi reati) sia da cattive ragioni (ad esempio criminali che vogliono nascondere le proprie comunicazioni).

Questa dicotomia nell'utilizzo della crittografia è uno dei dilemmi oggetto di varie discussioni nel mondo accademico e pubblico.

Come ogni tecnologia o scoperta scientifica, nel corso della storia, si è rivelata un'arma a doppio taglio, anche la crittografia ha una doppia anima e può essere usata nel bene o nel male.

La crittografia può essere usata per proteggere informazioni vitali per la sicurezza nazionale o per la propria privacy, come pure può essere usata per scopi illeciti (si veda ad esempio il malware *ransomware*, il quale cifra tutti i dati di un determinato dispositivo e poi, tramite un particolare sistema, richiede un riscatto economico al fine di sbloccare i dati, ossia fornire la chiave di decifratura necessaria per riottenere i dati bloccati).

D'altro canto, se la crittografia è in grado di proteggere i segreti commerciali e le informazioni proprietarie delle aziende, allora riduce lo spionaggio economico e quindi facilita il lavoro delle forze dell'ordine (che vengono coinvolte quando il *data breach* viene scoperto e denunciato). Se la crittografia può aiutare a proteggere le informazioni che transitano in infrastrutture critiche nazionali (ad esempio comunicazioni militari di un certo livello), allora la crittografia supporta la sicurezza nazionale e quindi è un bene.

La battaglia fra crittografi e crittoanalisti nel corso della storia

La battaglia fra cifratori e decifratori si perde nei secoli ed è una testimonianza storica della dicotomia enunciata nel paragrafo precedente.

Giulio Cesare inventò un sistema di cifratura basato sulla tecnica della sostituzione, con il quale una lettera all'interno di un messaggio veniva sostituita dalla terza lettera dell'alfabeto successiva a quella da sostituire. Questo sistema per l'epoca si rivelò abbastanza efficace, anche se con gli occhi di oggi un simile algoritmo farebbe ovviamente sorridere.

Nonostante ciò, la cifratura monoalfabetica ha resistito per molti secoli, fino a quando nel IX secolo lo studioso arabo Al-Kindi evidenziò come il contenuto di un messaggio cifrato mediante la sostituzione monoalfabetica può essere scoperto calcolando semplicemente la frequenza dei singoli elementi del testo in cifra. Se in una determinata lingua è noto che la lettera 'a' ha una certa percentuale di comparsa in un testo di una certa lunghezza, appare evidente come ricercare la medesima frequenza in un testo cifrato conduce il crittoanalista a rivelare che la lettera in questione sia propria la cifratura della lettera 'a'.

L'analisi delle frequenze mise quindi in crisi l'efficacia della cifratura a sostituzione monoalfabetica. I crittoanalisti passarono quindi in vantaggio nella battaglia con i crittografi.

Nel XVI Secolo, però, il diplomatico francese Blaise de Vigenère, studiando alcuni scritti di Leon Battista Alberti, (pittore, musicista, filosofo e poeta fiorentino), dell'abate tedesco Trithemius e dello scienziato italiano Giambattista Della Porta, realizzò un nuovo algoritmo di cifratura che era resistente all'analisi delle frequenze, ammettendo inoltre un grande numero di chiavi (a differenza della cifratura di Giulio Cesare che ne prevedeva solo ventuno, tante quante le lettere dell'alfabeto). Nel suo trattato *Sulle scritture segrete* del 1586, Vigenère descrisse il suo algoritmo, che per molti secoli rimase inviolato, assicurandosi il titolo di 'cifratura indecifrabile'. Ma nel XIX secolo il londinese Charles Babbage, precursore dei moderni calcolatori, prima, e l'ufficiale in pensione dell'esercito prussiano Kasiski poi, violarono la cifratura di Vigenère. A dire il vero, fu Babbage a scoprire per primo come violare l'algoritmo, ma attese anni prima di pubblicare la sua scoperta: molto probabilmente perché ebbe pressioni dal controspionaggio britannico al fine di non rivelare la sua scoperta. La crittoanalisi passò pertanto nuovamente in vantaggio.

Nel corso della prima guerra mondiale alcuni scienziati americani, basandosi sul cifrario di Vigenère ma eliminando la ciclicità delle chiavi usate da questo sistema, introdussero un sistema che, ancora oggi, rimane assolutamente indecifrabile sotto certe condizioni.

Stiamo parlando della cifratura a blocco mono uso, *One Time Pad* (OTP), un sistema che prevede l'impiego di una chiave, che sia una sequenza assolutamente casuale, lunga quanto il messaggio da cifrare e che, infine, sia utilizzata come chiave solo una volta.

La cifratura OTP è l'unico algoritmo esistente che garantisce una sicurezza matematicamente inviolabile, anche disponendo di calcolatori in grado di eseguire un numero infinito di operazioni. OTP è stato usato nella famosa 'Linea Rossa' fra Stati Uniti e Unione Sovietica durante la Guerra Fredda (che, per la cronaca, non era un telefono, bensì un sistema di scambio di messaggi testuali).

I vincoli di OTP sono relativi alla necessità di avere una chiave davvero casuale, di dover disporre di un set di chiavi molto grande (in quanto la chiave va distrutta dopo l'uso, mai impiegata per due cifrature differenti) e nella difficoltà di distribuire le chiavi.

Proprio per questo motivo si chiama *One Time Pad*: le spie della Guerra Fredda conservavano le proprie chiavi in un blocchetto monouso dal quale strappavano la pagina una volta che la chiave in esso contenuta era stata impiegata.

Nel corso della seconda guerra mondiale la temibile macchina denominata *Enigma* spostò l'ago della bilancia a favore dei tedeschi, fino a quando il genio di Alan Turing permise di violare *Enigma*, assicurando la sconfitta militare tedesca.

La crittografia (e la crittoanalisi) sono state in grado di modificare il corso della Storia.

Il futuro della crittografia

Al di là delle tecniche di cifratura e decifratura del futuro, la crittografia è una scienza matematica affascinante che ha ormai risvolti sempre più concreti nella vita reale di ciascuno di noi. Ogni individuo, in numerose sue attività quotidiane, usufruisce oggi dei benefici della crittografia senza nemmeno saperlo.

Qual è il futuro della crittografia? Se proviamo a dipingere uno scenario possibile, sicuramente vi sarà ancora un'alternanza di vittorie e sconfitte fra crittografi e crittoanalisti, così come è accaduto nel passato. Le nuove tecnologie saranno protagoniste di questa nuova sfida.

Molto si parla della cosiddetta crittografia quantistica, che sarebbe un'evoluzione di OTP ancora più sicura in quanto fra le tante cose non ci sarebbe più la necessità, fra i due utenti, di scambiarsi preventivamente la chiave. Come anche si parla dei calcolatori quantistici che, se realizzati, farebbero 'saltare' immediatamente la crittografia attualmente esistente, rendendola quindi totalmente insicura. Chi arriverà per primo? Chi vivrà vedrà.

Se mentre in passato la competizione fra crittografi e analisti aveva un impatto esclusivamente in ambiti governativi e militari, nel mondo moderno questa battaglia diventa più globale, in quanto l'Era dell'Informazione impone una sicurezza dei dati più diffusa e che investe settori di ogni tipo, che pervadono la vita di ciascuno di noi: immaginiamo come il settore economico e industriale potrebbero avere grandi benefici nell'uso della crittografia, come protezione dei propri dati nel contrastare lo spionaggio industriale.

Bisogna però superare anche una barriera culturale ancora esistente in molti di noi: l'implementazione di 'sicurezza' comporta, per i produttori di hardware e software, dei costi aggiuntivi che normalmente non vengono visti con entusiasmo, anche perché apparentemente non vengono richiesti nemmeno dai clienti stessi dei prodotti. Anche all'interno di grandi organizzazioni, private o pubbliche, si tende a interpretare i costi della sicurezza come un qualcosa di inutile. Questo modo di vedere le cose si traduce in prodotti e procedure che sono carenti dal punto di vista della sicurezza.

La crittografia è una scienza che merita di essere conosciuta in maniera approfondita. Oltre alla conoscenza tecnica di protocolli e procedure, la conoscenza dei principi generali della crittografia (e della sua 'nemica', la crittoanalisi) educa ad un approccio alla sicurezza più completo e maturo, requisito fondamentale per chiunque, a suo modo, si trovi ad occuparsi di sicurezza delle informazioni.

Bibliografia

B. SCHNEIER, Applied Cryptography, John Wiley & Sons, 1996

B. SCHNEIER, N. FERGUSON, T. KOHNO, Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, 2010

S. SINGH, The Code Book: the Secret History of Codes and Code-Breaking, Fourth Estate, 2002

W. STALLINGS, Cryptography and Network Security, Prentice-Hall, 2013