La crittografia

In molti casi è necessario rendere segrete le informazioni che viaggiano, cioè renderle disponibili solo a determinati utenti, ad esempio mittente e destinatario. Per raggiungere tale obiettivo è necessario codificare le informazioni. Il processo di codifica è identico a quello utilizzato dal codice ASCII: per questo l'ASCII è un codice. Il codice ASCII è noto a tutti: serve a far corrispondere i caratteri alfanumerici ai byte. Si creano allora dei codici noti solo agli interessati. L'idea non è certo moderna: fin dalle guerre più antiche si ha testimonianza di codici con cui venivano scritte le lettere tra i generali degli eserciti. A livello informatico la codifica delle informazioni si sviluppa molto durante le guerre mondiali.

Uno tra i primi casi in cui si è utilizzato un codice identificativo di apparecchiature elettroniche è quello dei telefonini. Inizialmente i telefonini erano grossi apparecchi installati sulle automobili e inviavano dati con il codice NMTS, l'antenato del GSM. Ogni telefono aveva inoltre un numero seriale assegnato dall'ETACS. Perciò per rubare le chiamate bisognava conoscere il numero seriale di un telefono e sostituirlo a quello della vittima per addebitare sul suo conto le chiamate.
Il codice GSM oggi non è più abbinato al numero seriale, ma fa uso di un algoritmo, una sorta di serratura apribile solo con una chiave. Ciò che possiede la chiave è il telefono.

Un algoritmo è un insieme di passaggi logico-matematici che permettono di risolvere un problema. Il problema che noi dobbiamo risolvere è quello di codificare le informazioni. Facciamo un esempio. Se voglio codificare la parola "Alberto" posso aggiungere una posizione alfabetica a ciascuna lettera. Così "A" diviene "B", "l" diviene "m", ecc. Alla fine si ottiene "Bmcfsup". La codifica può essere vista matematicamente come "+1". La decodifica è "-1". Infine + è l'algoritmo ("aggiungere posizioni"), 1 è la chiave ("quanto aggiungo"). Questo tipo di chiave è simmetrica: assume valori opposti per codifica e decodifica.
Il metodo è utile, tuttavia non possibile essere sicuri che solo chi è autorizzato conosca la chiave per leggere le informazioni.. Non si può neppure sapere se chi invia le informazioni sia davvero chi io penso le stia inviando. Se la chiave è divulgata o scoperta è facile falsificare le informazioni.

Si rende allora necessario elaborare un metodo più sicuro affinché le telefonate siano protette. Vediamo come viene risolto il problema. Ogni SIM è come un calcolatore su cui viene scritto un numero, che chiamiamo divisore D. Il divisore è noto esclusivamente al gestore telefonico. L'utente non può leggerlo. Per identificare l'utente e metterlo in comunicazione col destinatario della telefonata, il gestore invia un numero N molto grande al cellulare. A questo punto sia il cellulare che il gestore eseguono la divisione di N per D e calcolano il resto. Il cellulare lo invia al gestore. Se i due resti coincidono, l'invio di dati avviene. È vero che chi ascolta numero N e R può scoprire D, ma le prove da fare sono molte. Infatti parliamo di numeri N molto grandi. Ragioniamo: se N ha tre cifre, cioè oscilla tra 0 e 999 e se D ne ha due, cioè oscilla tra 0 e 99, il resto sarà compreso tra 0 e 98. Quindi esistono molti casi che danno lo stesso resto. Semplice esempio è: 8 diviso 3 fa 2 con resto 2; 10 diviso 4 fa 2, ancora con resto 2 e così via. Non è facile scoprire il divisore: bisogna carpire molti N e molti R.
Questo tipo di chiave è comunque simmetrica: il processo è opposto per codifica è decodifica. Si pensi infatti all'operazione da svolgere per scoprire il divisore.

Alcuni anni fa dei matematici hanno sfruttato un antico teorema di Eulero per elaborare una chiave che non fosse conoscibile nemmeno usando quella associata. Ogni utente coinvolto nella trasmissione possiede infatti due chiavi: una privata e una pubblica (quella associata). Il teorema di Eulero riguarda i numeri primi: il prodotto di due numeri primi è divisibile solo per i due numeri stessi. Pertanto moltiplicando due numeri primi molto grandi ottengo un numero enorme divisibile solo per quei due numeri ed è veramente difficile riuscire a scoprire quali essi siano.
Immaginiamo ora di voler trasmettere dati che devono rimanere segreti a una banca. Il nostro computer, sfruttando il teorema di Eulero, genera le due chiavi, privata e pubblica. La chiave pubblica è visibile alla banca e a tutti coloro che devono interagire con noi. La chiave privata è segreta. Allo stesso modo la banca genera due chiavi, privata e pubblica. Quella privata è segreta, quella pubblica è nota a tutti i clienti che devono comunicare, quindi anche al nostro computer.
Quando inviamo dati, il computer esegue la codifica degli stessi usando la chiave pubblica della banca e la nostra chiave privata. Solo la banca potrà eseguire la decodifica dei dati usando la propria chiave privata. La banca invia i dati codificando con la propria privata e la nostra pubblica. Noi li riceviamo e usiamo nostra privata e la pubblica della banca per la codifica.
Il fatto che noi usiamo la nostra privata per la codifica garantisce che siamo davvero noi a inviare i dati. Nessuno può usare la nostra chiave privata. Inoltre il fatto che per la codifica e la decodifica serva una coppia di chiavi appartenente ai due diversi utenti coinvolti nella comunicazione garantisce la segretezza dell'informazione.
Di conseguenza è necessario che le chiavi pubbliche siano corrette e reali, cioè rappresentino realmente l'ente cui dicono di appartenere. Esistono allora enti certificatori delle chiavi pubbliche delle banche e degli enti vari.