PILLOLE DI COLORE

LA PROTEZIONE DELLE COMUNICAZIONI SU INTERNET

*Articolo scritto durante il periodo di lockdown.

In questi giorni di forzato isolamento trascorriamo davanti al computer molto del nostro tempo, per lavoro, per svago, per fare acquisti. E sempre di più trasmettiamo tramite questo potente strumento una quantità considerevole di informazioni sensibili. Ma come sono protette?

La connessione sicura, ovvero criptata, è testimoniata da un lucchetto posto a sinistra dell'indirizzo del sito. Ma come è possibile trasmettere informazioni criptate ad uno sconosciuto con il quale non è stato preso alcun accordo riguardo a come criptare le informazioni stesse ?

Immaginiamo di dover comunicare il nostro numero di carta di credito al negozio on line sul quale abbiamo trovato un articolo interessante. Purtroppo tale comunicazione, fatta "in chiaro", è molto rischiosa in quanto esiste la possibilità che qualcuno stia spiando il traffico dati nostro o del nostro interlocutore allo scopo di carpire informazioni di rilevante valore economico, quale potrebbero essere appunto i dati di una carta di credito. Essendo il negozio on line a noi sconosciuto, non possiamo metterci d'accordo in separata sede sul metodo per criptare le informazioni trasmesse, e l'unico modo è quindi che il metodo di crittografia delle informazioni deve essere pubblico. Ma se il metodo è pubblico, allora sembrerebbe inutile criptare le informazioni, questo perché se tutti sanno come si cripta, allora teoricamente tutti sapranno come decriptare.

Ma fortunatamente non è sempre così La risposta sta nelle funzioni unidirezionali e nei numeri primi.

Sì quei numeri che ai tempi della scuola sembrava servissero solo per poter fare gli esercizi di scomposizione di numeri più grandi, apparente inutili per ogni applicazione pratica, ora scopriamo che, permettendo lo scambio di informazioni riservate tra due persone che non si sono mai viste prima, assumono oggi una grande importanza e sono tra gli elementi di base dello sviluppo di internet

E poi ci sono le funzioni unidirezionali.

Esistono infatti due tipi di funzioni: quelle bidirezionali e quelle unidirezionali. La differenza tra le due è che nel primo caso è possibile l'operazione inversa, nel secondo no.

Ad esempio se stabiliamo che la chiave di criptazione del numero (per un computer anche le lettere sono identificate con numeri, detti codici ASCII) che vogliamo trasmettere è il doppio più 3, allora se il nostro messaggio da trasmettere è 88, quello che andremo a

trasmettere sarà 179, ma questa crittografia servirà a ben poco se chi ci sta spiando conosce la regola per la crittografia utilizzata perché pubblica. Ricalcolare il numero di partenza è un gioco da ragazzi.

Se la chiave di criptazione è una funzione unidirezionale, ad esempio il resto che si ottiene dividendo il numero da trasmettere per 10, quello che noi andremo a trasmettere sarà 8. Ma non è possibile, una volta ricevuta l'informazione, sapere se il numero del messaggio era 8, 18, 28, 38, e così via. Questo tipo di funzione univoca, chiamata modulo, è stata sviluppata da Gauss nel XIX secolo.

Viene scritta mod(12) e tra parentesi indichiamo il divisore, che può essere un numero intero a piacere diverso da 0. In realtà è una funzione che usiamo inconsciamente tutti i giorni, per comunicare l'ora: chi non sa che 17 mod(12) è uguale a 5 ?

Ma ci sono casi in cui funzioni più complesse contenenti mod() possono diventare bidirezionali, ma solo per chi conosce un segreto: il divisore deve essere il prodotto di due numeri primi noti, e chiameremo questo numero chiave pubblica.

Se il negozio ci fornisce tale chiave ed un altro numero a piacere detto ausiliario, anche se tale informazione è visibile a tutti, solo il negozio, che conosce i due numeri primi utilizzati per la creazione della chiave pubblica sarà in grado di ricalcolare il numero di partenza.

Ovviamente come prodotto di due numeri primi non andremo certo a scegliere il prodotto di due numeri "facili", come potrebbe essere 17 x 23 = 391, ma andremo a cercare due numeri primi formati da un numero elevato di cifre, numeri come 349052951084765094914784961990389813341776463849338784399082057 7, numeri la cui sola conoscenza è alla portata di pochi e per tale motivo hanno anche un rilevante valore economico.

Dalla corretta scelta della coppia di numeri primi, ed anche dal loro frequente rinnovarsi, dipenderà la sicurezza delle informazioni inviate tramite internet.

Ma continuiamo con il nostro esempio.

Immaginiamo come nel caso precedente di dover trasmettere il numero 88 e di avere ricevuto come chiave pubblica il numero 391 e come numero ausiliario 7.

Per crittografare il nostro messaggio calcoleremo il resto della divisione per 391 del nostro numero (88) elevato al numero ausiliario, ovvero 7.

88^7 mod(391) = 40.867.559.636.992 mod(391) = 130.

Dal numero 130 inviato come messaggio, noti solo la chiave pubblica ed il numero ausiliario, è pressoché impossibile risalire al numero di partenza.

Ad esempio si potrebbe sommare 391, ottenendo 521, la cui radice settima è 2,444.

Allora proviamo a sommare due volte 391, ottenendo 912, la cui radice settima è 2,647 e così via.

Con i numeri piccoli da noi scelti occorreranno poco più di 104 miliardi di tentativi che, se immaginiamo un tentativo ogni millesimo di secondo, farebbero comunque più di 3 anni.

Se i numeri fossero molto più grandi, i tempi richiesti aumenterebbero in modo esponenziale.

Però, se sappiamo che 391 è il prodotto tra 17 e 23, allora possiamo ricavare il numero di partenza con un calcolo che, per quanto complesso, può essere svolto in un secondo da un elaboratore.

Tutto questo grazie alla geniale intuizione dei matematici, Diffie, Merkle ed Hellman. Siamo nel 1975 e con la loro intuizione, si sono gettate le basi della crittografia a chiave pubblica, base per il futuro sviluppo del commercio elettronico.
Per i più temerari, in appendice è riportato il procedimento per ricalcolare il numero originale.

Appendice: la decodifica del messaggio
Occorre innanzitutto calcolare un numero di decodifica, tale per cui
7 x D = 1 mod((17-1)(23-1))
Dove 7 è il numero ausiliario e 17 e 23 sono i due numeri primi il cui prodotto è la chiave pubblica.
Svolgendo i calcoli:
7 x D = 1 mod(352)
D = 1mod(352) / 7
1mod(352) non è un numero soltanto, ma una serie di numeri multipli di 352 cui è stato aggiunto 1 e dobbiamo scegliere tra questa serie il primo divisibile per 7. Bastano pochi tentativi per trovare 1056 (352x3 +1)
Ne consegue che la nostra chiave di decodifica sarà uguale a 1056 / 7 = 151
Per decodificare il nostro numero occorre applicare la seguente formula:
130 ^ 151 (mod391) ossia il resto che si ottiene dividendo per la chiave pubblica il numero del messaggio elevato per la chiave di decodifica.
Ma come facciamo a calcolare 130 ^ 151? E' troppo grande.
In realtà a noi non interessa sapere esattamente quanto fa, ma solo qual è il suo resto una volta diviso per 391. Possiamo quindi sfruttare le proprietà dei moduli e scomporre il numero nei suoi fattori:
dato che 130 ^ 151 = (130 ^ 7)^21 x 130^4 (gli esponenti sono stati scelti in base alla capacità di visualizzazione delle cifre della mia calcolatrice) allora
130 ^ 151 mod (391) = ((130 ^ 7 mod(391))^21 x 130 ^ 4 mod(391))mod(391)

si noti che 7 x 21 + 4 = 150. Fatti i calcoli ricaviamo
= (241^21 x 140) mod(391)
ancora troppo grande. Ma possiamo proseguire allo stesso modo
= ((241^6 mod(391))^3 x 241^3 mod(391) x 140) mod(391)
= (32^3 x 112 x 140) mod (391)
= 513802240 mod(391)
= 88

Alla prossima!

Ugo Zaroli