time key" in quanto la chiave può essere utilizzata una sola volta dato che generalmente ha una validità temporale modesta (10-20 secondi) dopo che è generata da un dispositivo elettronico (key generator) che è sincronizzato con il sistema di controllo di accesso al servizio.

Conclusioni

Alla base della criptografia c'è la matematica, in particolare:
A l'artimetica modulare, con lo studio dei resti delle divisioni aritmetiche;
B la teoria dei numeri, in particolare quella dei numeri primi.

Artimetica modulare

Nella aritmetica modulare il quoziente nell'operazione di divisione è irrilevante mentre unica importanza lo assume il resto, e viene così indicato:
Q il quoziente della divisione fra il dividendo **X** e il divisore **m**, mentre è **R** il resto e viene indicato con la seguente notazione:

$$X(\text{mod } m) = R$$

che si legge: "X modulo m è uguale a R" e si dice anche "R è congruo a X modulo m".

ESEMPIO

Vediamo alcuni esempi:
- $14(\text{mod } 4) = 2$
- $79(\text{mod } 7) = 2$
- $21(\text{mod } 33) = 21$ dalla quale deduciamo che $X(\text{mod } m) = X$ se $X < m$
- $37(\text{mod } 37) = 0$ quindi $m(\text{mod } m) = 0$
- $27(\text{mod } 1) = 0$ quindi $X(\text{mod } 1) = 0$
- $77(\text{mod } 76) = 1$ quindi $(m + 1)(\text{mod } m) = 1$

Possiamo fare tre osservazioni sul resto R:
- vale sempre la relazione $R < m$;
- tutti i possibili resti sono in numero pari a m e con valori compresi fra 0 e $m - 1$, e l'insieme dei resti viene indicato con $Z_n = \{0, 1, 2, \dots, n - 1\}$;
- se $X < m$ allora $X(\text{mod } m)=X$.

CLASSE DI RESTI

Dato un numero intero positivo *X*, i numeri interi si distribuiscono in *X* classi di resto modulo m, a seconda del resto che danno quando vengono divisi per *m*.

Valgono inoltre le seguenti due equivalenze:

(X + Y)(mod m) = X(mod m) + Y(mod m), e cioè: ***il resto di una somma è pari alla somma dei resti***
(X Y)(mod m) = X(mod m) Y(mod m), e cioè: ***il resto di un prodotto è pari al prodotto dei resti***.

L'equivalenza sul prodotto conduce alla importante equivalenza sul quadrato:

il resto di un quadrato è pari al quadrato del resto

$$X^2(\text{mod m}) = (X \cdot X)(\text{mod m}) = x(\text{mod m}) \cdot x(\text{mod m}) = R \cdot R = R^2$$

Grazie a questa equivalenza sarà possibile determinare resti di divisioni fra numeri con un incalcolabile numero di cifre, base della crittografia a chiave pubblica che utilizza i numeri primi.

ESEMPIO

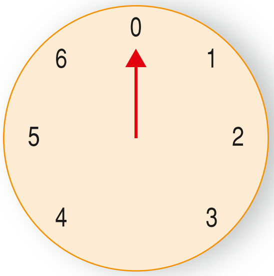
A 13^2(mod 11) = 169(mod 11) = 4 = 13(mod 11) · 13(mod 11) = 2 · 2 = 4
B 25^2(mod 7) = 625(mod 7) = 2 = 25(mod 7) · 25(mod 7) = 4 · 4 = 16

16, essendo maggiore di m, deve essere ulteriormente elaborato ottenendo:

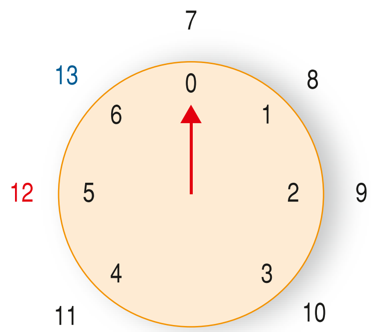
$$16(\text{mod } 7) = 2$$

L'aritmetica in modulo viene anche chiamata aritmetica *dell'orologio* in quanto è possibile ottenere il risultato considerando un orologio con m ore e muovendo la lancetta su di esso fino a che non si raggiunge il numero X di ore.

Vediamo ad esempio come risolvere 12(mod 7) =



Dopo il primo giro della lancetta dell'orologio sono trascorse 7 ore, quindi procediamo fino a raggiungere la 12_{ima} ora, che corrisponde al numero 5, che è anche il nostro risultato.



Numeri primi

I numeri primi sono stati oggetto di studio dai matematici di ogni periodo storico: tutti sanno che un numero primo non è rappresentabile come prodotto di interi che lo precedono e si dice primo se è divisibile esattamente solo per 1 e per se stesso.
Ancora oggi il metodi più semplici per trovare tutti i numeri primi risale a qualche millennio fa, cioè al ben noto crivello di Eratostene.

I numeri primi sono stati utilizzati da Euclide che enunciò due teoremi su di essi:

TEOREMI DI EUCLIDE SUI NUMERI PRIMI

Primo Teorema di Euclide: ogni numero intero N si scrive in modo unico (a parte l'ordine) come prodotto di numeri primi.
Secondo Teorema di Euclide: i numeri primi formano una successione infinita.

Anche Eulero li studio ed enunciò un famoso teorema dal quale Fermat arrivo a promulgare il suo famoso piccolo teorema (dimostrato in seguito proprio da Eulero).

> Noi non entriamo in particolare nella trattazione dei numeri primi ma ci limitiamo a sottolineare che questi sono alla base della criptologia e si lascia l'approfondimento a chi è interessato allo sviluppo degli algoritmi di cifratura.

Simbologia utilizzata

Prima di proseguire riportiamo la simbologia che viene normalmente utilizzata nei testi di crittografia.

Generalmente plaintext e ciphertext si indicano rispettivamente con le lettere m (come "**m**essaggio") e c (come "**c**odice"); la chiave con il simbolo k ("**k**ey").
La funzione di cifratura viene indicata con il simbolo f, con f^{-1} quella di decifratura (alcuni testi riportano la lettera E (**E**ncrypt)).

Possiamo scrivere quindi la procedura di cifratura con la seguente espressione:

$$c = F_k(m)$$

oppure

$$c = E_k(m)$$

e per la decifratura

$$m = f_k^{-1}(c)$$

o

$$m = E_k^{-1}(c)$$

Nel caso di chiave simmetrica, dato che si utilizza la stessa chiave per la cifratura e la decifratura si può scrivere:

$$m = f_k^{-1}(f_k(m))$$

e quindi:

$$m = E_k^{-1}(E_k(m))$$

Nel resto della nostra trattazione utilizzeremo la seconda notazione, cioè:
- per la cifratura $c = E_k(m)$
- per la decifratura $m = E_k^{-1}(c)$