Gli strumenti matematici per l’utilizzo degli algoritmi di crittografia

Autore:
In: Diritto civile e commerciale

Alcuni strumenti matematici che risultano essere di grande utilità nell’utilizzo di algoritmi di crittografia sono cosi elencati:

1. Campi di Galois

Sono dei campi finiti (dove per campo intendiamo un insieme di “numeri” con due operazioni l’addizione e la moltiplicazione) che giocano un ruolo chiave in crittografia. Nei campi di Galois il numero di elementi deve essere una potenza di un numero primo, nello specifico vengono utilizzati i Campi di Galois che si basano sulla potenza del numero primo 2, definiti GF(p2). In particolare i più usati sono:

a)

GF(p)

b)

GF(2n)

Dove GF(p) è un insieme di interi {0,1, … , p-1} con le operazioni di addizione e moltiplicazione in modulo p.

2. Un altro strumento matematico utilizzato per lo sviluppo di algoritmi crittografici è l’aritmetica

Diritto & Diritti ISSN 1127-8579

polinomiale modulare che viene utilizzata ad esempio per l'algoritmo di crittografia asimmetrico RSA, la cui validità è data da una coppia di numeri primi fra loro difficili da fattorizzare. Praticamente RSA critta solamente la chiave di cifratura utilizzata dal cifrario simmetrico. Tale chiave viene generata in modo randomico ogni volta che si cifra un messaggio. Attualmente la ricerca si è rivolta verso l'applicazione delle funzioni di hash, che si basano sulla non invertibilità (un esempio tipico di funzione di hash è quello dell'attacco del compleanno) e delle curve ellittiche, basate sulla teoria dei numeri.

a cura del Dottor Antonio Guzzo

Responsabile CED

Sistemi Informativi del Comune di Praia a Mare

https://www.diritto.it/gli-strumenti-matematici-per-l-utilizzo-degli-algoritmi-di-crittografia/

Diritto & Diritti ISSN 1127-8579