di Massimo Nannini

L'IMPORTANZA DELLA CRITTOGRAFIA OMOMORFICA

La crittografia omomorfica consente sia la crittografia dei dati e allo stesso tempo ne permette la loro elaborazione in forma criptata

La crittografia è conosciuta ed utilizzata sin dai tempi antichi, soprattutto in ambito militare, per celare al nemico informazioni che, se conosciute, avrebbero potuto cambiare le sorti dei conflitti. Anche Giulio Cesare aveva capito l'importanza di questo strumento tanto che nelle sue comunicazioni militari utilizzava un sistema di cifratura che consisteva nella sostituzione di ciascuna lettera con quella che la seguiva di un numero fisso di posizioni nell'alfabeto.
Il Dizionario Treccani riporta la seguente definizione di Crittografia: "Tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in essa contenuta possa essere recepita solo dal destinatario; ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile".
Cifrare un dato significa renderlo incomprensibile a tutti tranne al destinatario che, possedendo la "chiave" di decifratura, è in grado di accedere al messaggio nella sua forma originaria. La cifratura a chiave simmetrica prevede l'utilizzo di una sola chiave sia per "nascondere" il messaggio sia per "leggerlo". La cifratura a chiave asimmetrica prevede l'utilizzo di due chiavi interdipendenti, una per crittografare i dati e l'altra per decodificarli.

Come funziona e perché è importante la crittografia omomorfica

La crittografia omomorfica detta anche omomorfa è una tipologia di crittografia a chiave pubblica che prende il suo nome dal concetto matematico di omomorfismo algebrico.
In algebra astratta un omomorfismo è una trasformazione che applicata ad una struttura dati ne produce una nuova con la stessa struttura e dove le operazioni produrranno risultati equivalenti.
Poiché la trasformazione applicata non è altro che l'algoritmo di criptazione, la criptografia omomorfica definisce che le operazioni effettuate sui dati in chiaro sono equivalenti a quelle effettuate sui dati cifrati.
Si tratta dunque di trovare un algoritmo di criptazione (trasformazione) omomorfo per cui sia possibile applicare all'insieme dei dati trasformati tutte le possibili operazioni ammesse sull'insieme di partenza.
Ad oggi esistono due tipi principali di crittografia omomorfica quella parziale (PHE) e quella completa (FHE).
La crittografia PHE contempla l'utilizzo di una sola operazione matematica sui dati crittografati, nello specifico addizioni o moltiplicazioni per un numero illimitato di volte. La versione basata sulla moltiplicazione è la base della crittografia RSA utilizzata nel protocollo SSL/TSL.
La crittografia (FHE) contempla l'utilizzo di qualunque tipologia di calcolo per un numero illimitato di volte.
Questa ultima tipologia è decisamente la più ambita perché consente di preservare il dato fin dall'origine, concedendo la possibilità di effettuare qualunque tipo di elaborazione senza mai rivelare il vero contenuto dei dati stessi.
Due sono dunque i fronti aperti su cui la comunità scientifica ed i grandi player dell'IT stanno lavorando, da un lato aumentando le capacità elaborative attraverso lo sviluppo di acceleratori hardware dedicati alla fully homomorphic encryption e dall'altro la ricerca di algoritmi più efficienti in grado di velocizzare i calcoli sui dati cifrati.
Siamo solo all'inizio di un percorso che permetterà di avere accesso ad una grande quantità di dati presenti nel cloud, utilizzabili soprattutto a fini statistici e nel machine learning, senza per questo avere la necessità di decriptarli salvaguardando così la privacy dei singoli utenti.

***Massimo Nannini**
Ingegnere elettronico e consulente di impresa
info@gemaxconsulting.it