# MATEMATICA PER LA TECNOLOGIA: CRITTOGRAFIA, BLOCKCHAIN E CRIPTOMONETE

## LAUREA IN MATEMATICA PER L'INGEGNERIA

COLLEGIO DI INGEGNERIA MATEMATICA
DIPARTIMENTO DI SCIENZE MATEMATICHE "G. L. LAGRANGE"
POLITECNICO DI TORINO

# Crittografia, blockchain e criptomonete

Il mondo di oggi è sempre più digitalizzato. Le comunicazioni avvengono soprattutto tramite la posta elettronica, le chat, i social e le video call e molte operazioni con un valore legale ed economico sono svolte on line. Per mantenere un livello adeguato di sicurezza e di privacy è quindi fondamentale che i dati di tutte queste comunicazioni e transazioni siano cifrati, quindi leggibili solo da chi ne ha l'autorizzazione, e ci sia certezza sull'identità del mittente. Lo strumento fondamentale per assicurare tutto ciò è la crittografia.

Diversamente da quanto si può pensare al centro della Crittografia non ci sono tanto le implementazioni degli algoritmi di cifratura e decifratura dei dati, ma soprattutto la capacità di identificare strutture e proprietà matematiche che permettano di costruire sistemi efficienti e sicuri di offuscamento dei dati, di garanzia di autenticità e di identità degli utenti.

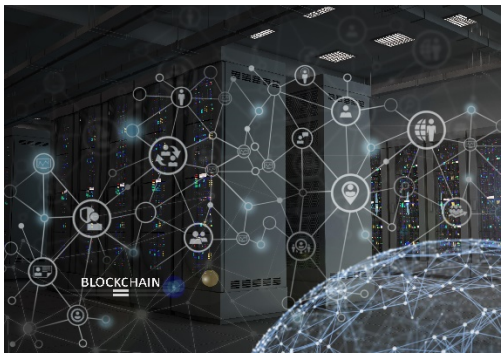


*Figura 1: Blockchain (Credits: ID 106051171 © Ravil Sayfullin | Dreamstime.com, 24/08/2021).*

Per usare questo strumento così fondamentale nell'economia del digitale non serve essere dei matematici, ma per capire veramente la Crittografia e ancora di più per modificare i sistemi esistenti o crearne di nuovi, è fondamentale una buona conoscenza della Matematica, in particolare dell'Algebra e della Teoria dei numeri.

Per esempio, una proprietà elementare dei numeri naturali, e molto utilizzata in crittografia, è che dati due numeri primi $p$ e  è molto semplice e veloce moltiplicarli e determinare $n=pq$. Se invece si conosce $n$ è molto più difficile risalire ai suoi fattori $p$ e $q$. Certo tutti sono in grado di fattorizzare $n=15$ come $3x5$, ma se il numero $n$ in questione ha centinaia di cifre, anche con i più potenti computer esistenti e con i migliori algoritmi di fattorizzazione, il tempo per risalire da $n$ ai due fattori $p$ e $q$ è dell'ordine dei millenni!

Nel 1991, per incoraggiare la ricerca nella Teoria dei numeri computazionale, gli RSA laboratories hanno selezionato un certo numero di interi molto grandi, i cosiddetti RSA-numbers, ottenuti dal prodotto di coppie accuratamente scelte di numeri primi, lanciando ai matematici di tutto il mondo la sfida di trovarne una fattorizzazione.

Tra gli RSA-numbers il più grande ad essere stato fattorizzato è R-250, il seguente enorme numero di 250 cifre:

RSA-250
=214032465024074496126442307283933356300861471514475501779775492088141802344714013664334551909580467961099285187247091458768739626192155736304745477052080511905649310668769159001975940569345745223058932597669747168173806936489469987157849497593749793 7.

La sua fattorizzazione è stata ottenuta nel 2020 da Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, e Paul Zimmermann[1] ed i suoi fattori sono

$p$=64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367,

$q$=33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711.

Tutti gli RSA-numbers più grandi non sono stati ancora fattorizzati e la sfida prosegue oramai da oltre 30 anni.[2]

[1] [Cado-nfs-discuss] Factorization of RSA-250, https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html

[2] https://it.wikipedia.org/wiki/Numeri_RSA

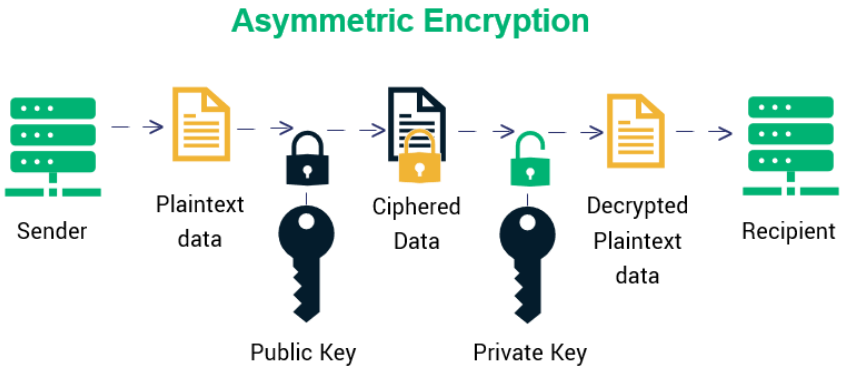


*Figura 2: Algoritmo di decifratura (Credits: https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/, 24/08/2021)*

Sul problema della fattorizzazione sono costruiti i più semplici, ma comunque molto sicuri, sistemi di crittografia asimmetrica. Rendendo pubblico il numero *n* e utilizzandolo come chiave per la cifratura dei dati, e tenendo invece segreti *p* e *q*, necessari invece per l'algoritmo di decifratura, si possono costruire sistemi dove chiunque può cifrare i dati, essendo *n* pubblico, e mandarli a chi conosce opportune informazioni su *p* e *q*, che sarà l'unico a poterli decifrare, sfruttando gli strumenti della Teoria dei numeri.
Si può costruire un sistema analogo, ma più sicuro a parità di dimensione delle chiavi, considerando come spazio di riferimento, invece dei numeri interi, l'insieme dei punti di una curva ellittica e sfruttando l'operazione di somma definita tra i punti di tale curva, al posto dell'usuale somma tra interi.

Esistono tante altre strutture matematiche, con le relative operazioni e teoremi, che possono essere utilizzate per costruire sistemi con diverse caratteristiche di sicurezza e di versatilità ed è per questo che la Crittografia è fortemente basata sulla Matematica.

A sua volta la Crittografia può diventare la base per costruire tecnologie molto interessanti e complesse e senza dubbio la Blockchain è una delle più promettenti. Grazie alle funzioni hash, ai sistemi crittografici a chiave pubblica e alla firma digitale, è possibile definire una struttura di dati a blocchi, detta appunto Blockchain (catena di blocchi), che ha una particolare resistenza ad essere modificata e che quindi permette di costruire un archivio dove registrare delle transazioni, sostanzialmente impossibili da contraffare.

È implementando questa struttura che un non identificato programmatore (sotto lo pseudonimo di Satoshi Natamoto) ha creato nel 2009 la prima criptomoneta e la più famosa delle blockchain: Bitcoin. Negli anni successivi sono state ideate e implementate molte altre criptomonete, alcune simili a Bitcoin e altre anche molto diverse. Nel 2021 il mercato delle criptomonete è arrivato a superare i 1.500 miliardi di dollari di valore e le criptomonete acquistabili nei maggiori exchange sono più di 4.500.

*Figura 3: Bitcoin (Credits: ID 130168548 © Syda Productions | Dreamstime.com, 24/08/2021)*

Gli aspetti interessanti delle criptomonete non risiedono solo nell'essere monete alternative alle valute fiat e nell'essere totalmente digitali e anonime, senza un'autorità centrale che le controlli, ma soprattutto nelle loro particolari proprietà che le rendono utilizzabili come una sorta di denaro programmabile e eventualmente con caratteristiche particolari come la non fungibilità, aprendo possibilità commerciali impensabili con le normali monete.

La difficoltà più grande che è stata affrontata per creare le criptomonete è stata trovare modi affidabili per ottenere un accordo di tutta la rete sui passaggi di proprietà, i cosiddetti protocolli di consenso.

Una volta ideati questi protocolli che permettono di trovare un consenso sulle transazioni fra persone che non si conoscono e che quindi generalmente non si fidano le une delle altre, si sono aperte possibilità veramente dirompenti che potrebbero cambiare in modo radicale il nostro mondo e l'intera struttura della nostra economia: servizi di assicurazione, senza le società di assicurazione,

servizi finanziari, senza le società finanziarie, servizi di notarizzazione, senza i notai, servizi bancari, senza le banche...

La decentralizzazione permessa dalla Blockchain e la conseguente obsolescenza delle autorità centrali, cambierà il nostro mondo e lo sta già facendo.


*Figura 4: Le competenze più richieste per il 2020 (Credits: https://www.linkedin.com/business/learning/blog/learning-and-development/most-in-demand-skills-2020?epik=dj0yJnU9VE8wMU5IOTJoWEVYYjB6TnVZaGNCbzdiLXBfQ2ZTYlkmcD0wJm49azZqbHBXV1U5aW9LRmxNMDZKZVMwdyZ0PUFBQUF, 24/08/2021)*

Per gestire questa rivoluzione e non esserne travolti è fondamentale il contributo degli esperti di Crittografia e della tecnologia Blockchain. Nei corsi di laurea di Matematica per l'Ingegneria e Ingegneria Matematica, potrete ricevere una formazione matematica generale all'interno della quale vi sarà possibile inquadrare oltre a importanti conoscenze teoriche, anche una formazione più specifica in questi campi. Figure professionali che siano dotate di tale formazione sono già estremamente richieste dal mercato e sempre più lo saranno, come si può dedurre consultando: https://www.linkedin.com/business/talent/blog/talent-strategy/linkedin-most-in-demand-hard-and-soft-skills