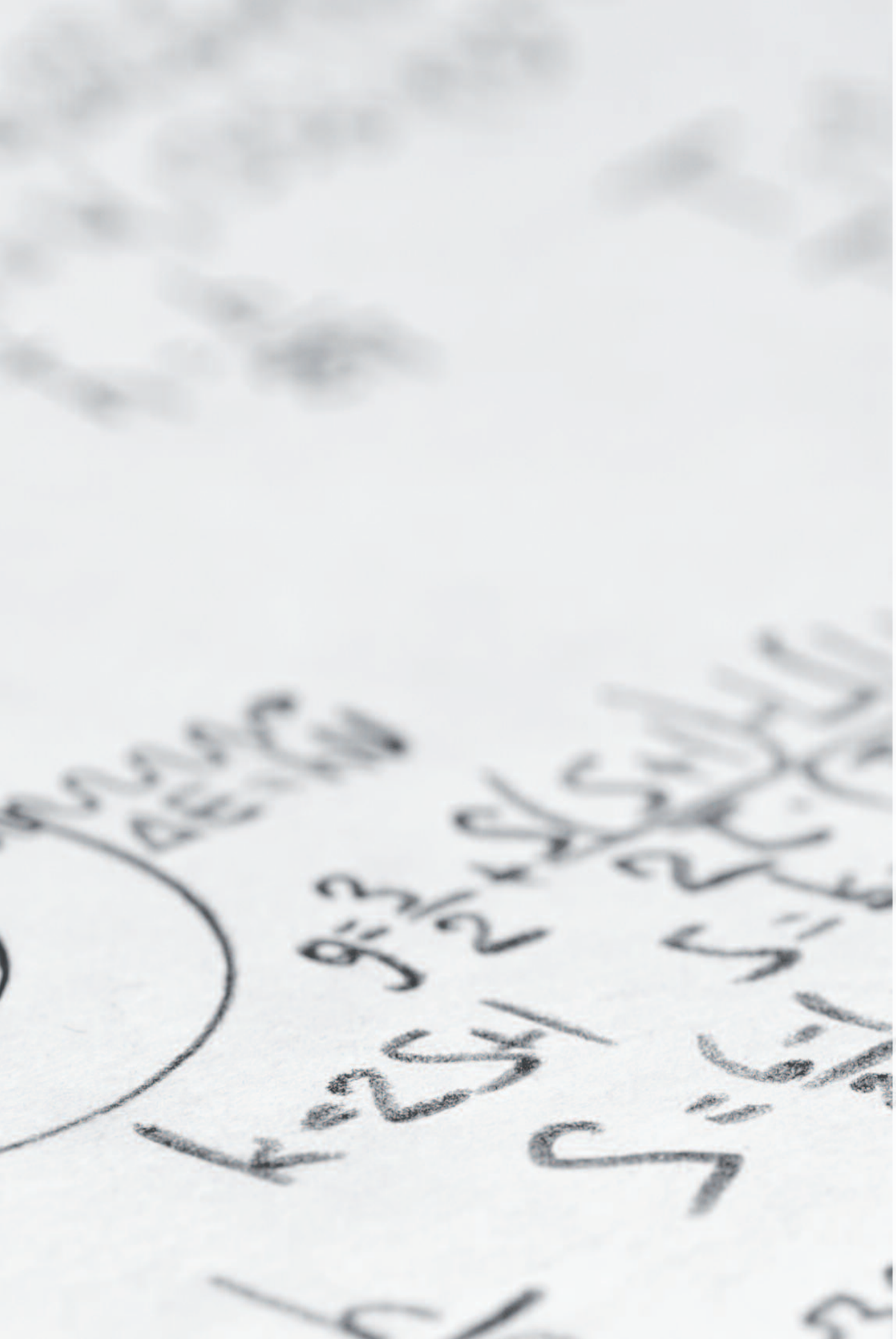

Crt

I pratici effetti dell'astrazione matematica nella crittografia

Marco Baldi – Michele Elia – Massimiliano Sala

L'identificazione della matematica astratta con la crittografia ha consentito di formulare e risolvere problemi altrimenti insuperabili. L'ubiquità del sistema di telecomunicazioni ha permesso la dislocazione di un gran numero di operazioni presso l'utente, quali servizi bancari, servizi postali, vendite e transazioni commerciali, solo per elencarne alcune, ponendo problemi di sicurezza sconosciuti in passato. La tecnologia crittografica è maturata giusto in tempo per offrire a questo assetto globale gli strumenti indispensabili per assicurarne funzionalità e sicurezza. Antichi e profondi risultati teorici della matematica hanno fornito la chiave di volta che ha consentito di eseguire operazioni delicate o riservate a distanza su scala mondiale senza ridurne la sicurezza.

In order for the light to shine so brightly, the darkness must be present.
Francis Bacon

Le basi assiomatiche della crittografia poste da Claude Elwood Shannon (1916-2001) hanno permesso di rivederne sia il ruolo sia le potenzialità, anche alla luce della nascente società dell'informazione e dei computer. Il tempo per assimilare il profondo significato della visione che Shannon ebbe della crittografia è stato giusto quello in cui la società mondiale ha conosciuto uno sviluppo senza precedenti, raggiungendo uno stato di opulenza mai immaginato. Trascorsi circa vent'anni dalla Seconda guerra mondiale, nelle prospere economie degli stati nazionali, con la globalizzazione della produzione industriale e agricola, l'espansione dei commerci e la conseguente diffusione del sistema bancario, si è posto il problema di realizzare telecomunicazioni sicure e, nello stesso tempo, disponibili su amplissima scala a costi sostenibili. Allora fu necessario realizzare strutture di protezione dell'informazione semplici, sicure e praticabili da non specialisti. Eserciti e governi usavano da secoli metodi di cifratura basati sulla conoscenza di un segreto condiviso, chiamato chiave. Tali metodi erano dispiegati mediante macchine cifranti sicure ma economiche,

utilizzate da personale addestrato ma non esperto in crittografia, e fu naturale proporre soluzioni cifranti standardizzate. Nello specifico del sistema bancario, l'elevata quantità di connessioni tra agenzie periferiche e banche centrali, protette da sistemi di cifratura proprietari, sollevò in termini pratici sia quello dell'intercomunicazione sia il problema della distribuzione delle chiavi.

Problema, quest'ultimo, che l'esperienza bellica appena trascorsa aveva dimostrato essere molto critico. Nei primi anni 70 del secolo scorso il National Bureau of Standard (Nbs) americano, ora denominato National Institute for Standards and Technology (Nist), sollecitò le industrie interessate a proporre un algoritmo di cifratura per comunicazioni sensibili di dati civili non classificati. L'algoritmo che parve poter rispondere meglio alle specifiche di uno standard e che destò l'interesse dell'Agenzia fu quello su cui si lavorava all'Ibm, basato su una funzione bilanciata, inventata dal matematico tedesco Horst Feistel. Inoltre, la vastità delle connessioni bancarie, protette da metodi proprietari di cifratura dei dati senza alcuna certificazione, richiedeva un ingente e costoso traffico di chiavi segrete, difficile da gestire. Maturò allora l'idea di scambiare piccoli set di dati (le chiavi) in maniera sicura sui canali pubblici e senza accordi preventivi. Questa stravagante intuizione, come tutte quelle molto originali, poteva apparire impraticabile finché nel 1976 due giovani ricercatori dell'università di Stanford in California, Bailey Whitfield Diffie e Martin Edward Hellman, dimostrarono che, in linea di principio, il problema dello scambio pubblico di chiavi segrete era risolvibile. In realtà, già nel 1970 il crittografo inglese James Henry Ellis, impiegato nei Servizi d'intelligence presso il Government Communications Headquarters (Gchq), aveva formulato l'ipotesi di 'cifratura non segreta', ma non era stato possibile pubblicare il suo lavoro classificato. La proposta di crittografia a chiave pubblica fu quasi coeva con l'ufficializzazione del primo standard per crittografia in chiave privata, il Data Encryption Standard (Des). La rivoluzionaria idea scatenò molteplici controversie e venne accolta con diffidenza negli ambienti della National Security Agency (Nsa), perché erroneamente ritenuta in concorrenza con gli standard di cifratura classica in chiave privata che si stavano proponendo. Va rilevato che l'introduzione, nel 1977, dello standard Des e la sua successiva diffusione hanno avuto come indiretto e positivo effetto la divulgazione della cultura crittografica in ambienti che ne erano tradizionalmente sprovvisti. Come accennato, solo negli anni 60 del secolo scorso si è dato seguito ad alcune intuizioni di Shannon, tra cui due principi di cifratura.

Il primo consiste nel far eseguire in sequenza molte operazioni semplici (*round*), ognuna dipendente dalla chiave in maniera diretta, di modo che il risultato dell'operazione appaia incomprensibile all'attaccante sprovvisto di chiave.

Il secondo è compendiabile nella necessità di realizzare il sistema crittografico in modo tale da non poter essere attaccabile, anche nell'improbabile ipotesi che un abilissimo avversario riesca a convertire il problema critto-analitico in un problema matematico ben definito. Anzi, la laboriosità del problema matematico sottostante rafforza, secondo Shannon, la confidenza degli utilizzatori del cifrario stesso.

I primi cifrari di questo tipo apparvero solo negli anni 60, quando fu possibile effettuare con una macchina delle operazioni molto più complesse di quelle eseguite dalle macchine cifranti belliche e dell'immediato periodo post-bellico. Questi sistemi di cifratura sono chiamati cifrari a blocchi perché richiedono di cifrare un blocco di bit alla volta. Il primo esempio di largo utilizzo fu proprio il Des che, rilasciato come standard, fu subito adottato da grandi multinazionali e sostenuto da tecnologie di ampio consumo e penetrazione. Esso rispondeva appieno al primo principio di Shannon, essendo formato da ben 16 round consecutivi, ma era ben lontano dal secondo principio, in quanto la giustificazione nella scelta delle componenti matematiche del cifrario era oscura e poco motivata. Nonostante quest'aspetto avesse suscitato dubbi negli ambienti crittografici più attenti, il Des ebbe una diffusione enorme e lanciò lo studio dei cifrari a blocchi finché, tra la fine degli ani 80 e l'inizio degli anni 90, arrivarono nuove sofisticate tecniche di crittoanalisi specializzate per quei cifrari, tra i quali ricordiamo la devastante tecnica di crittoanalisi differenziale a opera di Adi Shamir e Eli Biham, che ne distrusse moltissimi in pochi anni. Il Des, che pur aveva resistito più di altri, dovette soccombere, sul finire del secolo scorso, al continuo miglioramento tecnologico che rendeva disponibile agli attaccanti computer sempre più potenti. Nel 2001 fu così rimpiazzato dallo standard attuale, l'Advanced Encryption Standard (Aes), ma il Nist, memore anche del secondo principio di Shannon, bandì una gara pubblica aperta a tutti coloro che volessero presentare nuove idee, purché supportate da motivazioni matematiche sulla robustezza del cifrario proposto. A quattordici anni dalla sua ufficializzazione, l'Aes è il cifrario a blocchi più usato del mondo, appena scalfito da un mirato e sofisticato attacco nel 2011.

È una coincidenza, difficile dire quanto fortuita, che la matematica utilizzata in Des e Aes e quella per realizzare le idee di Diffie e Hellman sulla crittografia in chiave privata avessero le stesse radici nell'aritmetica come si era sviluppata nei secoli, e che avevano trovato una quasi prodigiosa formulazione per merito di Carl Fredrick Gauss. La teoria dei numeri, che aveva sempre avuto il ruolo di raffinato gioco intellettuale, divenne negli anni 70 l'unico strumento teorico della crittografia. Non è questa la sede per una digressione tecnica sull'algebra moderna e sull'aritmetica ma, solo per illustrare le direzioni in cui la crittografia è orientata, è utile richiamare il semplice concetto di aritmetica modulare che, fino a qualche anno fa e non con questo nome, era esemplificata nelle scuole italiane dalla

prova del nove per le moltiplicazioni di numeri interi. Fu un'intuizione di Gauss quella di considerare un'aritmetica nell'insieme dei resti della divisione per un intero prefissato che fu detto 'modulo'. Nella prova del nove, il modulo è il 9, e i possibili resti sono i numeri da 0 a 8. Il test consisteva nel calcolare il resto della divisione per 9 di ciascun fattore, quindi si verificava se il prodotto di questi resti, eseguibile mentalmente, coincidesse col resto della divisione per 9 del prodotto dei numeri. Nella teoria dei numeri appare il concetto di complessità – peraltro ancor privo di una soddisfacente e risolutiva definizione. Argomentare con le aritmetiche modulari offre anche esempi di quanto sia difficile tale concetto: per il matematico è quasi banale, per altri appare molto ostico. Il concetto di complessità è, in sintesi, una nozione relativa dipendente dall'ambito in cui si opera.

L'idea su cui si fondò la chiave pubblica fu quella di richiedere una corrispondenza invertibile tra due sequenze distinte, costituite dallo stesso numero di numeri distinti e tale che, dato un numero della prima sequenza, fosse facile calcolarne uno della seconda, mentre dato un numero della seconda sequenza fosse molto difficile risalire a quello corrispondente della prima. Questo tipo di corrispondenza fu detto funzione one-way. In seguito venne introdotta una funzione, detta *trapdoor*, tale che fosse facile da calcolare in senso diretto ma per la quale fosse difficile (molto oneroso come calcoli) trovare il valore inverso, salvo che non si disponesse di particolari informazioni segrete. È sorprendente che l'idea di costruire tali funzioni abbia preso forma solo così di recente, dato che il quotidiano è ricco di esempi siffatti, come il miscelare due colori che è poi impossibile separare, oppure recuperare un oggetto caduto in un luogo recintato, se non si possiede la chiave per accedervi. Da queste banali osservazioni, peraltro, si può dedurre che la nozione astratta di funzione trapdoor, in termini tecnici, va intesa più ampiamente e non solo come una semplice corrispondenza calcolabile mediante somme e prodotti di numeri.

Al riguardo, merita ricordare il problema della moneta, più noto come problema dello zaino (*knapsack*), sia per l'originalità e sia per la temporanea importanza che ebbe come metodo per definire una funzione trapdoor. Seppure sia stato un tentativo fallito, è illustrativo dei metodi matematici usati. Si supponga di avere un insieme ordinato di cinque tagli di euro, rispettivamente da 1, 2, 5, 10, 20, e che l'informazione sia un numero che può essere rappresentato come somma di queste monete, ad esempio 17. L'informazione segreta è una stringa binaria di 0, 1, ove 1 indica che la moneta nella corrispondente posizione è considerata nella somma. Per esempio, a 17 corrisponde la stringa (0, 1, 1, 1, 0) poiché 17 è uguale a 2+3+10. Ora si supponga cha la chiave pubblica sia la sequenza 3, 6, 15, 30, 19, ottenuta moltiplicando per 3 i singoli numeri della sequenza 1, 2, 5, 10, 20 e prendendone i resti della divisione per 41.

Chi vuole cifrare 17 calcola il valore della corrispondente stringa binaria riferendosi alla sequenza pubblica, ovvero calcola la somma 6+15+30=51, per cui il messaggio pubblico da comunicare è 51. Chi riceve 51 lo moltiplica per 14 (numero che svolge il ruolo di chiave segreta), inverso di 3 modulo 41, e ottiene 714, che considerato modulo 41 ritorna 17, il numero segreto di euro da comunicare. Benché questo sistema celi apparentemente l'informazione segreta e implementi una funzione trapdoor (la cui chiave segreta è costituita dalla coppia di numeri 3, 41 e dal 14), esso nasconde una debolezza. Tale debolezza giace nel fatto che la sequenza originale deve necessariamente essere super crescente, ossia ogni numero della sequenza deve essere maggiore della somma di tutti quelli che lo precedono. Ciò rende la chiave segreta attaccabile in modo molto meno complesso di quanto appaia a prima vista.

Per offrire un esempio del tipo di soluzione da loro astrattamente proposta, Diffie e Hellman fecero ricorso a un problema elementare di teoria dei numeri riconducibile alla corrispondenza tra sequenze di numeri ricordata nella definizione di funzione one-way. La procedura proposta era incredibilmente semplice eppure ancora oggi valida. Si supponga che Alice e Bob vogliano stabilire un comune numero segreto impiegando solo il canale pubblico. Ciascuno dei due considera una sequenza di numeri ordinati in modo naturale e la costruisce impiegando un'opportuna regola matematica, tale che alla prima sequenza, nota come logaritmo discreto, ne corrisponda una costituita dagli stessi numeri e da tenere segreta; quindi ognuno sceglie un numero della seconda sequenza che invia all'altro tramite un canale pubblico (ad esempio, per posta ordinaria oppure per telefono). Eva può osservare il transito di informazioni sul canale pubblico e, quindi, conoscere i due numeri scambiati. Alice, ricevuto il numero pubblico di Bob, trova il corrispondente sulla seconda sequenza. Lo stesso fa Bob, se la regola di costruzione della seconda sequenza era stata scelta sagacemente, i due numeri trovati da Alice e Bob sono uguali. Siccome Eva non conosce le sequenze segrete di Alice e di Bob non può trovare il numero segreto.

La proposta di questa nuova procedura per la condivisione di chiavi segrete su un canale pubblico fu dirompente e determinò lo sviluppo della moderna crittografia a chiave pubblica. Lo scambio di chiavi di Diffie ed

Hellmann è inoltre alla base di molti moderni protocolli per la generazione e la distribuzione di chiavi segrete. Come spesso accade con i codici segreti, una procedura del tutto equivalente era stata già scoperta nel 1974 da Malcolm John Williamson, altro crittografo britannico impiegato presso il Gchq. Tuttavia, come per Ellis, il lavoro di Williamson fu declassificato dal governo britannico solo nel 1997.

Dovette comunque trascorrere un anno dalla scoperta di Diffie e Hellman per veder pubblicato il primo metodo pratico che producesse una funzione trapdoor utile per un sistema crittografico in chiave pubblica. Nel 1977 tre ricercatori del Massachusetts Institute of Technology (il mitico Mit) Ronald Rivest, Adi Shamir e Leonard Adleman, proposero una soluzione che fu denominata Rsa, dalle iniziali dei loro cognomi. Essi intuirono che il problema della fattorizzazione di grandi numeri interi presentava alcune caratteristiche che lo rendevano adatto a costruire una funzione trapdoor, e proposero un sistema crittografico in chiave pubblica basato sul calcolo di potenze di numeri nell'insieme dei resti, modulo un numero prodotto di due numeri primi. Due importanti caratteristiche del sistema Rsa, che oggi ne fanno uno dei più diffusi a livello globale, sono la brevità delle chiavi pubbliche e la capacità di non espandere la lunghezza dei messaggi dopo la cifratura. D'altro canto, però, le operazioni di cifratura e decifratura sono caratterizzate da una discreta onerosità di calcolo. Va ricordato che, anche in questo caso, un crittografo britannico del Gchq, Clifford Cristopher Cocks, era giunto alla stessa scoperta già nel 1973, ma anche il suo lavoro rimase coperto da segreto fino al 1997.

Più simile al principio di funzionamento di Diffie ed Hellman è invece il critto-sistema a chiave pubblica proposto da Taher ElGamal nel 1985. In questo caso, per costruire la funzione trapdoor, si sfrutta il problema del calcolo del logaritmo discreto. Lo schema di ElGamal ha però lo svantaggio che la versione cifrata di ciascun messaggio ha lunghezza doppia rispetto a quello in chiaro.

A questi primi sistemi se ne sono poi aggiunti altri, basati su funzioni trapdoor che sfruttano diversi problemi teorici, come il calcolo di punti sulle curve ellittiche (Koblitz e Miller, 1985), e la decodifica di codici correttori d'errore (McEliece, 1978). Quest'ultimo approccio ha assunto particolare rilevanza in epoca recente, perché capace di resistere agli attuali attacchi basati su computer quantistici. Infatti, le prime realizzazioni di computer quantistici stanno per diventare realtà. Ne è dimostrazione il programma da circa 80 milioni di dollari della Nsa, denominato *Penetrating Hard Targets*, che si prefigge, tra gli altri, l'obiettivo di realizzare un computer quantistico utile per scopi crittografici.

Un altro importante uso delle funzioni trapdoor consiste nella realizzazione di schemi per la firma digitale. Come per uno schema di firma tradizionale, si pensi al classico sigillo su ceralacca, un qualsiasi sistema di firma digitale deve avere i requisiti di autenticità (certezza del mittente), integrità (non modificabilità del messaggio firmato), non ripudio (innegabilità da parte del firmatario) e, opzionalmente, riservatezza del messaggio firmato. Un modo semplice per ottenerlo consiste nell'invertire le macchine cifranti e decifranti di un sistema di crittografia a chiave pubblica, a condizione che questo abbia determinati requisiti. Ciò ha consentito, ad esempio, di ottenere il diffuso schema di firma Rsa.

La combinazione di schemi di crittografia a chiave pubblica e firma digitale si trova nei moderni standard per la distribuzione di chiavi. Le corrispondenti soluzioni ingegneristiche oggi consentono a ciascuno di noi di utilizzare, da remoto e in sicurezza tramite internet, sistemi di home banking, commercio elettronico, posta elettronica certificata, telemedicina, e molte altre attività proprie della vita civile.

Con l'avvento di internet agli inizi degli anni 90, l'assetto mondiale delle telecomunicazioni ha consentito la connessione e la trasmissione di ogni tipo d'informazione in ogni parte del globo. Ha modificato l'antico sistema del commercio e dei rapporti sociali, ingenerando nello stesso tempo nuove problematiche di sicurezza. Nel contempo la diffusione dei personal computer con grandi capacità di calcolo e collegati in rete ha posto il problema del calcolo parallelo, con la necessità di eseguire detti calcoli in maniera distribuita ma sicura. Da tutte queste potenzialità e dalla condivisione di risorse per mezzo della 'rete', sono scaturite nuove sfide per i gestori delle reti e un'inaspettata fonte di problemi per i crittografi