Università degli Studi di Perugia

Dipartimento di Ingegneria

Corso di Laurea Triennale in Ingegneria Informatica ed Elettronica

La crittografia: dagli algoritmi a chiave simmetrica alle curve ellittiche

Relatore
Prof. Gianluca Reali

Laureando
Gian Marco Ferri

Anno Accademico 2021–2022

Indice

Prefazione

Il problema di scambiarsi informazioni private, che risultino indecifrabili da terze persone, è più che mai attuale. Se per secoli la crittografia è stata associata ad aspetti ben lontani dalla vita ordinaria e fino a pochi decenni fa veniva utilizzata soprattutto in ambito militare e governativo, al giorno d'oggi ciascuno di noi ne fa uso quotidianamente anche se spesso in maniera inconsapevole.

L'informatica e internet hanno reso il problema della segretezza delle comunicazioni sempre più rilevante. Attività quotidiane come l'utilizzo del telefono per chiamare o inviare messaggi, l'apertura dell'auto con il telecomando o l'utilizzo del bancomat ci portano a trasmettere informazioni che potrebbero essere intercettate e utilizzate contro di noi. Per evitare che ciò accada bisogna fare in modo che, anche se un'eventuale terza parte dovesse intercettare il nostro messaggio, questo sarebbe per lui incomprensibile. Lo stesso destinatario del messaggio avrà quindi la certezza che le informazioni non solo siano state mantenute segrete, ma anche che non siano state manomesse da terzi.

La crittografia si occupa proprio dell'insieme dei sistemi in grado di rendere incomprensibile un messaggio a chiunque ne venga in possesso ad eccezione del legittimo destinatario. Essa è una disciplina che ha un ruolo fondamentale in tutti quegli ambiti nei quali è necessario mantenere private delle informazioni riservate. Nata nell'antichità con la necessità di scambiarsi informazioni segrete,

soprattutto di tipo militare, oggi la crittografia ha molteplici applicazioni in ambito industriale, economico, civile, etc. Risulta evidente, pertanto, l'importanza di sviluppare tecniche e metodi di cifratura sempre più sicuri.

Ad oggi, possiamo distinguere due tipi di crittografia: la crittografia a chiave simmetrica e quella a chiave pubblica. Nella prima viene utilizzata un'unica chiave sia per cifrare che per decifrare i messaggi. La seconda, nota anche come crittografia asimmetrica, presuppone invece l'utilizzo di due chiavi: una pubblica e una privata.

L'introduzione della crittografia basata sulle Curve Ellittiche (ECC, Elliptic Curve Cryptography) è relativamente recente ma, negli ultimi dieci anni, tale tecnica si è rapidamente imposta come alternativa ai sistemi crittografici a chiave pubblica già largamente utilizzati, come l'algoritmo RSA. La principale attrattiva dell'ECC è che al momento non esistono algoritmi sufficientemente veloci che risolvano il problema matematico sul quale essa si basa. Ciò significa che la crittografia basata sulle curve ellittiche offre lo stesso livello di sicurezza dei sistemi tradizionali utilizzando chiavi di dimensione inferiore, richiedendo così elaborazioni più veloci, consumi energetici contenuti e un risparmio di utilizzo della banda. Tali caratteristiche quindi, rendono l'ECC particolarmente adatta all'utilizzo in ambienti con limitata disponibilità di risorse: palmari, telefoni cellulari, smart cards.

Obbiettivi e Organizzazione della Tesi

Questa Tesi si pone l'obbiettivo di presentare la Crittografia a chiave simmetrica, a chiave pubblica e quella basata sulle curve ellittiche, analizzando sia gli aspetti teorici che gli algoritmi utilizzati e soprattutto confrontando l'ECC con le moderne soluzioni a chiave pubblica.

Il primo capitolo introduce la crittografia in generale, con un excursus sulla sua storia; nei capitoli successivi viene poi presentato il funzionamento della crittografia a chiave simmetrica e a chiave pubblica, descrivendo anche i relativi algoritmi. Il quinto capitolo analizza le Curve Ellittiche e l'aritmetica ad esse abbinata. Viene trattato inoltre lo studio del problema matematico sul quale si basa l'ECC, ossia l'Elliptic Curve Discrete Logarithm Problem (ECDLP). Nel capitolo successivo viene affrontata la crittografia basata sulle Curve Ellittiche, mentre nel capitolo finale viene presentato il confronto tra l'ECC con altri sistemi a chiave pubblica, con le relative conclusioni a cui si giunge.

Acronimi

AES Advanced Encryption Standard

ANSI American National Standards Institute

CA Certificate Authority

DES Data Encryption Standard

DLP Discrete Logarithm Problem

DSA Digital Signature Algorithm

ECC Elliptic Curve Cryptography

ECDLP Elliptic Curve Discrete Logarithm Problem

ECDSA Elliptic Curve Digital Signature Algorithm

ISO International Standards Organization

RSA Rivest Shamir Adleman

Capitolo 1

Cenni storici sulla crittografia

La Crittografia (dall'unione di due parole greche "kryptós" che significa "nascosto" e "graphía" che significa "scrittura") è la disciplina che studia le tecniche per trasformare un messaggio, detto testo in chiaro, in un altro messaggio, detto testo cifrato, in modo che risulti incomprensibile a chiunque non conosca tutti i dettagli della tecnica usata per la trasformazione (o sistema di cifratura).

Un tale messaggio si chiama comunemente "crittogramma"; esso è apparentemente privo di significato e tale che solamente al legittimo destinatario sia possibile estrarre l'informazione trasmessa. Il sistema funziona se mittente e destinatario condividono un segreto di cui l'avversario non deve essere a conoscenza: questo segreto costituisce la "chiave" del sistema che permette di tradurre il "testo cifrato" nel "testo in chiaro", ovvero il messaggio originale.

Sin dalla antichità si è avvertita la necessità di proteggere delle informazioni che dovevano rimanere segrete; infatti il più antico esempio di crittografia è stato rinvenuto in alcuni geroglifici egiziani più di 4500 anni fa. Per questo si ritiene che la crittografia sia antica quanto la scrittura; anche nella Bibbia si possono ritrovare numerosi esempi di scritture segrete e codici cifranti, tra i quali il Co-

dice Atbash. Un rudimentale sistema crittografico venne usato anche nell'antica Grecia: si pensi alla "scitala spartana", in uso intorno al 400 a.C.; essa consisteva in un bastoncino su cui veniva arrotolata una strisciolina di cuoio su cui era scritto il messaggio, decifrabile solo se si era in possesso di una bacchetta identica a quella del mittente.

Anche i Romani utilizzarono la crittografia, basti pensare al Codice di Cesare, la prima forma di crittografia monoalfabetica o a sostituzione. Fu il più semplice codice simmetrico possibile che consisteva nel sostituire una lettera del "testo in chiaro" con una lettera successiva dell'alfabeto. Veniva utilizzato soprattutto per proteggere le comunicazioni militari e familiari e rimase in uso fino al Rinascimento.

Parallelamente alla crittografia, si sviluppò anche la crittoanalisi, la disciplina che, a partire da un testo cifrato, studia i metodi di decrittazione, cioè di ricostruzione del testo in chiaro, a partire dal testo cifrato di cui non si possiede la chiave; l'oggetto dell'analisi quindi è la chiave segreta di accesso.
Una delle più importanti scoperte della crittoanalisi la dobbiamo al filosofo arabo Al-Kindi che, intorno al IX secolo, scrisse l'"Epistola sulla decifrazione dei messaggi crittati"; egli inventò la tecnica dell'analisi delle frequenze che permise di violare molto più facilmente i codici a sostituzione monoalfabetici.

Solo nel '500 si ebbe un successivo sviluppo della crittografia, quando Leon Battista Alberti inventò il "disco cifrante" e la "chiave crittografica" che fino al XVI secolo restò l'unico metodo conosciuto per utilizzare un cifrario polialfabetico.

Alla fine del XVI secolo il francese Vigenère propose un nuovo metodo di

cifratura polialfabetica e a chiave simmetrica. Considerato per secoli inattaccabile, esso utilizzava 26 alfabeti per cifrare un solo messaggio. Da tale metodo deriva il Cifrario di Vernam, considerato teoricamente perfetto ma di difficile realizzazione.

Dalla seconda metà del XIX secolo, l'invenzione di nuovi mezzi di comunicazione come il telegrafo, il telefono e soprattutto la radio cambiò radicalmente il modo di comunicare: la trasmissione dei messaggi divenne sempre più veloce, anche da luoghi molto distanti, mentre le intercettazioni da parte dei nemici furono ancora più facilitate. Nacque quindi l'esigenza di poter usufruire di una crittografia più sicura, veloce e facilmente utilizzabile. È proprio in questo periodo che si svilupparono la prime macchine cifranti, che permisero di ridurre notevolmente i tempi di cifratura e decifratura, trasformando automaticamente le lettere del testo in chiaro in quelle del testo cifrato e viceversa. Queste macchine, che possono essere ritenute una versione meccanica del Cifrario di Vigenère, resero i sistemi crittografici sempre più rapidi e sicuri.

Fin dalla Prima Guerra Mondiale molti Stati cominciarono a dare sempre più importanza alla crittografia e ad organizzare appositi uffici: pensiamo ai crittografi britannici che si riunivano nella famosa "Stanza 40" in cui venivano decrittati moltissimi radiomessaggi tedeschi. Il più famoso di questi fu il "Telegramma Zimmermann", ritenuto uno dei fattori che spinsero gli Stati Uniti ad entrare in guerra nel 1917.

Poi nel 1918 venne brevettata una nuova macchina per cifrare i messaggi, destinata a diventare una delle più famose di tutti i tempi: la macchina cifrante Enigma. Furono i tedeschi a capirne l'importanza e, dopo il 1924, iniziarono ad utilizzarne una versione adattata alle esigenze militari; essi continuarono a

fare affidamento su questa macchina anche durante la Seconda Guerra Mondiale, credendo che fosse assolutamente sicura. Inizialmente il metodo crittografico tedesco apparve insormontabile, al punto da mettere in crisi l'intero apparato di controspionaggio inglese e francese.
Poi nel '39 i britannici costituirono una scuola dei codici e dei cifrari che riuniva i migliori crittoanalisti, matematici e scienziati; ciò consentì loro, in seguito, di forzare sistematicamente i messaggi cifrati con Enigma e successivamente dalla macchina Lorenz.
Il ruolo della crittografia diventerà quindi assolutamente fondamentale nella Seconda Guerra Mondiale: si pensi, ad esempio, allo sbarco in Normandia, reso possibile dal fatto che gli americani erano in grado di leggere tutti i messaggi degli alti comandi tedeschi.

Se in passato, fino alla Seconda Guerra Mondiale, la crittografia era una scienza applicata per attuare piani militari e nascondere messaggi di rilevanza strategica, oggi, con l'avvento dell'Intelligenza Artificiale e dei Big Data, sta vivendo una nuova fase con finalità totalmente differenti come la privacy e la protezione dei dati.

Oggi la crittografia è presente in molti aspetti della vita di tutti i giorni e viene usata costantemente, spesso in modo inconsapevole quando, ad esempio, si apre una pagina web, si invia o si riceve una mail o un messaggio su una delle tante applicazioni di messaggistica oppure quando vengono inseriti dati personali sul sito della banca per autorizzare un bonifico.

In tutti questi casi si è certi che quelle informazioni sono note solo a chi le riceve, oltre a chi esegue le operazioni, senza che siano diffuse verso altri soggetti. Risulta evidente, pertanto, l'importanza di sviluppare tecniche e metodi

di cifratura sempre più sicuri.

Capitolo 2

Introduzione alla crittografia moderna

Nonostante tracce di sistemi crittografici si ritrovino nell'antichità a partire dal 2000 a.C., la nascita della crittografia moderna si può collocare durante la Seconda Guerra Mondiale, quando gli sforzi dei crittoanalisti alleati ebbero la meglio sul sistema tedesco basato sulla macchina Enigma.

La crittografia moderna si differenzia notevolmente dalla crittografia di cui si è parlato finora. L'avvento dei calcolatori e dell'informatica infatti ha rivoluzionato profondamente sia i sistemi crittografici sia il modo di vedere e utilizzare la crittografia permettendo di sviluppare, a partire dai lavori del matematico Alan Turing, algoritmi basati su proprietà matematiche, in precedenza intrattabili.

Molti sistemi crittografici analizzati in precedenza e considerati ragionevolmente sicuri fino al XIX secolo, possono oggi essere forzati in tempi brevissimi grazie alla velocità di elaborazione del computer. Inoltre, possono essere ora utilizzati sistemi crittografici molto complessi e che, un tempo, avrebbero richiesto tempi di cifratura "a mano" troppo lunghi.

I principali obiettivi della crittografia moderna che devono essere perseguiti per garantire una comunicazione sicura sono:

- Confidenzialità: i messaggi che vengono scambiati non devono essere visibili ad altri. Solo il mittente e il destinatario previsto devono "capire" il contenuto del messaggio. Il mittente codifica il messaggio mentre il destinatario lo decodifica.

- Autenticazione: quando si parla con un interlocutore bisogna essere sicuri della sua identità. Il mittente e il destinatario devono assicurarsi dell'identità reciproca.

- Integrità del messaggio: quando un messaggio viene scambiato in rete, il destinatario deve vedere una copia identica del messaggio non alterata. Il mittente e il destinatario vogliono essere certi che il messaggio in transito non sia alterato (volontariamente o meno).

- Disponibilità sia dell'accesso che delle risorse: i servizi devono essere accessibili e disponibili per gli utenti.

Gli algoritmi crittografici possono essere divisi in due classi principali: gli algoritmi a chiave simmetrica e quelli a chiave pubblica (o asimmetrica). Nei capitoli successivi verranno presentate queste due famiglie di algoritmi.

Capitolo 3

Crittografia a chiave simmetrica

Gli algoritmi di crittografia a chiave simmetrica sono così denominati perché utilizzano la stessa chiave sia per la cifratura che per la decifratura. Questo tipo di algoritmi, storicamente nati per primi, fa uso di tecniche di trasposizione e di sostituzione. Una delle caratteristiche più significative dei sistemi a chiave simmetrica è la velocità dell'implementazione perché, dal punto di vista del costo di calcolo, sono i più leggeri.

Un aspetto negativo di questo tipo di algoritmi riguarda il cosiddetto "Problema della Distribuzione delle Chiavi". Se si hanno N entità che devono comunicare tra loro in modo sicuro attraverso un sistema crittografico a chiave simmetrica, si deve fare in modo che ogni entità possegga $N - 1$ chiavi differenti, una per ciascuna delle altre entità. Ciò significa che si deve essere in grado di generare, trasmettere e conservare $\frac{N(N-1)}{2}$ chiavi diverse. Naturalmente, per valori molto grandi di N, la gestione del sistema diventa troppo complessa.

La chiave di cifratura non deve essere scambiata in maniera ingenua, come ad esempio in internet, altrimenti la robustezza dell'algoritmo di cifratura crolla. Infatti tale chiave dovrà essere comunicata attraverso un canale sicuro che, nella

realtà dei fatti, è difficile da realizzare.

I cifrari simmetrici fanno uso, in modo più o meno evoluto, di tecniche di sostituzione e di trasposizione. Questi cifrari, che sono stati concepiti in tempi antichissimi, anche se non più impiegabili da soli poiché facilmente forzabili, costituiscono tuttavia il nucleo essenziale per costruire i moderni cifrari a chiave segreta del tipo a blocco, nei quali il flusso dei bit del messaggio viene suddiviso in blocchi di lunghezza costante, sui quali vengono eseguite delle operazioni di sostituzione e trasposizione.
Due esempi di cifrari classici sono quello a sostituzione (monoalfabetica) e quello a trasposizione.
Nel cifrario a sostituzione ogni lettera dell'alfabeto A che usiamo per la trasmissione del messaggio viene posta in corrispondenza con un'altra lettera dello stesso alfabeto, ottenuta a seguito di una permutazione di A. La chiave di cifratura in questo caso è l'alfabeto cifrato, ovvero con le lettere scambiate di posizione. Nel cifrario a trasposizione invece si suddivide il messaggio in blocchi di una certa lunghezza, permutando successivamente le lettere di ciascun blocco secondo uno schema predefinito.

Esempi di questi cifrari sono costituiti dal DES e dall'AES.

Il codice DES (Data Encryption Standard) è stato progettato dall'IBM nel 1975, per poi essere introdotto nel 1977 come sistema ufficiale di cifratura del Governo degli USA.
Il DES è un algoritmo a chiave simmetrica. Fa uso di chiavi di cifratura di 56 bit. La dimensione dei segmenti in cui viene frammentato il testo in chiaro è di 64 bit.
Il primo passo dell'algoritmo prevede una permutazione (sparpagliamento dei

bit) sempre in 64 bit. Viene poi considerato la parte di sinistra $L1$ di 32 bit e la parte di destra $R1$, sempre di 32 bit.
Il DES prevede 16 passaggi; per ognuno di essi il blocco di destra viene copiato nel blocco di sinistra del passaggio successivo ($L2 = R1$). Il blocco di destra del passaggio successivo viene generato utilizzando una funzione di cifratura che prende in ingresso i blocchi di sinistra e di destra del passo precedente, che vengono poi codificati con una chiave di cifratura di 48 bit, generata dalla chiave primaria.
La chiave primaria viene utilizzata con un algoritmo standard per generare altre 16 sottochiavi che sono utilizzate nei 16 stadi. Per ogni blocco la funzione è sempre la stessa. Infine c'è una permutazione finale che porta ai 64 bit cifrati.

Con il DES si hanno quindi un numero possibile di chiavi pari a 2^{56} che, fino agli anni '70, erano sufficienti per proteggere il sistema da un attacco di tipo "forza bruta", ma non più al giorno d'oggi, a causa dell'avvento dei calcolatori moderni. Per questo motivo il DES è stato aggiornato con il più robusto sistema crittografico AES, che costituisce oggi il modello crittografico a chiave simmetrica più diffuso.

L'AES infatti elabora dati di 128 bit con chiavi di cifratura di 128, 192 o 256 bit; per questo motivo esso è molto più difficile da decriptare rispetto al DES, ed è impensabile violarlo con un attacco "forza bruta". Nel 2001 è diventato uno standard del governo degli Stati Uniti.

Capitolo 4

Crittografia a chiave pubblica

Un problema di tutti i sistemi crittografici a chiave simmetrica, dai più rudimentali ai più sofisticati, è dato dalla necessità della distribuzione delle chiavi in modo sicuro tra mittenti e destinatari. Quando si utilizza questo particolare tipo di algoritmi infatti, la chiave di cifratura, coincidendo con quella di decifratura, deve essere protetta e al tempo stesso distribuita agli utenti legittimi del sistema.

Viste le difficoltà dovute alla distribuzione delle chiavi dei cifrari simmetrici, nel 1976 i ricercatori Diffie ed Hellman illustrarono il concetto di crittografia a chiave pubblica nel famoso articolo "New Directions in Cryptography" [2].

Con questa tecnica, ogni utente ha due chiavi distinte: una pubblica e una privata. Si tratta quindi di un sistema crittografico asimmetrico in cui la chiave pubblica serve per la cifratura del messaggio, mentre per la decifrazione il destinatario deve utilizzare la sua chiave privata, che deve restare totalmente segreta. La cifratura del messaggio dovrà essere alla portata di tutti con l'utilizzo della chiave pubblica; mentre la decifrazione sarà possibile solo al possessore della chiave privata corretta.

Un sistema a chiave pubblica prevede che la chiave di decifratura non sia facilmente derivabile da quella di cifratura. L'idea si basa quindi sul concetto di funzione unidirezionale: esistono funzioni che sono facili da calcolare in una direzione, ma diventano computazionalmente pesantissime nella direzione opposta (funzione inversa).

Nella teoria di Diffie-Hellman, l'algoritmo di cifratura $E(\cdot)$ e quello di decifratura $D(\cdot)$ devono soddisfare due condizioni:

- $D(E(M)) = M$;
- deve essere difficile dedurre $D(\cdot)$ da $E(\cdot)$.

Questo metodo funziona nel seguente modo: Alice, che vuole ricevere messaggi segreti da Bob, trova due funzioni E e D, che soddisfano le precedenti condizioni, parametrizzate dalla chiave per criptare e da quella per decriptare. La chiave di cifratura viene resa pubblica mentre quella di decifratura viene mantenuta segreta da Alice. Se Bob vuole spedire un messaggio M ad Alice, si procura la sua chiave pubblica, calcola $C = E(M)$, che è il messaggio cifrato, e glielo invia. A questo punto Alice, utilizzando la sua chiave privata, calcolerà $M = D(C)$.

La crittografia a chiave pubblica richiede quindi che l'utente possegga due chiavi: una pubblica usata per cifrare i messaggi da chiunque voglia comunicare con lui ed una privata per decifrare i messaggi ricevuti. Queste due chiavi devono essere tra loro correlate, ma deve essere difficile risalire alla chiave privata a partire da quella pubblica, sulla base della quasi impossibilità di risoluzione di alcuni problemi matematici.

I sistemi crittografici a chiave pubblica sono molto più lenti di quelli a chiave simmetrica ma, allo stesso tempo, risolvono il "Problema della Distribuzione delle Chiavi". Proprio per questo motivo, si preferisce l'utilizzo di un sistema che accomuni entrambi: gli schemi a chiave pubblica vengono utilizzati per lo scambio delle chiavi simmetriche (in genere molto più brevi del messaggio), mentre la crittografia simmetrica viene utilizzata per cifrare i messaggi.

Il sistema crittografico a chiave pubblica più conosciuto è l'algoritmo RSA, che fu proposto dai ricercatori Rivest, Shamir e Adleman nel 1978 [8]. Esso fa uso dell'aritmetica modulare: x mod n = resto della divisione (tra interi) tra x ed n.

Un qualunque messaggio da codificare è una stringa di bit. Una stringa di bit può essere rappresentata con un intero. Quindi codificare un messaggio equivale a codificare un numero intero. Qualunque sia l'origine di un messaggio, esso è sempre composto da bit che possono essere frazionati in blocchi di una certa lunghezza e associati ad un numero intero corrispondente.

L'algoritmo RSA fa uso dell'aritmetica modulare e si basa sull'uso di numeri primi. Affinché la tecnica sia robusta, questi numeri primi devono essere molto lunghi. La robustezza sta nel fatto che è computazionalmente difficile stabilire se una stringa binaria molto lunga è un numero primo. Quindi l'algoritmo RSA è sicuro perché fattorizzare grandi numeri è difficile.

La chiave pubblica e la chiave privata vengono calcolate attraverso i seguenti passi:

1. Si supponga di avere due numeri primi molto lunghi, p e q.

2. Questi numeri vengono moltiplicati tra loro ottenendo n, quindi $n = pq$.
   Si moltiplica $p - 1$ e $q - 1$ ottenendo z, quindi $z = (p - 1)(q - 1)$.

3. Si sceglie un numero e, con $e < n$, in modo che non abbia fattori in comune con z.
   I numeri e, z non devono essere per forza numeri primi, possono essere anche fattorizzabili, purché non abbiano fattori in comune, devono essere quindi primi relativi.
   Si sceglie poi un numero d tale che il prodotto ed–1 sia esattamente divisibile per z, in altri termini ed mod $z = 1$.

4. La coppia (n, e) è la chiave pubblica K_b^+, mentre la coppia (n, d) è la chiave privata K_b^-.

La cifratura e la decifratura vengono così eseguite:
Data la chiave pubblica (n, e), la chiave privata (n, d) e il messaggio m:

- per cifrare il messaggio m $(< n)$, si calcola $c = m^e$ mod n.
- per decifrare il messaggio, si calcola $m = c^d$ mod n.
  Infatti $m = (m^e \text{ mod } n)^d$ mod n, dove m^e mod $n = c$

Un esempio di utilizzo dell'algoritmo RSA è il seguente:
Bob sceglie $p = 5$ e $q = 7$, quindi $n = 35$ e $z = 24$.
Quindi $e = 5$ (e, z sono primi relativi), mentre $d = 29$ ($ed - 1$ è esattamente divisibile per z).
La chiave pubblica K_b^+ è $(n, e) = (35, 5)$, mentre la chiave privata K_b^- è $(n, d) = (35, 29)$. Il numero c^d è molto grande, nonostante sia stato ottenuto da numeri piccoli. Invece, usando numeri molto più grandi, si sarebbe ottenuto un numero enorme.

Un'importante proprietà dell'algoritmo RSA è la seguente:

$$K_b^-(K_b^+(m)) = m = K_b^+(K_b^-(m)).$$

Ovvero se si usa prima la chiave pubblica e poi quella privata, si ottiene lo stesso risultato di quando si usa prima la chiave privata e poi quella pubblica.

Non bisogna pensare che la crittografia a chiave simmetrica sia stata superata dagli algoritmi del sistema RSA, in quanto questi ultimi sono efficienti ma molto più lenti dei sistemi come il DES. Come detto anche in precedenza quindi, la moderna crittografia utilizza entrambi i due tipi di sistemi, sfruttando un algoritmo asimmetrico come l'RSA solamente per permettere lo scambio sicuro di una chiave simmetrica con cui vengono trattati tutti i messaggi successivi.

Si può quindi dedurre che le tecniche di codifica a chiave simmetrica sono pesanti dal punto di vista di calcolo. Se c'è possibilità di scegliere tra chiave simmetrica e chiave pubblica, è preferibile quella pubblica perché computazionalmente più leggera.

Gli algoritmi a chiave pubblica sono molto utili dal punto di vista della sicurezza.
Ad esempio se Bob cifra un messaggio con la propria chiave privata, chiunque al mondo può usare la chiave pubblica che Bob aveva distribuito per decifrare il messaggio.
La corretta decifrazione del file con la chiave pubblica di Bob implica che solo quest'ultimo può aver cifrato il file, e quindi si ha la certezza che il mittente sia Bob. In questo modo si fornisce il servizio di autenticazione del mittente.
Inoltre, se qualcuno vuole inviare un messaggio a Bob e vuole essere sicuro che solo quest'ultimo possa leggerlo, lo cifra con la chiave pubblica di Bob. In questo

modo si è sicuri che solo Bob potrà decifrarlo. Viene quindi implementata una certa segretezza. Se Bob riesce a decifrare il messaggio, ha la certezza che esso è integro, ovvero che non è stato alterato, perché altrimenti non sarebbe riuscito a decifrarlo.

4.1 Firma digitale

In tutti i sistemi utilizzati nelle applicazioni pratiche, gli utenti devono autenticarsi, ovvero devono garantire all'interlocutore la propria identità.

Il problema dell'autenticazione del mittente non si pone nel contesto della crittografia simmetrica. Infatti, l'acquisizione da parte di Bob di un messaggio inviato da Alice, decifrabile utilizzando una chiave simmetrica precedentemente condivisa, fornisce implicitamente una garanzia sull'autenticità del mittente.

Nel caso della crittografia a chiave pubblica invece le cose cambiano radicalmente. La condivisione di chiavi segrete infatti non è possibile e tutti gli utenti della rete sono uguali dal punto di vista delle credenziali pubbliche che sono in grado di fornire. L'unica informazione che può essere utilizzata per identificare con certezza un utente è la sua chiave privata, quindi è di fondamentale importanza utilizzarla in un qualche modo per poter autenticare i mittenti dei vari messaggi scambiati in rete.

Una delle applicazioni più importanti della crittografia a chiave pubblica è la cosiddetta firma digitale. Essa consiste in un procedimento matematico che permette di associare un documento elettronico al suo legittimo proprietario e che produce una determinata sequenza binaria, chiamata appunto firma. Per firmare un documento, il mittente lo cifra utilizzando la propria chiave privata. Quando il destinatario utilizza la chiave pubblica del mittente per decifrare il

messaggio, sa che solo il mittente può averlo firmato ed è sicuro della sua integrità, altrimenti non sarebbe stato in grado di decifrarlo.

Nella pratica la firma digitale non viene applicata all'intero documento ma ad una sua versione compressa, chiamata "message digest", ottenuta con l'impiego di funzioni hash.

Definizione 1: Una funzione hash è una funzione $H(\cdot)$ con le seguenti proprietà:

1. H mappa un input x di lunghezza arbitraria in un valore $H(x)$ di lunghezza fissa n.

2. dato x e $H(\cdot)$, è facile calcolare $H(x)$.

3. per un qualunque valore hash z, è computazionalmente infattibile trovare un input x tale che $z = H(x)$.

4. dato x è computazionalmente infattibile trovare un $x' \neq x$ tale che $H(x) = H(x')$.

5. è computazionalmente infattibile trovare due input distinti $x' \neq x$ tali che $H(x) = H(x')$.

Ad un messaggio in chiaro m di lunghezza qualsiasi viene applicata una funzione di hash, generando così il digest $H(m)$, a cui viene applicato un algoritmo di cifratura a chiave pubblica utilizzando la chiave privata.

Il digest cifrato dalla chiave privata rappresenta la firma digitale, che è una stringa binaria di pochi bit a prescindere dalla dimensione del file. Questa firma è sicura perché la si può decifrare solamente usando la chiave pubblica del mittente, che viene quindi autenticato.

Al destinatario vengono inviati il messaggio e la firma digitale. Esso applica al messaggio la funzione di hash usata per cifrarlo, ottenendo così il digest, poi applica alla firma digitale la chiave pubblica del mittente trovando un digest. Se questo digest coincide con quello calcolato dal messaggio, il destinatario è sicuro dell'identità del mittente e dell'integrità del file.

Tutto ciò vale solamente se si è sicuri dell'identità del possessore della chiave pubblica. Proprio per questo motivo, ci sono delle organizzazioni fidate, chiamate Autorità di Certificazione (CA), che certificano il possesso della chiave pubblica di un determinato utente firmandola digitalmente, ovvero applicando la propria chiave privata alla chiave pubblica da certificare, generando così il certificato dell'utente.
Chiunque nel mondo può prendere il certificato di Bob e applicargli la chiave pubblica dell'Autorità di Certificazione, recuperando così la chiave pubblica di Bob. In questo modo si è sicuri che quella chiave pubblica appartiene sicuramente a Bob.

Capitolo 5

Curve Ellittiche

5.1 Concetti di base

Tutti i moderni algoritmi crittografici basati sulle curve ellittiche fanno uso sulla teoria dei gruppi per garantire la sicurezza dei sistemi. Di seguito vengono fornite alcune definizioni per inquadrare al meglio i concetti relativi all'ECC.

Definizione 2: Un gruppo è un insieme di elementi G dotati di un'operazione binaria $f : G \times G \to G$, tale che f è associativa con un elemento identità e ed ogni elemento in G ha un inverso. G si dice abeliano se e solo se f è commutativa.

Sia "f" l'operazione di gruppo. Nelle realizzazioni pratiche, i gruppi possono essere additivi (se f rappresenta un'addizione di elementi) o moltiplicativi (se f rappresenta una moltiplicazione). Indipendentemente dalla realizzazione del gruppo, la notazione è spesso moltiplicativa.
L'operazione di gruppo è denotata da "$*$", l'elemento identità in G è "1" mentre l'inverso per ogni a in G è a^{-1}. L'applicazione consecutiva (n volte) dell'operazione di gruppo su un elemento del gruppo p è solitamente rappresentata come p^n.

Poiché la difficoltà di qualsiasi problema matematico definito su un qualsiasi gruppo utilizzato in crittografia è correlata al numero di elementi nel gruppo, è fondamentale determinare la cardinalità di qualsiasi gruppo utilizzato.

Definizione 3: Un gruppo è finito se e solo se G è un insieme finito, in tal caso il numero di elementi in G, ovvero la sua cardinalità, è chiamato ordine di G.

Un sottogruppo H di G è un sottoinsieme di G contenente e se e solo se $f : H \times H \to H$ vale per ogni elemento in H e anche l'inverso di tali elementi è in H.
Per ogni $p \in G$, $q = p^n \ \forall n \in \mathbb{Z}$ è un sottogruppo di G generato da p, indicato con $\langle p \rangle$.

Invece di elencare ogni elemento dell'insieme, è possibile specificare un ampio insieme di elementi con un singolo elemento radice, ovvero il generatore di gruppo.
Definizione 4: Il generatore di gruppo, denominato anche come radice o elemento primitivo di G, è un qualsiasi $r \in G$ tale che $\langle r \rangle = G$

I gruppi ciclici sono uno specifico tipo di gruppo utile per le applicazioni crittografiche poiché i risultati di qualsiasi operazione di gruppo sono inclusi nel gruppo; di conseguenza, i calcoli non devono essere ripetuti e i risultati non devono essere verificati.
Definizione 5: Se esiste un $r \in G$ tale che $\langle r \rangle = G$, allora G si dice ciclico. Anche i sottogruppi di un gruppo ciclico sono ciclici.

La cardinalità di un sottogruppo di G rappresentato da un generatore è un'altra proprietà di notevole interesse. L'ordine del generatore è rappresentato dal

numero di elementi in un sottogruppo prodotto da esso.

Definizione 6: Un elemento $p \in G$ ha ordine finito se e solo se $\langle p \rangle$ è finito. L'ordine di p è rappresentato dalla cardinalità di $\langle p \rangle$ ed è dato dal più piccolo $t \in \mathbb{Z}$ tale che $p^t = e$. Questo è anche chiamato ordine del generatore per $\langle p \rangle$.

I gruppi sono definiti per un'unica operazione di gruppo. Un anello invece, è una struttura algebrica che utilizza sia una legge di composizione additiva che moltiplicativa.

Definizione 7: Un insieme di elementi R con due operazioni binarie $\{f, g\}$ è un anello se e solo se: R è un gruppo commutativo con f, e g è associativo e distributivo su f. In questo caso f e g rappresentano rispettivamente operazioni di gruppo additive e moltiplicative con 0 e 1 come elemento di identità rispettivamente.

Definizione 8: Un anello R è un campo se è commutativo e tutti i suoi elementi diversi da zero sono invertibili.

Un campo deve essere definito da 0 o da un numero primo affinché ogni elemento in esso contenuto abbia un inverso.

Definizione 9: Se l'ordine di un campo K è finito, allora si dice che è un campo finito.

Le curve ellittiche sono sempre definite su campi finiti nell'ECC. L'ordine del campo finito K è dato da p^m, dove p è un numero primo ed m è la dimensione finita dello spazio vettoriale in K. I campi finiti sono anche noti come campi di Galois, indicati con $GF(p^m)$.

Definizione 10: Per ogni numero primo p e per ogni intero positivo m esiste un campo finito con $q = p^m$ elementi denotati con $\mathbb{F}_q$.

Un campo finito di ordine q ($\mathbb{F}_q$) esiste se e solo se il suo ordine è una potenza prima $q = p^m$. Le costruzioni più comuni includono i casi in cui $q = p$ (chiamato campo primo $\mathbb{F}_p$) e dove $q = 2^m$ (chiamato campo binario $\mathbb{F}_{2^m}$). Queste sono le basi per definire i più diffusi sistemi di curve ellittiche.

5.2 Curve Ellittiche

5.2.1 Proprietà

L'ordine di un gruppo di curve ellittiche $\{E(\mathbb{F}_q) \cup \theta\}$, dove θ è il punto all'infinito, viene indicato con o, e rappresenta il numero di punti in E. I valori di o e q sono correlati dalla traccia di Frobenius $t = q + 1 - o$. Il teorema di Hasse implica che $|t| < 2\sqrt{q}$.

Dato un punto $P \in E(\mathbb{F}_q)$, il suo ordine è il più piccolo intero positivo n tale che $nP = \theta$. Per il teorema di Lagrange, l'ordine di un punto $P \in E(\mathbb{F}_q)$ divide l'ordine o del gruppo $E(\mathbb{F}_q)$. Quindi $oP = \theta$ per ogni $P \in E(\mathbb{F}_q)$ e, di conseguenza, l'ordine di un punto è sempre minore o uguale all'ordine della curva ellittica.

5.2.2 Aritmetica

Nella crittografia basata sulle curve ellittiche (ECC) sono coinvolte diversi tipi di operazioni. Queste possono essere di diversa natura, a seconda che siano definite per la curva ellittica, per il gruppo di curve ellittiche, o per il campo finito.

Aritmetica della curva

Gli input per le operazioni sulla curva sono i punti della curva ellittica, che vengono poi utilizzati per trovare altri punti della curva. Questo gruppo di operazioni

include solamente la moltiplicazione scalare.
Tutto ciò rappresenta la legge di gruppo: l'applicazione di successive operazioni di gruppo (addizione) ad un punto $P \in E(\mathbb{F}_q)$ genererà come risultato altri punti, sempre nella curva. Se il numero di addizioni applicate al punto è uguale all'ordine del gruppo di curve ellittiche, il risultato è il punto originario.

Fare una moltiplicazione scalare sulla curva $E(\mathbb{F}_q)$ significa calcolare k addizioni di un punto P, rappresentate da kP. In questo processo, vengono utilizzati uno scalare $k \in \mathbb{N}$ e un punto della curva $P \in E(\mathbb{F}_q)$ per trovare un altro punto $Q \in E(\mathbb{F}_q)$ tale che $Q = kP$, attraverso un insieme definito di regole.

Sono stati proposti diversi metodi per eseguire la moltiplicazione scalare, tutti costruiti su operazioni di gruppo definite per una specifica curva ellittica.

Aritmetica del gruppo

L'addizione dei punti della curva ellittica viene realizzata utilizzando questo tipo di aritmetica. Varia a seconda del tipo di curva, del campo finito e del tipo di coordinate utilizzato ed è indipendente dagli algoritmi kP.

L'addizione di due punti nella curva ellittica

$$P + Q \qquad \forall P, Q \in E(\mathbb{F}_q)$$

e il raddoppio dei punti

$$P + P \qquad \forall P \in E(\mathbb{F}_q)$$

sono i punti fermi delle operazioni di gruppo.

Trovare formule efficaci per le operazioni di gruppo è fondamentale poiché una moltiplicazione scalare richiede in genere entrambi i calcoli appena descritti.

Aritmetica del campo

Le operazioni del campo sono quelle definite per $\mathbb{F}_q$.

L'addizione e il raddoppio dei punti vengono eseguiti tramite una serie di operazioni su diversi elementi del campo che differiscono dalle coordinate dei punti di input. L'aritmetica dei campi è collegata ma non è dipendente dall'aritmetica delle curve o dalle operazioni di gruppo.

Le operazioni del gruppo vengono eseguite utilizzando varie configurazioni delle operazioni sul campo. Tra queste, la moltiplicazione del campo, la riduzione polinomiale, l'addizione e la sottrazione del campo, la quadratura del campo e l'inversione del campo sono le più comuni.

5.2.3 Rappresentazione dei punti

Un punto $P \in E(\mathbb{F}_q)$ può avere diverse rappresentazioni che soddisfano modelli equivalenti dell'equazione di Weierstrass. Ogni punto è soggetto a trasformazioni matematiche per generare una proiezione della curva. Queste funzioni di trasformazione devono essere biiettive.
Il motivo principale per eseguire una trasformazione di coordinate su un punto è ottenere delle semplificazioni per l'esecuzione di operazioni sulle curve.

Il sistema di base della rappresentazione dei punti è quello affine. In questo sistema ogni punto $P \in E(\mathbb{F}_q)$ è rappresentato da una coppia di coordinate, generalmente (x, y).

Sono necessari solo due valori per rappresentare un punto e, in alcuni casi, è sufficiente un'unica coordinata. Lo svantaggio principale è che devono essere eseguite diverse inversioni di campo per recuperare un risultato in coordinate affini durante il calcolo dell'operazione di gruppo.
Poiché le inversioni in $\mathbb{F}_q$ sono processi ad alto utilizzo di risorse, esse dovrebbero essere evitate in tutte quelle situazioni in cui si hanno risorse limitate.

Per risolvere questo problema vengono utilizzate le coordinate proiettive. Un punto proiettivo $P \in E(\mathbb{F}_q)$ è denotato da una tupla di coordinate $(X : Y : Z)$. La trasformazione da coordinate affini a coordinate proiettive generalmente segue la legge $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$. In questo caso il risultato può essere ottenuto senza alcuna operazione di inversione, ma la rappresentazione di un punto della curva richiede un valore aggiuntivo (per la coordinata Z).

Per i sistemi che eseguono operazioni di gruppo con rappresentazioni miste di punti si dice che utilizzano coordinate miste. Per evitare l'impiego di inversioni di campo, l'addizione di punti accetta tipicamente un input in coordinate affini e produce un output in coordinate proiettive.
D'altra parte, il raddoppio dei punti può sfruttare input proiettivi per generare output proiettivi ad un basso costo. Questi sistemi aumentano l'efficienza di calcolo richiedendo solo una trasformazione di coordinate alla fine di ogni moltiplicazione scalare.

5.2.4 Famiglie di curve ellittiche

È possibile identificare specifiche famiglie di curve riducendo o semplificando la forma generalizzata di una curva ellittica. Di seguito sono descritte quelle più rilevanti.

Definizione 11: Per le curve ellittiche definite su un campo $\mathbb{F}_q$ con $q = p^m$ e $m = 1$, l'equazione di Weierstrass può essere semplificata come

$$E_p : y^2 = x^3 + ax + b$$

con $a, b \in Fp$ e $4a^3 + 27b^2 \neq 0$.
Queste curve sono generalmente denominate curve prime e il modello che le definisce è indicato come equazione di Weierstrass ridotta.

Definizione 12: Curve ellittiche non supersingolari su un campo finito $\mathbb{F}_q$ con $q = p^m$ e $p = 2$ sono definite da

$$E_b : y^2 + xy = x^3 + ax^2 + b$$

con $a, b \in \mathbb{F}_{2^m}$.
Questa equazione rappresenta il cosiddetto insieme di curve ellittiche binarie.

Altre importanti famiglie di curve includono le curve di Montgomery, le curve di Koblitz, le curve di Edwards e le nuove curve MoTE.

Definizione 13: Una curva di Montgomery è una forma di curva ellittica su $\mathbb{F}_q$, con caratteristica diversa da 2, definita da

$$E_M : By^2 = x^3 + Ax^2 + x$$

con $A \in \mathbb{F}_q \setminus \{-2, 2\}$, $B \in \mathbb{F}_q \setminus \{0\}$ e $B(A^2 - 4) \neq 0$.
Introdotte da Peter L. Montgomery nel 1987, queste curve sono utilizzate in varie applicazioni crittografiche. La capacità di eseguire l'aritmetica dei punti utilizzando solo la coordinata x rappresenza la principale ragione per utilizzare

queste curve.

Le curve di Koblitz, note anche come curve binarie anomale, sono state proposte da Neal Koblitz per uso crittografico nel 1992. Con questo particolare tipo di curve è possibile utilizzare tecniche di moltiplicazione dei punti molto più veloci rispetto a quelle impiegate con le curve binarie casuali.
Definizione 14: Le curve di Koblitz soddisfano un'equazione della forma

$$E_K : y^2 + xy = x^3 + ax^2 + 1$$

con $a \in \mathbb{F}_2$.

La famiglia delle curve ellittiche di Edwards è definita come segue.
Definizione 15: Sia $\mathbb{F}_q$ un campo in cui $2 \neq 0$ e sia $d \in \mathbb{F}_q \setminus \{0, 1\}$; allora

$$E_E : x^2 + y^2 = 1 + dx^2y^2$$

definisce una curva di Edwards.
Il calcolo dei multipli scalari in queste curve richiede meno operazioni sul campo rispetto ad altre rappresentazioni.

Definizione 16: Una variazione di queste curve chiamata curve Twisted Edwards soddisfa l'equazione

$$E_T : a^2 + y^2 = 1 + dx^2y^2$$

con $a, d \in \mathbb{F}_q \setminus \{0\}$ e $a \neq d$.

Una curva MoTE può essere descritta come una curva ellittica che presenta

sia il modello Montgomery che il modello Twisted Edwards.

Definizione 17: Il modello Montgomery di una curva MoTE è dato da un'equazione del tipo

$$E_M : -(A+2)y^2 = x^3 + Ax^2 + x$$

dove è possibile utilizzare il parametro $B = -(A+2)$.

5.3 Il problema del logaritmo discreto

Un logaritmo discreto è un numero intero k che risolve $b^k = g$, dove b e g sono elementi di un gruppo finito. Questa costruzione è stata utilizzata per proporre funzioni unidirezionali utilizzate come base per la crittografia asimmetrica.

Affinché un sistema basato su logaritmi discreti sia efficiente, devono essere disponibili algoritmi veloci per il calcolo dell'operazione di gruppo. Per motivi di sicurezza, il problema del logaritmo discreto dovrebbe essere computazionalmente irrisolvibile.

I gruppi più utilizzati per l'implementazione di sistemi basati sul logaritmo discreto sono i sottogruppi ciclici del gruppo moltiplicativo di un campo finito e i sottogruppi ciclici di gruppi di curve ellittiche.

Definizione 18: Problema del logaritmo discreto su curve ellittiche.
Sia E una curva ellittica definita su un campo finito $\mathbb{F}_q$. Sia P un punto in $E(\mathbb{F}_q)$, e supponiamo che P abbia un ordine primo n. Allora, il sottogruppo ciclico di $E(\mathbb{F}_q)$ generato da P è

$$\langle P \rangle = \{\theta, P, 2 \cdot P, 3 \cdot P, ..., (n-1) \cdot P\}.$$

Per questi sistemi l'operazione di gruppo "$\cdot$" è l'addizione consecutiva di punti della curva ellittica o la moltiplicazione scalare.
Dato un punto

$$Q = k \cdot P \in \langle P \rangle$$

e l'elemento radice o generatore P, il problema di determinare k è chiamato problema del logaritmo discreto sulle curve ellittiche (ECDLP), ed è computazionalmente intrattabile.

Il problema del logaritmo discreto (DLP) è di uso pratico nella crittografia asimmetrica poiché è la base per il sistema di coppie di chiavi.

Nel caso della crittografia basata sulle curve ellittiche, il numero primo q, l'equazione della curva ellittica E, il punto P e il suo ordine n sono parametri di dominio pubblico. Una chiave privata è un numero intero k selezionato casualmente in modo uniforme dall'intervallo $[1, n-1]$ e la corrispondente chiave pubblica è rappresentata da

$$Q = k \cdot P.$$

Capitolo 6

Crittografia basata sulle curve ellittiche

6.1 Introduzione

La sicurezza della crittografia a chiave pubblica si basa sulla risoluzione di un problema matematico molto difficile da risolvere senza informazioni preliminari, ma di semplice e rapida risoluzione se si è in possesso di determinate informazioni, ovvero la chiave privata o pubblica, a seconda dei casi.

Quando si utilizza l'algoritmo RSA, ad esempio, è necessario risalire ai due numeri o fattori primi che compongono la chiave per decifrare i messaggi. Questo è un processo molto semplice se uno dei due numeri primi è noto, ma è molto oneroso dal punto di vista computazionale se non si hanno informazioni preliminari.

Nonostante ciò, con l'evoluzione della potenza di calcolo dei computer e delle tecniche di fattorizzazione, per ottenere una sicurezza adeguata con tale algoritmo è ora necessario utilizzare numeri primi di migliaia di cifre, con conseguenti

chiavi molto lunghe e difficili da usare sia dal punto di vista pratico che dal punto di vista dell'occupazione di memoria.

Gli algoritmi a chiave pubblica utilizzano anche un'altra tipologia di problemi matematici per cifrare messaggi, rappresentata dall'equazione $a^x = b$ con x ignoto e a e b noti. Per decifrare il messaggio bisogna risolvere l'operazione inversa, ovvero $x = \log_a b$. Usando i logaritmi, questa classe di equazioni è semplice da risolvere sia nel campo dei numeri reali che dei complessi. Tuttavia, se portate in un campo finito, queste equazioni possono diventare piuttosto difficili da risolvere poiché coinvolgono il noto problema del logaritmo discreto.

La teoria delle curve ellittiche non è giovane, ma risale addirittura al Seicento; tuttavia, solo nell'ultimo mezzo secolo si è intuita una sua potenziale applicazione in ambito crittografico. Furono i matematici Koblitz e Miller nel 1985 a capirne l'importanza nel campo della sicurezza digitale. Da quel momento, lo studio delle curve ellittiche ha conosciuto un incremento importante, tanto è vero che, ad oggi, sono ampiamente diffuse.
In particolare, una curva ellittica è una curva piana definita da un'equazione del tipo:

$$y^2 = x^3 + ax + b.$$

A parità di dimensione del campo, il problema del logaritmo discreto utilizzato nella crittografia a curva ellittica è molto più difficile del problema della fattorizzazione di numeri primi impiegato nell'algoritmo RSA. Di conseguenza, per raggiungere lo stesso livello di sicurezza, questo tipo di crittografia necessita di chiavi pubbliche di dimensione inferiore, più facilmente utilizzabili rispetto a quelle utilizzate dall'algoritmo RSA.

Per questo motivo la crittografia ellittica costituisce attualmente il più valido sistema di crittografia a chiave pubblica alternativo all'algoritmo RSA, il quale un giorno potrebbe diventare non sicuro.
Nonostante ciò, il protocollo RSA viene ancora utilizzato, per esempio, per cifrare e decifrare i messaggi. Il motivo è che esso è più rapido nello scambio di informazioni, fornendo comunque una adeguata sicurezza.

Nei paragrafi successivi verrà trattata approfonditamente la crittografia basata sulle curve ellittiche (ECC).

6.2 Premessa

L'utilizzo delle curve ellittiche nel campo della Crittografia venne proposto dai matematici Victor Miller (IBM Watson Research Lab) e Neal Koblitz (University of Washington) rispettivamente nel 1985 e 1986. Furono i primi ad utilizzare le curve ellittiche nei già esistenti algoritmi crittografici a chiave pubblica.

Entrambi hanno implementato crittosistemi basati sul logaritmo discreto utilizzando un gruppo di punti di una curva ellittica definita su un campo finito. Il vantaggio principale di questo approccio risiede nella mancanza di algoritmi di complessità sub-esponenziale che possano calcolare logaritmi discreti in questi gruppi.

Infatti, contrariamente agli algoritmi a tempo sub-esponenziale, noti per il problema della fattorizzazione di interi utilizzati dai tradizionali algoritmi a chiave pubblica, i migliori algoritmi utilizzati per affrontare questo problema hanno un tempo di esecuzione completamente esponenziale. Di conseguenza, può essere mantenuto lo stesso livello di sicurezza utilizzando un gruppo basato sui punti di una curva ellittica con dimensioni inferiori. Questo si traduce in chiavi critto-

grafiche più piccole, risparmio di banda e implementazioni più veloci.

Nel 1991, i matematici Okamoto e Vanstone hanno introdotto la prima versione analoga dell'RSA basata sulle curve ellittiche. Questo sistema si basa su un insieme di punti di una curva ellittica definita sull'anello $\mathbb{Z}_n$ (con n intero non primo). Tuttavia, ricerche successive hanno rivelato che il nuovo sistema non apportava significativi miglioramenti rispetto al sistema originale.

Nel seguito di questo lavoro quindi, la Crittografia basata su Curve Ellittiche (ECC) verrà considerata come sola applicazione del Logaritmo Discreto sull'insieme dei punti di una curva ellittica (ECDLP).

I tre paragrafi successivi di questo capitolo introducono dei concetti fondamentali dell'ECC: i parametri di dominio, la generazione della coppia di chiavi e la firma digitale.

6.3 Parametri di dominio

Un crittosistema basato su curve ellittiche viene definito da un insieme di parametri che descrivono la curva ellittica $E(\mathbb{F}_q)$, il campo finito $\mathbb{F}_q$, un punto $P \in \mathbb{F}_q$ e l'ordine n di P. Questi parametri devono essere opportunamente selezionati in base alle scelte di implementazione e per garantire che l'ECDLP su $E(\mathbb{F}_q)$ possa resistere al maggior numero di attacchi. Gli elementi di tale insieme sono indicati come parametri di dominio.

Definizione 18: Un crittosistema basato su curve ellittiche ha come parametri di dominio l'insieme $D = (q, FR, S, a, b, P, n, h)$, dove:

- q è l'ordine del campo finito $\mathbb{F}_q$;

- FR (field representation) indica la rappresentazione usata per gli elementi di Fq;
- S è il random seed (dall'inglese, seme casuale) che viene utilizzato nel caso la curva ellittica venga generata in modo casuale;
- $a, b \in \mathbb{F}_q$ sono i coefficienti dell'equazione di Weiestrass che descrive la curva E ($y^2 = x^3 + ax + b$ nel caso di un campo primo, $y^2 + xy = x^3 + ax^2 + b$ nel caso di campo binario);
- $P = (x_p, y_p)$ è un punto di $E(\mathbb{F}_q)$ con ordine primo, detto punto base;
- n è l'ordine di P;
- $h = \frac{\#E(\mathbb{F}_q)}{n}$ è il cofattore, dove $\#E(\mathbb{F}_q)$ è la cardinalità del gruppo dei punti della curva ellittica.

6.4 Generazione delle chiavi

Un crittosistema basato su Curve Ellittiche utilizza una coppia di chiavi, perché è un sistema a chiave pubblica. Tale coppia sarà associata ad un particolare insieme di parametri di dominio $D = (q, FR, S, a, b, P, n, h)$.

La chiave pubblica non è altro che un punto Q scelto a caso nel gruppo $\langle P \rangle$ generato dal punto P. D'altra parte, la corrispondente chiave privata è uguale a $d = \log_P Q$. Appare evidente che il calcolo della chiave privata d, a partire dalla chiave pubblica Q, coincide con l'ECDLP. Quindi è fondamentale che i parametri di dominio siano stati selezionati in modo da rendere l'ECDLP intrattabile.

Algoritmo 1: Generazione delle chiavi
Inuput: parametri di dominio $D = (q, FR, S, a, b, P, n, h)$.
Output: chiave pubblica Q e chiave privata d.

1. Selezionare a caso $d \in [1, n-1]$,
2. Calcolare $Q = dP$.
3. Restituire (Q, d).

6.4.1 Validazione delle chiavi

L'obiettivo della validazione delle chiavi è di verificare che una chiave pubblica possieda qualità specifiche. Una validazione con esito positivo implica che una chiave privata associata è logicamente esistente, ma non garantisce che essa sia stata effettivamente calcolata o che il proprietario ne sia in possesso.

Algoritmo 2: Validazione della chiave pubblica
Inuput: parametri di dominio $D = (q, FR, S, a, b, P, n, h)$, chiave pubblica $Q = (x_Q, y_Q)$.
Output: validazione o rifiuto della chiave pubblica Q.

1. Verificare che $Q \neq \theta$, dove θ è il punto all'infinito,
2. Verificare che x_Q e y_Q siano elementi di $\mathbb{F}_q$,
3. Verificare che Q soddisfi l'equazione della curva E, definita da a e b,
4. Verificare che $nQ = \theta$,
5. Se almeno un controllo è fallito restituire "rifiutata", altrimenti restituire "accettata".

Esistono vari metodi per verificare che $nQ = \theta$. Ad esempio, se $h = 1$, ovvero il caso di curve ellittiche su campi primi che sono maggiormente utilizzati in pratica, i punti 1, 2 e 3 dell'algoritmo precedente implicano che $nQ = \theta$.

6.5 Firma digitale (ECDSA)

Una versione più recente della firma digitale utilizza le curve ellittiche: tale metodo viene chiamato Elliptic Curve Digital Signature Algorithm (ECDSA).

Alice vuole firmare e inviare a Bob un documento m, che è rappresentato da un numero intero. In realtà, firma il digest del documento, come descritto nella Sezione 4.1

Alice sceglie una curva ellittica definita su un campo finito $\mathbb{F}_q$ tale che la cardinalità del gruppo dei punti della curva $\#E(\mathbb{F}_q)$ sia uguale a fr, dove r è un numero primo di grande dimensione, mentre f è un numero intero piccolo, solitamente 1, 2 o 4 (f dovrebbe essere piccolo per mantenere l'algoritmo efficiente). Successivamente sceglie un punto base G in $E(\mathbb{F}_q)$ di ordine r, e infine sceglie un intero segreto a e calcola $Q = aG$.

Alice può rendere pubbliche le seguenti informazioni:

$$\mathbb{F}_q, \qquad E, \qquad r, \qquad G \qquad Q.$$

Per firmare il messaggio m, Alice svolge il seguente procedimento:

1. sceglie un numero intero casuale k con $1 \leq k < r$ e calcola $R = kG = (x, y)$,
2. calcola $s = k^{-1}(m + ax) \pmod{r}$.

Il documento firmato è rappresentato da

$$(m, R, s).$$

Per verificare la firma, Bob esegue le seguenti operazioni:

1. calcola $u_1 = s^{-1}m \pmod{r}$ e $u_2 = s^{-1}x \pmod{r}$,

2. calcola $V = u_1G + u_2Q$,

3. dichiara la firma valida se $V = R$.

Se il messaggio è firmato correttamente, l'equazione di verifica vale:

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R.$$

Capitolo 7

Conclusioni

La crittografia basata sulle curve ellittiche è stata introdotta negli ultimi decenni. La sua ricerca era inizialmente limitata agli ambienti accademici, ma in breve tempo ha attirato l'attenzione di varie società che lavorano nei settori delle telecomunicazioni e della sicurezza informatica, nonché di organizzazioni internazionali come ANSI e ISO.

Ormai dovrebbe essere chiaro perché ha suscitato tanto interesse: l'ECC si basa su un problema matematico estremamente difficile da risolvere (ECDLP), molto più impegnativo di quelli relativi agli algoritmi RSA e DSA, già ampiamente utilizzati. Pertanto, utilizzando chiavi notevolmente più piccole, la crittografia basata sulle curve ellittiche garantisce comunque lo stesso livello di sicurezza.

Inoltre, negli ultimi anni sono stati condotti vari studi su potenziali attacchi all'ECDLP, senza contare le innumerevoli ricerche fatte sull'ECC. Grazie a tutto ciò, la credibilità della crittografia basata sulle curve ellittiche è notevolmente aumentata.

Sebbene l'utilizzo dell'ECC sia ancora sporadico e i classici sistemi a chiave

pubblica (RSA e DSA) siano di gran lunga i più popolari al momento, tre semplici fattori indicano una tendenza ad una sempre maggiore adozione di questo approccio:

- la diffusione di dispositivi wireless è in costante aumento,
- gli standard di sicurezza stanno diventando sempre più esigenti,
- i sistemi ECC funzionano molto meglio dei sistemi RSA/DSA quando il livello di sicurezza necessario aumenta.

Quindi, in attesa di ulteriori nuovi metodi crittografici, il futuro dell'ECC è brillante e promettente.

Bibliografia

[1] Omar G Abood e Shawkat K Guirguis. «A survey on cryptography algorithms». In: *International Journal of Scientific and Research Publications* 8.7 (2018), pp. 495–516.

[2] Whitfield Diffie e Martin E Hellman. «New directions in cryptography». In: *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*. 2022, pp. 365–390.

[3] Samta Gajbhiye, Monisha Sharma e Samir Dashputre. «A survey report on elliptic curve cryptography». In: *International Journal of Electrical and Computer Engineering* 1.2 (2011), p. 195.

[4] Vivek Kapoor, Vivek Sonny Abraham e Ramesh Singh. «Elliptic curve cryptography». In: *Ubiquity* 2008.May (2008), pp. 1–8.

[5] Neal Koblitz. *A course in number theory and cryptography*. Vol. 114. Springer Science & Business Media, 1994.

[6] William August Kotas. «A brief history of cryptography». In: (2000).

[7] Alfred Menezes et al. «Evaluation of Security Level of Cryptography: ECDSA Signature Scheme». In: *Certicom Research. January* 15 (2001).

[8] Ronald L Rivest, Adi Shamir e Leonard Adleman. «A method for obtaining digital signatures and public-key cryptosystems». In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[9] Asep Saepulrohman e Agus Ismangil. «Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA)». In: *Int. J. Electron. Commun. Syst* 1.1 (2021), pp. 11–15.

[10] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[11] E Surya e C Diviya. «A Survey on Symmetric Key Encryption Algorithms». In: *International Journal of Computer Science & Communication Networks* 2.4 (2012), pp. 475–477.

[12] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman e Hall/CRC, 2008.