OliCyber.IT 2023 - Approfondimenti
Diffie-Hellman basics

Contenuti

1 Scambio di chiavi Diffie-Hellman

Il protocollo di Diffie-Hellman è uno degli elementi fondatori della crittografia moderna.
Esso dà una prima risposta al problema dello scambio di chiavi: come hai visto a lezione, spesso in crittografia è necessario che i due interlocutori siano in possesso di una *chiave (segreto) condivisa*.
Per mantenere un tono informale, supponi di volerti accordare con la tua amica Alice su una chiave condivisa da usare nella cifratura delle vostre conversazioni attraverso un qualche schema simmetrico, quando non avete la possibilità di chiacchierare faccia a faccia in un luogo lontano da occhi (e orecchie) indiscreti/e.
La soluzione più immediata sarebbe quella di incontrarvi in suddetto luogo (l'equivalente di un *canale sicuro*) e concordare sul vostro segreto condiviso, per poi proteggerlo e utilizzarlo quando siete distanti (*canale non sicuro*).
Qui possono sorgere molti interrogativi, ma il principale rimane il seguente: che succede se non hai la possibilità di incontrarti con Alice?
Si fa dunque avanti la necessità di trovare un modo per effettuare questo *scambio di chiavi* utilizzando un canale non sicuro. Fortunatamente abbiamo uno strumento estremamente abile nel complicare la vita di un intruso: la matematica!

1.1 Il problema del logaritmo discreto

Da qui in avanti lavoriamo in aritmetica modulare. In particolare p indica un *numero primo*.
Il problema del logaritmo discreto (Discrete Logarithm Problem, DLP) è il seguente:

Dati $a,\ c,\ p,$ trovare l'esponente e tale per cui

$$a^e \equiv c \pmod{p}$$

Questo è dunque il problema "inverso" dell'esponenziazione modulare: mentre quest'ultima è semplice da calcolare, in generale il DLP è molto difficile da risolvere!
Nota bene: questo non vuol dire che sia *sempre* un problema difficile, ma solo che *esistono casi* in cui non è computazionalmente fattibile risolverlo.

Esempi banali:

$$2^{?} \equiv 4 \pmod{41}\ [1]$$

$$2^{?} \equiv 5 \pmod{41}\ [2]$$

In [1] il modulo è inutile: esiste un logaritmo intero "normale" ($2^2 = 4$).
In [2] c'è un vero e proprio DLP; ciononostante il modulo è molto piccolo e possiamo fare un bruteforce dei possibili candidati senza troppi sforzi ($2^7 \equiv 5 \pmod{41}$).

1.2 Approfondimento sul protocollo

Ti rimando alle slides per il funzionamento del protocollo (penso che a questo punto sia chiaro, ma ti ricordo che tutte le esponenziazioni sono effettuate *modulo* p).
Un'osservazione che può essere utile effettuare è la seguente: perché g è chiamato *generatore*?
La risposta sta nei numeri *generati* dalle potenze di $g \pmod{p}$.
Esempio: considera $p = 11,\ g = 2$. I numeri *generati* dalle potenze di $g \pmod{p}$ sono:

e	0	1	2	3	4	5	6	7	8	9	10
$g^e \pmod{p}$	1	2	4	8	5	10	9	7	3	6	1

Come puoi notare, le potenze di g vanno a toccare (quindi g *genera*) *tutti* i numeri da 1 a 10.
Non per tutti i numeri da 1 a 10 vale però lo stesso! Considera ad esempio $g = 4 \pmod{11}$.

e	0	1	2	3	4	5
$g^e \pmod{p}$	1	4	5	9	3	1

Come puoi vedere, $g = 4$ genera molti meno numeri di $g = 2$! Tornando al nostro caso, cosa succede se nel protocollo di Diffie-Hellman si va a scegliere come generatore un numero che genera ben pochi elementi? Beh, molto banalmente, lo spazio di ricerca per il nostro logaritmo discreto si riduce (così come il numero di possibilità per il segreto condiviso).

Per questo motivo di solito con "g generatore" si intende "generatore di tutti gli interi da 1 a $p-1$ (estremi inclusi)", anche se spesso "generatore di un numero sufficientemente grande di elementi" è abbastanza per garantire la difficoltà del DLP.
Ci sarebbero altri casi particolari interessanti da studiare, ma il discorso diventa intricato abbastanza in fretta (anche lo studio di p - anzi, di $p-1$ - vorrebbe il suo spazio..).
"Bello tutto, ma io di queste informazioni che me ne faccio?" Beh, tutte queste osservazioni servono a farti entrare un po' nell'ottica delle cose che possono succedere (più o meno di proposito, a seconda della challenge, ma che anche nel mondo reale hanno causato disastri!).
Ti basti sapere che, in generale, con p un numero molto grande estratto casualmente e $g = 2$, la probabilità di incappare in questi casi particolari è molto bassa.
Quando però cominci a vedere primi non casuali (fissi o "generati male").. fai suonare qualche campanello d'allarme. Un'occhiatina in più a quel parametro non farà male.
Ti consiglio in ogni caso di dare un'occhiata alla pagina Wikipedia[1] sul logaritmo discreto, se vuoi provare a cercare qualcosa per conto tuo.

[1] https://it.wikipedia.org/wiki/Logaritmo_discreto