SCAMBIO DELLA CHIAVE CON ALGORITMO DIFFIE - HELLMAN

Nel 1976, **Whitfield Diffie** e **Martin Hellman** pubblicarono un protocollo crittografico - oggi noto come **scambio di chiavi di Diffie-Hellman** - che consente di scambiarsi una chiave di cifratura, anche se un intruso controlla il canale di comunicazione.

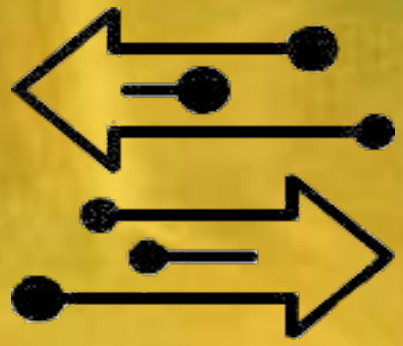
Nell'implementazione originale (e più semplice) del protocollo si considera inizialmente un **numero g**, generatore del gruppo moltiplicativo degli interi modulo **p**, dove **p** è un numero primo.
Uno dei due interlocutori (sia Alice) sceglie un **numero casuale** "**a**" e calcola il valore $A = g^a \bmod p$ (dove **mod** indica l'operazione modulo, ovvero il resto della divisione intera) e lo invia attraverso il canale pubblico all'altro interlocutore (sia Bob), assieme ai valori **g** e **p**. Bob sceglie un **numero casuale** "**b**" , calcola $B = g^b \bmod p$ e lo invia ad Alice.
A questo punto Alice calcola $K_A = B^a \bmod p$, mentre Bob calcola $K_B = A^b \bmod p$.
I valori calcolati sono gli stessi, in quanto $B^a \bmod p = A^b \bmod p = g^{ab} \bmod p$.

Alice				Bob		
Segreto	Pubblico	Calcola		Calcola	Pubblico	Segreto
	p, g				p, g	
a						b
		$g^a \bmod p$	→			
			←	$g^b \bmod p$		
$g^{ab} \bmod p$			=			$g^{ab} \bmod p$

1. Alice e Bob si accordano di usare un numero primo $p = 23$ e la base $g = 5$.
2. Alice sceglie un numero segreto $a = 6$ e invia a Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23 = 8$
3. Bob sceglie l'intero segreto $b = 15$ e invia ad Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23 = 19$.
4. Alice calcola $K_A = (g^b \bmod p)^a \bmod p = B^a \bmod p$
   - $K_A = 19^6 \bmod 23 = 2$.
5. Bob calcola $K_B = (g^a \bmod p)^b \bmod p = A^b \bmod p$
   - $K_B = 8^{15} \bmod 23 = 2$ = **CHIAVE SEGRETA**.

I due interlocutori possono ora usare $g^{ab} \bmod p$ come chiave segreta per cifrare le comunicazioni successive.

Si noti che un attaccante può ascoltare tutto lo scambio, ma per calcolare i valori "**a**" e "**b**" avrebbe bisogno di risolvere l'operazione del **logaritmo discreto**, che è computazionalmente onerosa e richiede parecchio tempo (sicuramente molto più del tempo di conversazione tra i 2 interlocutori).



SCAMBIO DI CHIAVI CRITTOGRAFICHE

Scopri come viene protetto il traffico dati su internet e come puoi condividere segretamente una chiave di comunicazione con il tuo partner.

RIFERIMENTI

- http://www.c3t.it/projects/awareness/articoli&brochure/scambio_chiavi/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

PERCHÉ LO SCAMBIO DELLE CHIAVI È IMPORTANTE

Per preservare la riservatezza dei dati durante la trasmissione su un canale pubblico, i *protocolli di trasferimento file sicuri* (come ad esempio **FTPS**, **HTTPS** e **SFTP**) cifrano i dati attraverso la crittografia simmetrica.

Questo tipo di cifratura richiede che le due parti in comunicazione dispongano di una chiave segreta.
Il problema è che, condividere la chiave in modo sicuro non è un compito facile; le due parti potrebbero essere **geograficamente separate** e potrebbero non essersi nemmeno **mai incontrate**.
La chiave non può essere semplicemente scambiata tramite uno degli ordinari metodi di comunicazione (es. **e-mail**), in quanto chiunque ne venga in possesso sarebbe in grado di decifrare tutti i file che le due parti si invieranno usando la chiave segreta.

C'è bisogno di un metodo facile da usare, sicuro e altamente scalabile, progettato per funzionare su canali insicuri.
Ecco perché sono stati sviluppati **protocolli di scambio delle chiavi** che consentono a due parti di scambiarsi chiavi simmetriche su reti non sicure come Internet.

SCAMBIO DELLA CHIAVE NELL' HTTPS

Il protocollo crittografico più comune quando si fa riferimento alla rete Internet è l'**HTTPS** (HyperText Transfer Protocol Secure).
In questo caso, il processo di **scambio della chiave** viene eseguito durante quello che è noto come **"handshake SSL"**, in una fase preliminare prima dello scambio di file e/o messaggi cifrati.

Un'applicazione (detta *client* - può essere ad esempio un browser web come Firefox o Google Chrome) richiede una connessione ad un *server* (es. una pagina web qualsiasi) inviando un messaggio noto come **"client Hello"**. Questo solitamente consiste di un insieme di dati casuali e di una lista detta **"suite di cifratura"**, cioè un insieme di algoritmi per lo scambio delle chiavi, la crittografia simmetrica e l'autenticazione dei messaggi.

Non appena il server riceve il **client Hello**, confronterà l'elenco di **suite di cifratura** supportate dal proprio sistema con l'elenco inviatogli dal client e (idealmente) sceglierà la suite migliore.
In particolare, verrà scelto l'algoritmo per lo **scambio della chiave** più adeguato, così che, *client* e *server*, possano avviare il processo di scambio della chiave e successivamente usarla per la cifratura dei messaggi.