public key encryprion

un piccolo ripasso sulla chiave simmetrica. abbiamo visto che:

- Alice e Bob si scambiano una chiave segreta attraverso un canale sicuro (io vado fisicamente in banca e ottengo la chiave)
- la stessa chiave è usata sia per criptare che per decriptare il messaggio (motivo per cui si chiama chiave simmetrica)

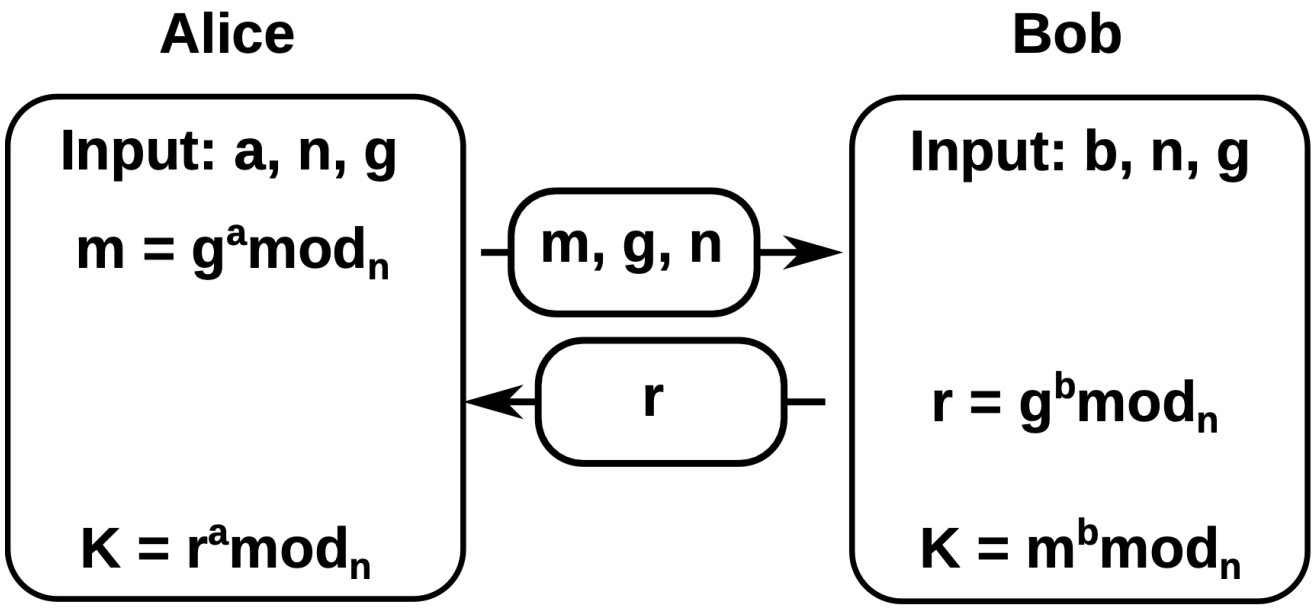
è necessario avere quindi un canale sicuro sul quale scambiarsi la chiave segreta, verrà usato solamente per lo scambio, il resto della comunicazione avviene in un canale non sicuro.

principi chiave pubblica

il principio alla base della chiave pubblica è permettere ad Alice e Bob di poter comunicare in modo sicuro senza doversi scambiare nessuna informazione sensibile. esistono molti algoritmi per assolvere a questo scopo, i più famosi sono:

- **Diffie-Halleman** Key exchange
- **RSA** public key encryption
- **Elliptic curve** encryption (non viene trattata all'interno del corso)

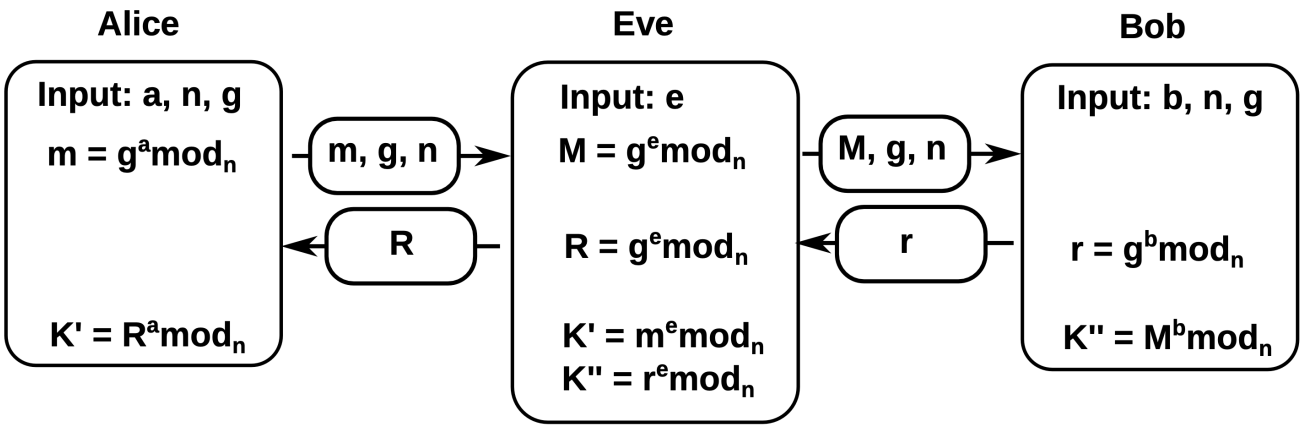
Diffie-Halleman DH è un protocollo pensato per permettere ad Alice e Bob di negoziare una chiave simmetrica segreta senza doversi scambiare alcuna informazione sensibile. è basato sulla difficoltà di computare il logaritmo discreto.



- Alice sceglie un numero n primo, a casuale, g che corrisponde ad una radice primitiva di n (cioè g è un generatore di n -> non so che vuol dire)
- Alice calcola $m = g^a mod_n$
- Alice invia m, g, n a Bob (anche lui ha effettuato gli stessi passaggi)
- Bob risponde con il suo m (nell'immagine rappresentato da r)

- sia Alice che Bob generano la chiave K

Nel caso in cui Eve dovesse intercettare il traffico, non sarebbe in grado di generare la chiave K perchè non sarebbe a conoscenza dei vaori a e b (che solo Alice e Bob conoscono). Il problema ricorrerebbe se Eve non facesse solo sniffing ma un vero e proprio man in the middle.



In **conclusione** il protocollo DH è in grado di garantire *confidenzialità* solamente se accoppiato con un sistema che garantisca *autenticazione*

RSA

è l'algoritmo più utilizzato il principio alla base di RSA è:

- ogni utente possiede **due chiavi**
- la chiave **privata** la conosce solamente l'utente
- la chiave **pubblica** è conosciuta da tutti

Tutto quello che viene criptato con la chiave pubblica può essere decriptato solamente con la relativa chiave privata, garantendo quindi **segretezza**.

Nella teoria stiamo parlando di una funzione $f: D \to R$ con un parametro t tale che:

- f è facile da calcolare da D a R;
- f è facile da calcolare da R a D se conosci t;
- f è teoricamente impossibile da calcolare da R a D se non conosci t.

In matematica una funzione di questo tipo non esiste. è necessario quindi trovare un'approssimazione che risulti *computazionalmente impossibile*.

creazione chiave

- scegliere due numeri primi grandi p e q che non devono essere mostrati
- computa $n=pq$ e $\phi(n) = (p-1)(q-1)$
- trova un numero e tale che $2 < e < \phi(n)$ e non abbia divisori comuni con $\phi(n)$ (devono essere coprimi)
- trova d tale che $d\cdot e \ mod_{\phi(n)} = 1$
- In questo modo (e, n) rappresenta la chiave **pubblica**
- d è la chiave **privata**

Dato quindi un messaggio M, per poterlo **criptare** devo fare $C = M^e mod_n$ Per **decriptarlo** devo fare $M = C^d mod_n$

RSA, inoltre funziona anche al contrario (cripto con la privata, decripto con la pubblica). Questo processo è usato per la **firma digitale**, permettendo quindi di garantire **autenticazione**.

performance Criptare risulta computazionalmente più costoso che decriptare, per questo motivo la soluzione che è stata adottata per le comunicazioni è una combinazione di chiave pubblica e chiave simmetrica: uso RSA per trasmettere in sicurezza la chiave privata condivisa. Uso poi la chiave condivisa per trasmettere i messaggi