La matematica della crittografia

a cura di Alessandro Musesti
Università Cattolica del Sacro Cuore, Brescia

Condivisione di una chiave: l'esempio con i colori

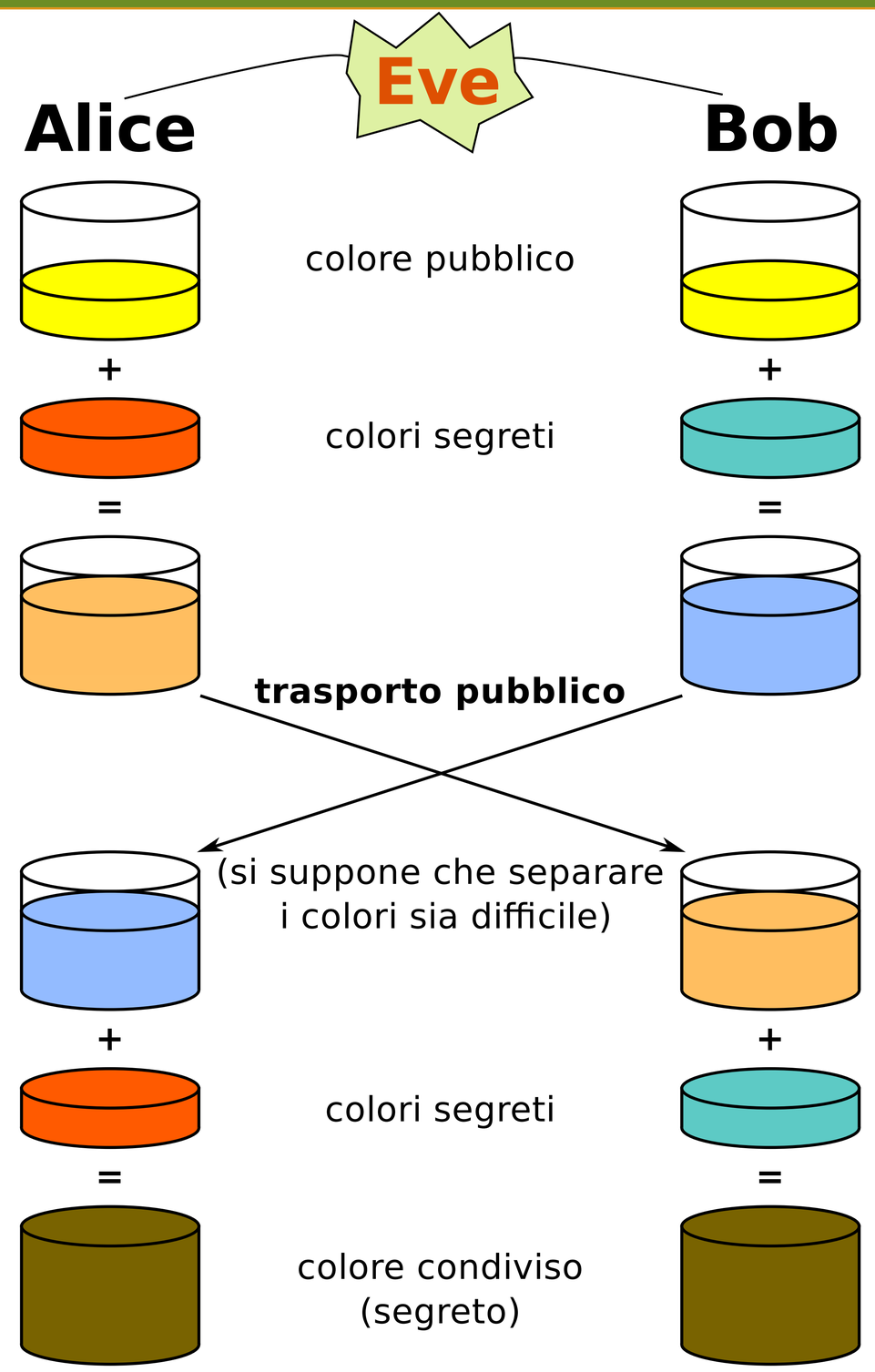
Alice e Bob vogliono poter scambiare messaggi senza che altri (rappresentati da Eve, il malvagio) li capiscano. Per fare questo devono entrambi avere una "chiave" che apra lo stesso lucchetto. Come possono fare a condividere questa chiave?
L'esempio qui a destra, fatto coi colori, si basa su un colore segreto (la chiave privata) e un colore noto a tutti (la chiave pubblica). Entrambi giungono a condividere un colore (quella tonalità di verde) senza che Eve ne sia a conoscenza.

È **facile** mescolare i colori, ma è **difficile** capire quali colori formano una miscela.

La matematica ci viene in aiuto: una **funzione unidirezionale** è una funzione facile da calcolare ma difficile da invertire. Ad esempio: è facile (con un calcolatrice!) calcolare

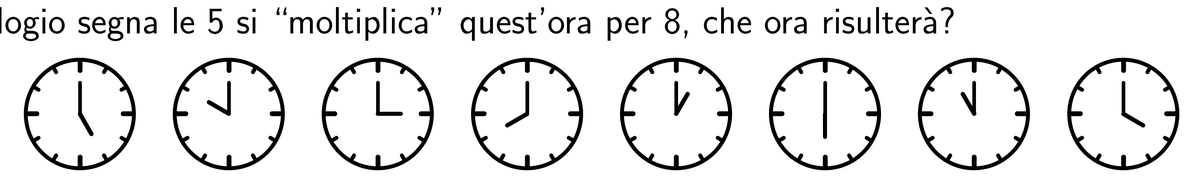
$$59 \times 31 = 1829$$

ma è più difficile (perché ci vuole molto tempo!) scoprire che 1829 è composto da 59 e 31.



Un attrezzo matematico: le moltiplicazioni e le potenze "sull'orologio"

Se l'orologio segna le 5 si "moltiplica" quest'ora per 8, che ora risulterà?



Le 4, poiché $5 \times 8 = 40 = 12 \times 3 + 4$. Quindi la lancetta delle ore fa tre giri e finisce sulle 4.
Nell'aritmetica "dell'orologio" non interessa il numero dei giri, ma solo quello che avanza alla fine (il **resto** della divisione).
Noi considereremo orologi con p ore, dove p è un numero primo. Le operazioni fatte su questi orologi verranno indicate col suffisso "mod p" (si legge **modulo** p).
Ad esempio, scegliendo $p = 11$ si ha $5 \times 8 = 7 \bmod 11$ e $2^6 = 9 \bmod 11$.

Lo scambio di chiavi Diffie–Hellman–Merkle (1976)

È un metodo basato sull'elevamento a potenza e sull'aritmetica dell'orologio.
Si prende un numero primo p, ad esempio $p = 17$, e un **generatore** g, cioè un numero più piccolo di p tale che calcolando

$$g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} \bmod p$$

si esauriscano tutti i numeri tra 1 e $p-1$. Ad esempio, si può verificare che 6 è un generatore per $p = 17$, poiché

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6^n	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Questi numeri p e g sono noti a tutti e decisi una volta per tutte. Poi si esegue la procedura seguente:
1) Alice sceglie un numero a caso a tra 1 e $p-1$, e lo stesso fa Bob con un numero b. Questi numeri sono le **chiavi private** di Alice e Bob, e sono **segreti**.
Nel nostro esempio, potrebbe essere $a = 10$ e $b = 15$.
2) Alice calcola il numero $A = g^a \bmod p = 6^{10} \bmod 17 = 15$. Allo stesso modo, Bob calcola il numero $B = g^b \bmod p = 6^{15} \bmod 17 = 3$.
I numeri A e B sono le **chiavi pubbliche** e vengono divulgati. Chiunque li può conoscere.
3) Infine Alice prende la chiave pubblica di Bob, $B = 3$, e calcola $B^a \bmod p = 3^{10} \bmod 17 = 8$.
Allo stesso modo, Bob prende la chiave pubblica di Alice, $A = 15$, e calcola $A^b \bmod p = 15^3 \bmod 17 = 8$.

È un caso che sia risultato lo stesso numero? Certamente no: si ha **sempre** $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a \bmod p$.
Quindi Alice e Bob hanno una chiave in comune: il numero 8.

Sicurezza della procedura

Che cosa conosce Eve? Conosce: il numero primo p, il generatore g, le chiavi pubbliche $A = g^a$ e $B = g^b$. Da questi dati si può scoprire la chiave comune $A^b = B^a$?
L'unico modo per farlo è scoprire almeno una delle due chiavi segrete a oppure b.
Nel nostro esempio, sapendo che $p = 17$, $g = 6$ e $A = g^a = 15$, si vorrebbe scoprire a: nella tabella scritta sopra si va a cercare quale potenza di 6 risulta 15 (modulo 17), e si trova $n = 10$. Quindi la chiave segreta di Alice è 10.
Dove sta la sicurezza della procedura? Nella realtà si usano numeri primi molto grandi, fatti da almeno 300 cifre, e la lista da scorrere per individuare l'esponente a a partire dalla conoscenza di g^a è molto, molto lunga! Questo è il problema del **logaritmo discreto**, ed è una funzione unidirezionale: è abbastanza facile calcolare $A = g^a$, ma è molto difficile scoprire l'esponente a conoscendo g e A. Anche i computer più potenti impiegherebbero centinaia di anni.

Utilizzo della chiave condivisa

Una volta ottenuta una chiave condivisa, si può procedere a crittografare un messaggio in vari modi. Ad esempio, se Alice vuole comunicare a Bob un numero segreto, per esempio il numero della sua carta di credito 2442 4243 5089 4523, può moltiplicarlo per la chiave comune 8, ottenendo 19539394807156184. Bob, ricevuto il numero, lo divide per 8 riottenendo il numero di partenza.
Il malvagio Eve, sempre in ascolto, vedrebbe passare il numero 19539394807156184, ma non potrebbe collegarlo al numero di carta di credito di Alice (a meno che non conosca la chiave comune 8). Oppure la chiave comune potrebbe essere il punto di partenza per un cifrario di Cesare, significando uno spostamento di 8 lettere: il nome ALESSANDRO diventerebbe ITODDIVNCZ (nell'alfabeto a 21 lettere) e Bob potrebbe facilmente decodificarlo.
Attualmente il metodo più usato per codificare messaggi con una chiave condivisa è l'algoritmo AES (Advanced Encryption Standard).