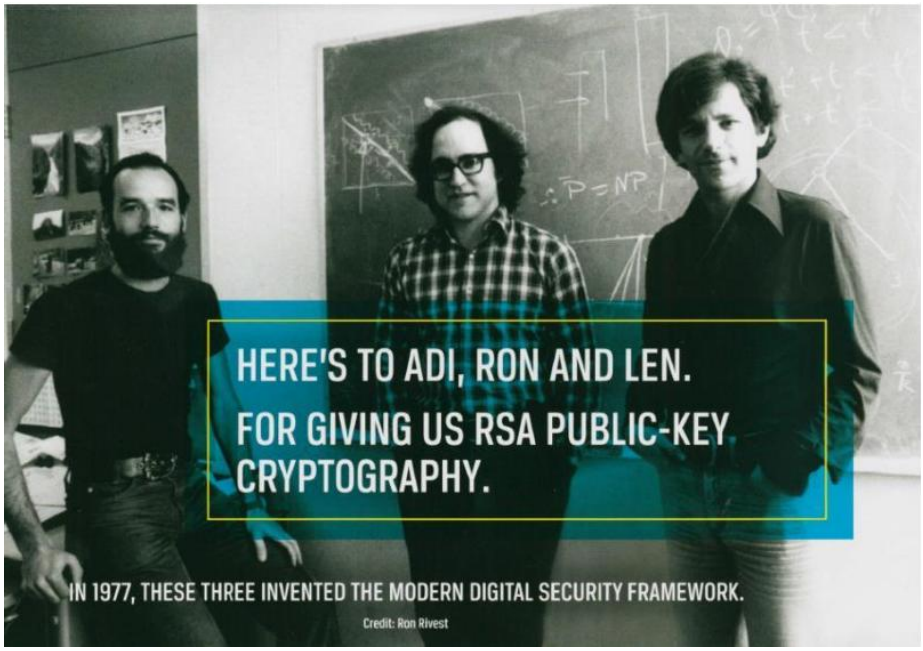
Nel loro celebre lavoro del 1976 [1], Whitfield Diffie e Martin Hellman introdussero il paradigma della crittografia asimmetrica come soluzione per scambio di chiavi, cifratura e autenticazione (firma digitale).

[1] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976.

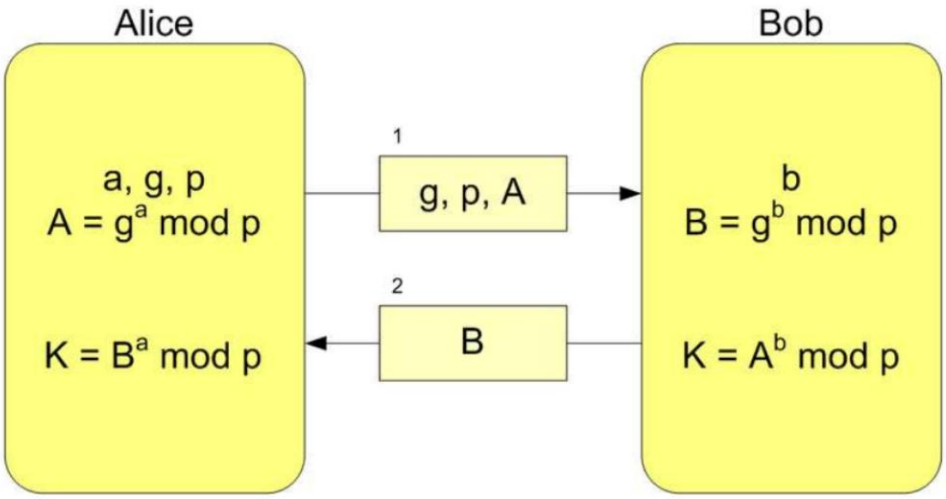
In termini pratici, Diffie e Hellman introdussero una procedura per lo scambio di chiavi basata sul logaritmo discreto.

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman proposero un metodo per la cifratura asimmetrica basato sulla fattorizzazione di numeri interi (RSA, dalle iniziali dei loro cognomi)



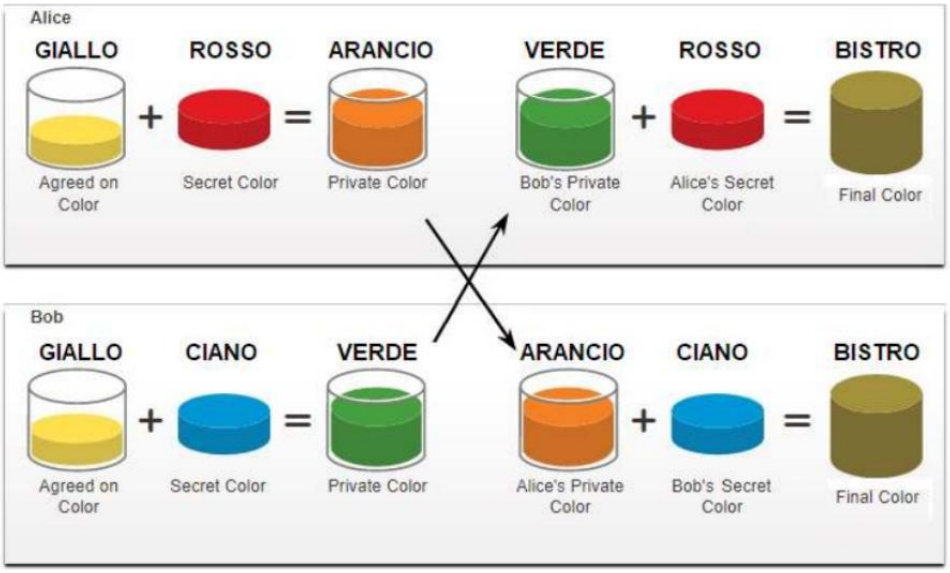
Diffie-Hellman key exchange

Tecnica crittografica sviluppato nel 1976 da Whitfield Diffie e Martin Hellman, per lo scambio di una chiave condivisa e segreta attraverso un canale di comunicazione insicuro (pubblico).



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

La seguente figura illustra come opera il sistema DH con una analogia, con tutti i limiti di queste operazioni.



C'è un'ipotesi da esplicitare: chi ha una vernice miscelata non riesce ad estrarre i colori (non invertibilità dell'operazione di miscelazione).

Un terzo, che conosca solo il giallo, l'arancio e il verde, non è in grado di produrre lo stesso bistro creato da Alice e Bob, cioè la loro PSK (pre-shared key) o session key.

Un esempio (calcolo) semplice DH in Excel

Nella figura seguente è riprodotto in Excel uno scambio di Diffie-Hellman per ricavare una PSK a 8 bit. Il numero generatore "g" (il giallo) è 2, il numero primo "p" a 8 bit è 233, mentre i colori segreti di Alice e Bob sono l'8 e il 9 (il rosso e il ciano).

Un problema è che i numeri scambiati tra Alice e Bob (23 e 46, cioè il verde e l'arancio), se elevati alle potenze 9 e 8 rispettivamente, danno dei numeri "importanti" (svariati miliardi), e non si può andare molto oltre, se si vuole evitare

che Excel passi alla notazione "mantissa + esponente" e perda precisione, che invece è essenziale per calcolare un resto esatto della divisione per 233. Si vede però che la parte frazionaria della divisione è identica nei due calcoli (0,3176), e quindi lo sarà anche il resto della divisione intera, pari alla PSK (74, il bistro) che sarà pertanto condivisa tra Alice e Bob.

Diffie-Hellman semplice			numeri "pubblici" =	2, (233?), 23, 46
			numeri "segreti" =	Alice=8, Bob=9
			PSK a 8 bit generata	**74**
g =	2	= numero generatore		
p =	233	= numero primo a 8 bit		= 11101001
Alice sceglie il n. segreto "a" =			8	
	calcola "2 alla 8" =		256	
	vi applica il "mod 233" =		23	
	e invia tale numero a Bob			
Bob sceglie il n. segreto "b" =			9	
	calcola "2 alla 9" =		512	
	vi applica il "mod 233" =		46	
	e invia tale numero ad Alice			
Alice calcola "46 alla 8" =			20.047.612.231.936	
	che diviso 233, ha fraz. 0,3176		86.041.254.214,3176	
	o, applicando il "mod 233" =		**74**	= 01001010
Bob calcola "23 alla 9" =			1.801.152.661.463	
	che diviso 233, ha fraz. 0,3176		7.730.268.933,3176	
	o, applicando il "mod 233" =		**74**	= 01001010