Protocollo Diffie-Hellman

Protocollo per lo "scambio" sicuro di una chiave simmetrica concordata tra due parti. Rispetto al sistema ibrido RSA/AES ha il vantaggio che la generazione della chiave non è a carico di una sola delle parti, che potrebbe non avere le risorse computazionali necessarie a garantirne la sicurezza.

Protocollo

Alice e Bob scelgono:

- un primo p molto grande (migliaia di bit);
- un generatore g di $\mathbb{Z}/p\mathbb{Z}^*$

p e g possono essere selezionati in una lista pubblica, visto che g è difficile da trovare e non è necessario che p e g rimangano segreti.

Alice	**Eve**	**Bob**
concorda p, g con Bob	intercetta p, g	concorda p, g con Alice
sceglie a caso $1 < a < p-1$		sceglie a caso $1 < b < p-1$
invia $A = g^a \bmod p$	intercetta A	riceve A
riceve B	intercetta B	invia $B = g^b \bmod p$
calcola $k = B^a \bmod p$		calcola $k = A^b \bmod p$

Il valore k calcolato da Alice è identico a quello calcolato da Bob:

$$B^a \equiv g^{ba} \equiv g^{ab} \equiv A^b \mod p.$$

Eve non può calcolarlo perché non conosce né a né b, e per ricavarli dovrebbe risolvere un logaritmo discreto (subesponenziale).

Alice e Bob possono estrarre una chiave AES da k selezionando 256 bit, per esempio i 256 meno significativi.

Escludiamo 1 e $p-1$ dalla scelta di a altrimenti A è g o 1, e ricavare a è immediato. Visto che g è un generatore, esponenti diversi producono valori diversi, ed è possibile generare uno qualsiasi degli elementi di $\mathbb{Z}/p\mathbb{Z}^* \setminus \{1\}$.