Attacchi a Diffie-Hellman

Vulnerabile ad un attacco attivo man-in-the-middle:

Alice	**Eve**	**Bob**
concorda p, g con Bob	intercetta p, g	concorda p, g con Alice
sceglie $1 < a < p - 1$	sceglie $1 < e < p - 1$	sceglie $1 < b < p - 1$
calcola $A = g^a \bmod p$	calcola $E = g^e \bmod p$	calcola $B = g^b \bmod p$
invia A	sostituisce A con E	riceve E
riceve E	sostituisce B con E	invia B
calcola $k_A = E^a \bmod p$	calcola $k_A = A^e \bmod p$ e k_B	calcola $k_B = E^b \bmod p$

Vale:

$$k_A = g^{ax} \bmod p \qquad k_B = g^{bx} \bmod p.$$

A questo punto Alice e Bob hanno generato due chiavi diverse, entrambe in possesso di Eve, che può intercettare i messaggi di Alice, decifrarli con k_A, leggerli e/o modificarli, cifrarli con k_B e spedirli a Bob (o viceversa).

Risolto con certificati digitali.