come utilizzare un PKCS

- abbiamo visto che affinché un CS sia sicuro, la cifratura deve essere randomizzata
- in un cifrario simmetrico (per esempio AES) si sceglia un'opportuna modalità di funzionamento (per esempio CBC)
- e in un PKCS?
- sia $f : A \to B$ una funzione trapdoor one-way (come quella RSA)
- f si utilizza per generare la chiave

come utilizzare un PKCS

- per cifrare si usa $f : A \to B$ funzione trapdoor one-way
- insieme a un CS simmetrico in modalità sicura (CBC-AES)
- Alice sceglie in modo casuale $a \in A$ e calcola $f(a) = b$ (facile - pubblico)
- Alice cifra il messaggio x con la chiave a e ottiene il CT y (usando AES: $y = e_a(x)$)
- trasmette a Bob la coppia (b, y)

come utilizzare un PKCS

- Bob riceve la coppia (b, y)
- per decifrare deve conoscere $a = f^{-1}(b)$
- è il solo a possedere l'informazione segreta che gli permette di invertire la f
- può ottenere a e decifrare con AES: $x = d_a(y)$
- la randomizzazione "viene" dall'AES
- per maggiore sicurezza, in genere la chiave non è a ma è $h(a)$ dove h è una fuzione hash

problemi della chiave pubblica

- la crittografia a PK è lenta - molto più lenta della crittografia simmetrica
- viene utilizzata come abbiamo appena visto - per cifrare la chiave che Alice utilizza per comunicare con Bob
- oppure viene usata all'inizio di una sessione fra due utenti per stabilire una chiave da usare con un algoritmo simmetrico (key exchange)
- e per gli schemi di firma digitale

problemi di sicurezza

- bisogna avere un modo per verificare la corrispondenza fra utenti e chiavi
- Alice scrive a Bob usando quella che crede essere la chiave pubblica di Bob
- se invece fosse quella di Eve?
- inoltre, in un CS simmetrico solo Alice e Bob conoscono la chiave
- se Bob riceve un messaggio di Alice e la decifratura del messaggio ha senso, il messaggio proviene certamente da Alice
- in un PKCS, chiunque può scrivere un messaggio cifrato a Bob affermando di essere Alice
- serve una firma digitale