Gestione della chiave

- La crittografia a chiave pubblica aiuta a risolvere il problema della distribuzione delle chiavi
- Dobbiamo occuparci...
  - Della distribuzione delle chiavi pubbliche
  - Dell'uso della crittografia a chiave pubblica per distribuire chiavi di sessione

Distribuzione delle chiavi pubbliche

- Vi sono 4 possibili strategie
  - Annuncio pubblico
  - Elenco pubblico
  - Autorità di distribuzione delle chiavi pubbliche
  - Certificati con chiave pubblica

Annuncio pubblico

- Gli utenti distribuiscono le chiavi pubbliche tramite messaggi di broadcast o in allegato ai loro messaggi
  - e.g., aggiungendo le chiavi alla fine delle loro e-mail o sui newsgroup
- Vi è però un grande punto debole....
  - Chiunque può spacciarsi per un altro e pubblicare una chiave falsa
  - Un utente malizioso può quindi spacciarsi per un altro

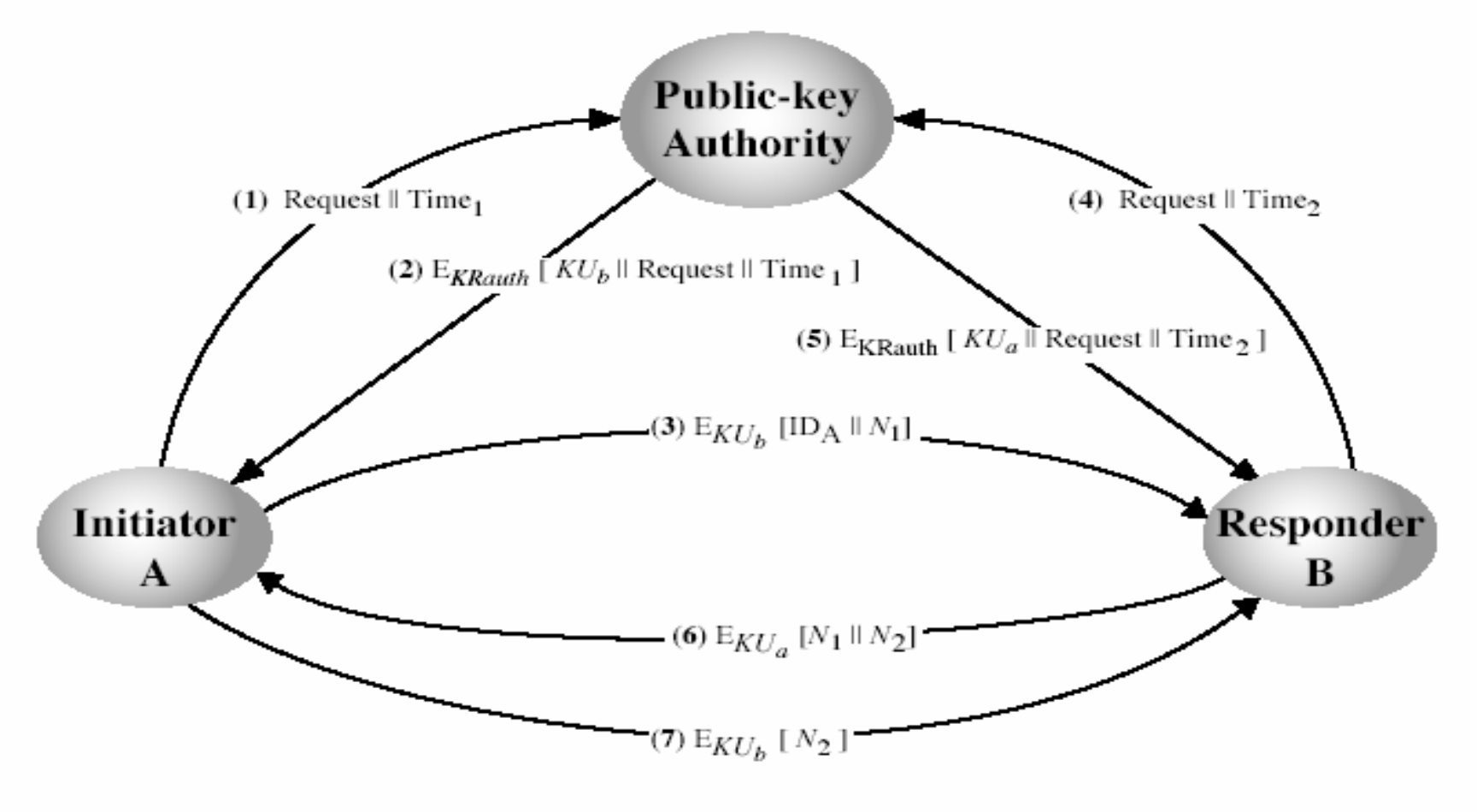
Elenco Pubblico

- Maggiore sicurezza si ha registrando le chiavi presso un elenco pubblico
- Tale elenco è tale che:
  - Contiene voci del tipo {nome,chiave pubblica}
  - Gli utenti registrano la loro chiave in forma sicura
  - Gli utenti possono sostituire la chiave quando vogliono
  - L'elenco viene pubblicato periodicamente
  - L'elenco può essere consultato elettronicamente (in modo protetto)
- L'elenco pubblico può comunque essere violato

Autorità di distribuzione delle chiavi pubbliche

- Migliora la sicurezza mediante un controllo più rigido sulla distribuzione delle chiavi
- Si tratta ancora di un database di chiavi
- Gli utenti devono conoscere la chiave pubblica dell'autorità di distribuzione
- Gli utenti interagiscono con l'autorità per ottenere in modo sicuro la chiave pubblica di altri utenti
  - È richiesto quindi l'accesso in tempo reale al database ogno volta che sono richieste delle chiavi

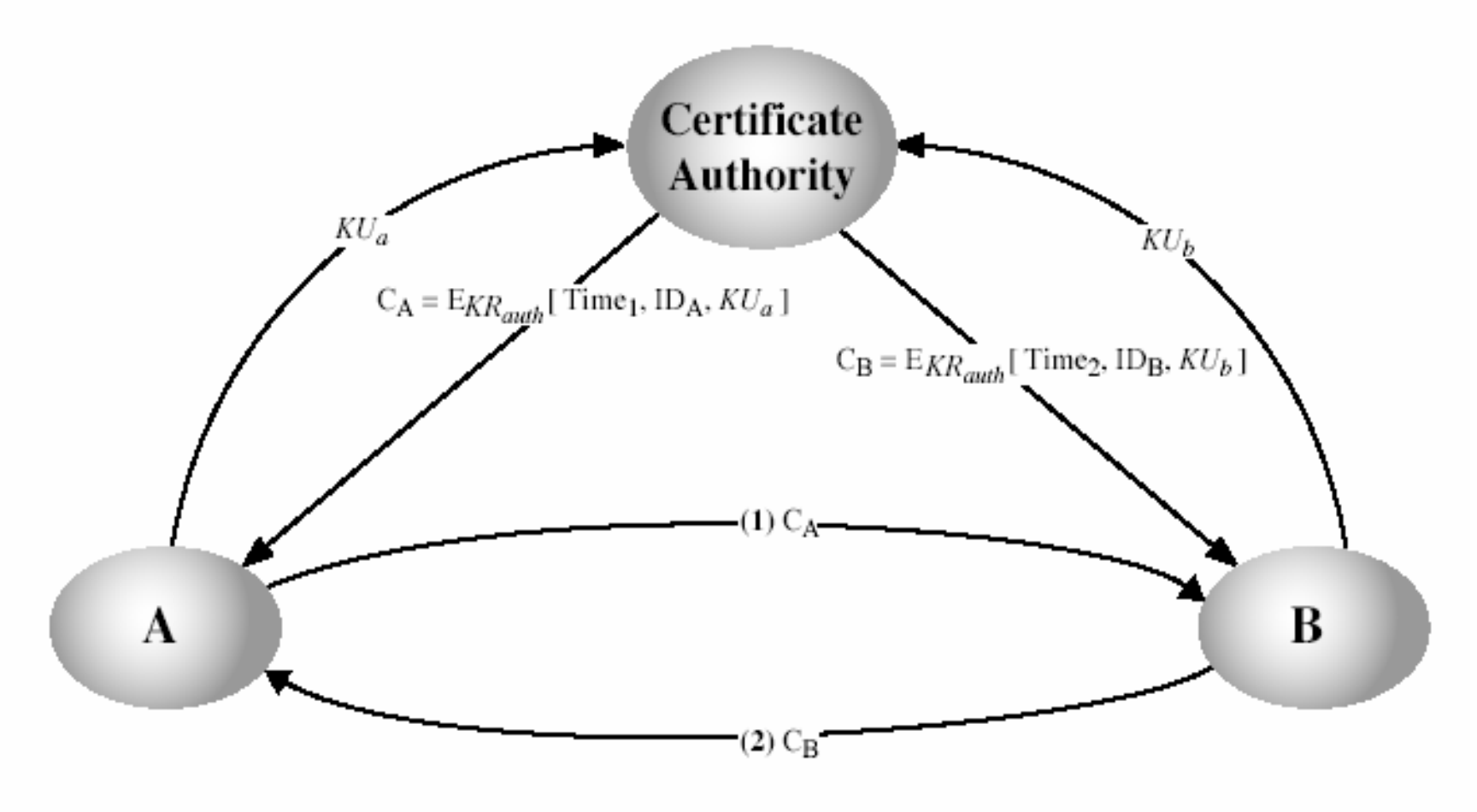
Autorità di distribuzione delle chiavi pubbliche



Certificati a chiave pubblica

- Permettono lo scambio delle chiavi senza bisogno di dover accedere in tempo reale al database pubblico appena considerato
- I certificati possono essere usati direttamente dagli utenti per scambiarsi le chiavi
- Ciascun certificato contiene una chiave pubblica, informazioni supplementari (periodo di validità, condizioni di uso, etc.), e la firma dell'**autorità di certificazione (CA)**
- Un utente invia agli altri la propria chiave trasmettendo il proprio certificato

Certificati a chiave pubblica



Distribuzione delle chiavi segrete tramite chiavi pubbliche

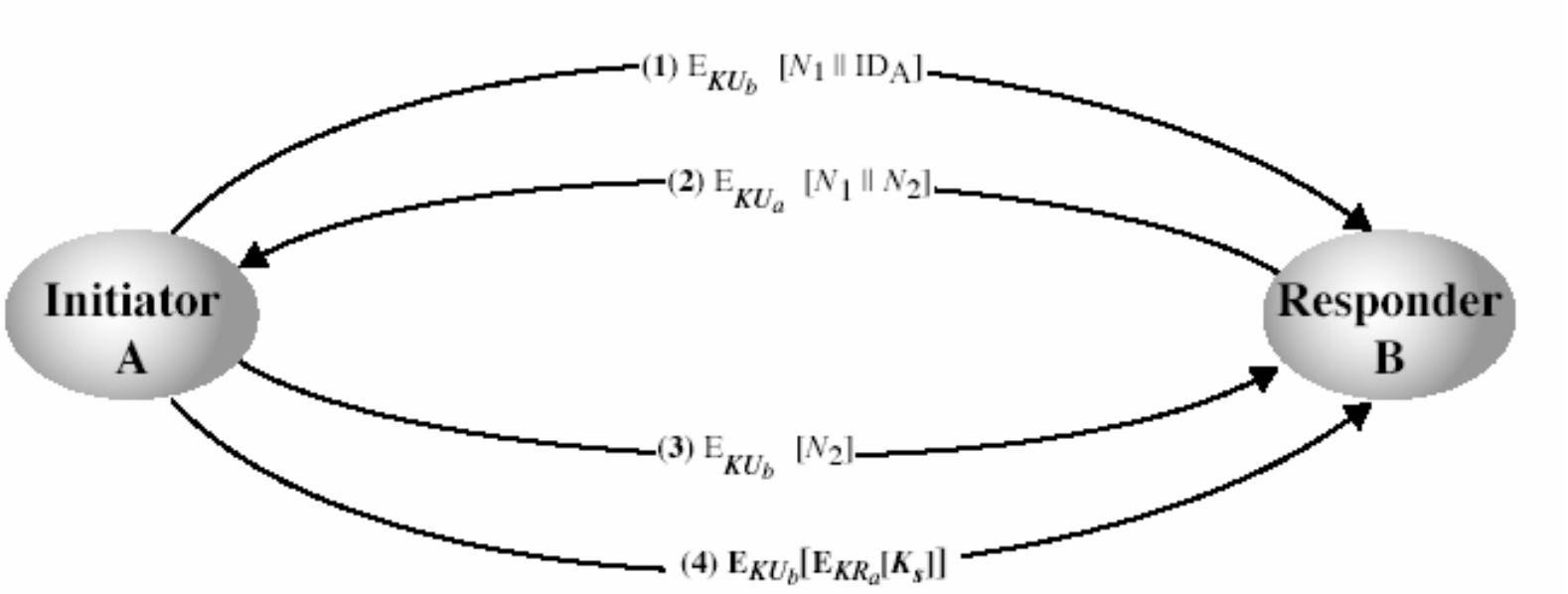
- I metodi presentati permettono di ottenere la chiave pubblica
- Possono essere utilizzati per la segretezza e l'autenticazione
- ...ma gli algoritmi a chiave pubblica sono lenti
- Quindi si preferisce commutare sulla crittografia a chiave segreta
- Bisogna quindi scambiarsi una chiave di sessione
- Vi sono varie strategie...

Semplice distribuzione (Merkle, 1979)

- proposta da Merkle nel 1979
  - A genera una coppia di chiavi
  - A invia a B la chiave pubblica e la sua identità *(in forma non protetta!!!)*
  - B genera una chiave di sessione K e la invia ad A criptata con la chiave pubblica di A
  - A decripta la chiave di sessione e comincia la comunicazione
- Il problema è che un intruso può intercettare il primo messaggio e impersonare entrambi i soggetti della comunicazione

Distibuzione della chiave con segretezza e autenticazione

- Si utilizza in tal caso la crittografia a chiave pubblica



Scambio delle chiavi Diffie-Hellman

- È il primo tipo di schema a chiave pubblica
- by Diffie & Hellman in 1976 insieme all'esposizione del concetto di crittografia a chiave pubblica
  - N.B.: dal 1987 si sa che James Ellis (UK CESG) aveva proposto tale tecnica nel 1970
- È un metodo pratico per lo scambio pubblico di una chiave segreta
- Usato in molti prodotti commerciali

Scambio delle chiavi Diffie-Hellman

- Lo schema di Diffie-Hellman
  - Non può essere usato per scambiarsi un messaggio arbitrario
  - Ma solo per stabilire una chiave nota solo ai due soggetti della comunicazione
- È basato sul concetto di esponenziazione in un campo finito di Galois
- La sua sicurezza si basa sulla difficoltà nel calcolare i logaritmi discreti

Diffie-Hellman: Inizializzazione

- Gli utenti concordano dei parametri comuni e noti:
  - Un grande numero primo o polinomio q
  - α, una radice primitiva di q
- Ogni utente (eg. A) genera la sua chiave
  - sceglie un numero: $x_A < q$
  - Calcola la **chiave pubblica**: $y_A = \alpha^{x_A} \bmod q$
- A rende poi nota la chiave y_A

Diffie-Hellman: Scambio delle chiavi

- La chiave di sessione per A e B è K_{AB}:

  $K_{AB} = \alpha^{x_A . x_B} \bmod q$

  $= y_A^{x_B} \bmod q$ (che B può calcolare)

  $= y_B^{x_A} \bmod q$ (che A può calcolare)

- K_{AB} è poi usata come chiave di sessione in uno schema di crittografia a chiave segreta tra Alice e Bob
- L'attacco a tale schema richiede che venga calcolato X_A, ovvero il logaritmo discreto di y_A in base α e modulo q

Diffie-Hellman: Esempio

- Alice & Bob vogliono scambiarsi le chiavi;
- Concordano su q=353 e α=3
- Selezionano in modo random le chiavi segrete:
  - A sceglie x_A=97, B sceglie x_B=233
- Calcolano le chiavi pubbliche:
  - $y_A = 3^{97} \bmod 353 = 40$ (Alice)
  - $y_B = 3^{233} \bmod 353 = 248$ (Bob)
- Calcolano la chiave di sessione segreta:

$K_{AB} = y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)

$K_{AB} = y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)