Criptografia Assimétrica

Distribuição de Chaves

Distribuição de Chaves Públicas (1)

- Técnicas de distribuição de chaves públicas:
  - Anúncio público
  - Disponibilização de uma directoria pública
  - Autoridade de chave pública
  - Certificados de chave pública

Distribuição de Chaves Públicas (2)

- Anúncio público
  - Chave-pública de conhecimento público
  - Utilização de um algoritmo como o RSA
  - Cada utilizador pode enviar a sua chave pública para outro participante ou realizar a sua difusão
  - Exemplo
    - PGP em que muitos utilizadores difundem a sua chave pública em anexo a mensagens
  - Um anúncio pode ser facilmente forjado

Distribuição de Chaves Públicas (3)

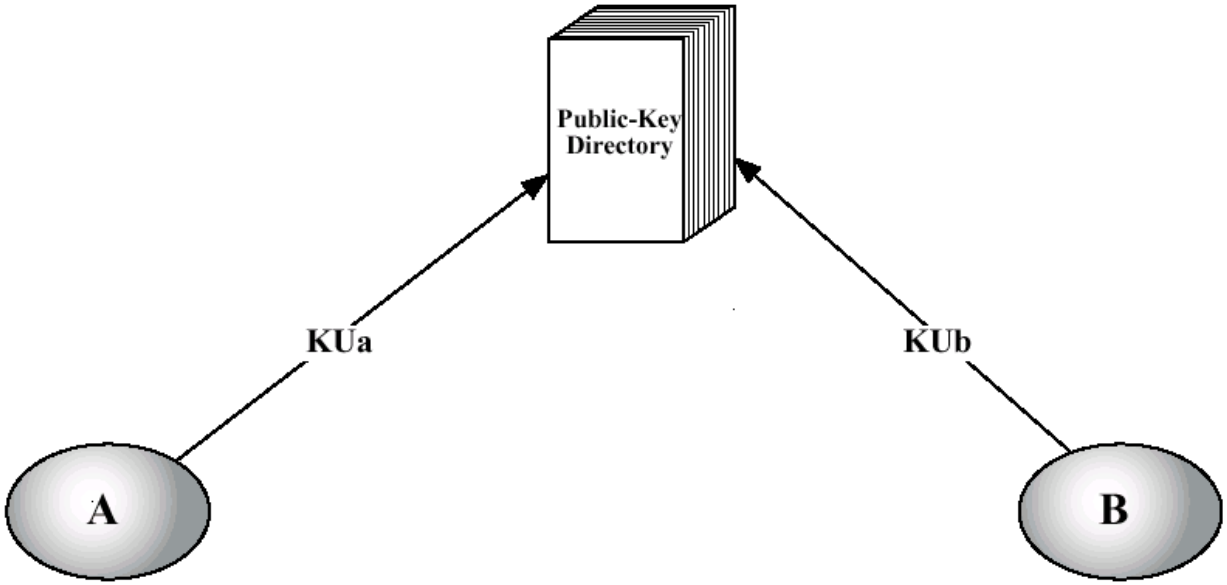
- Anúncio público (cont.)

Distribuição de Chaves Públicas (4)

- Disponibilização de uma directoria pública
  - Mais seguro que o anúncio público
  - Manutenção da responsabilidade de uma terceira entidade
  - Caracteristicas:
    1. Uma entrada por cada participante com o nome e chave pública
    2. Cada participante regista a sua chave pessoalmente ou através de um canal seguro e autenticado
    3. Os participantes podem substituir a sua chave pública em qualquer altura
    4. A lista completa de chaves deve ser publicada periodicamente pela entidade responsável pela directoria
    5. Acesso à directoria por meios electrónicos

Distribuição de Chaves Públicas (5)

- Disponibilização de uma directoria pública (cont.)
  - Se alguém conseguir obter a chave privada da entidade responsável pode forjar as chaves dos participantes e divulgá-las como válidas

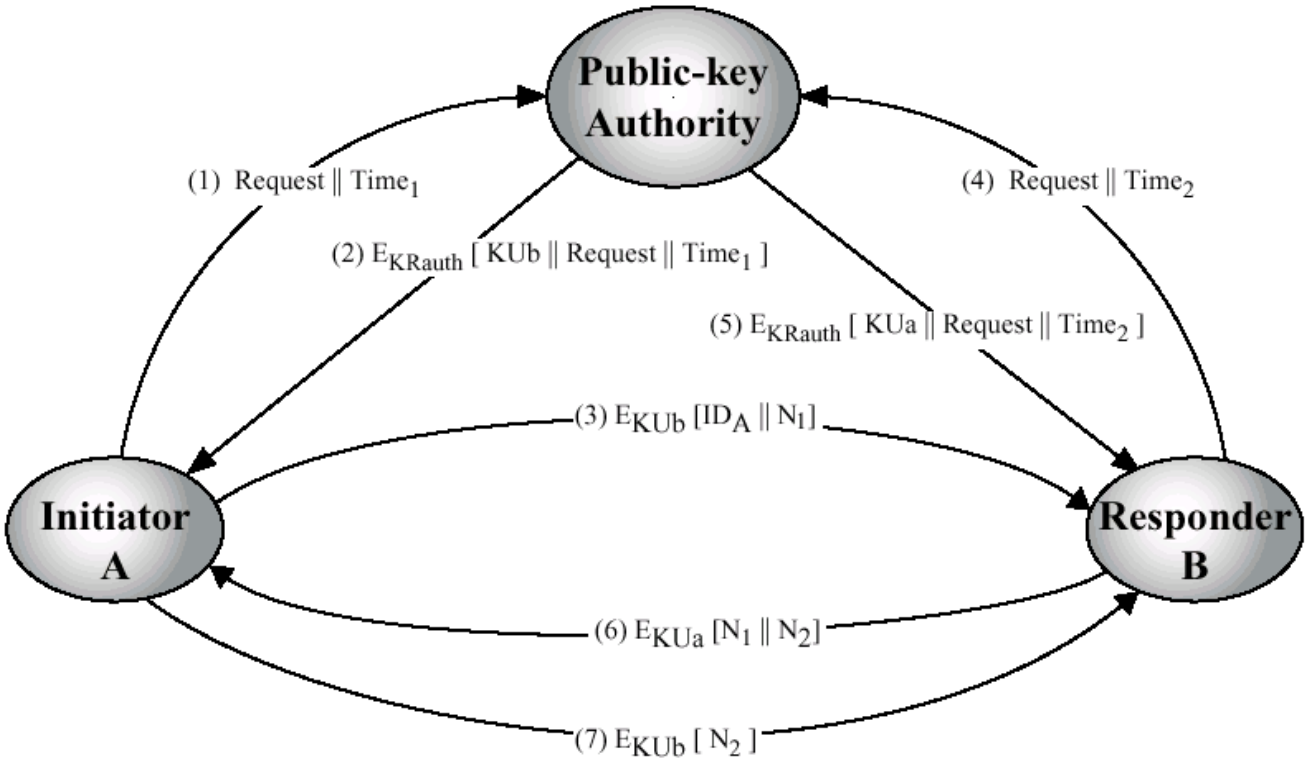


Distribuição de Chaves Públicas (6)

- Autoridade de chave pública (PKA)
  1. *A* envia envia um pedido, com *timestamp*, à *PKA* para obter a chave pública de *B*
  2. A *PKA* responde com uma mensagem cifrada com a sua chave privada KR_{auth}. A mensagem contém:
     - KU_b, o pedido original (para verificação) e o *timestamp*.
  3. *A* envia uma mensagem a *B* cifrada com KU_b contendo ID_A e N_1
  4. Igual ao passo *1*, mas para *B*
  5. Igual ao passo *2*, mas para *B* onde obtém KU_a
  6. *B* envia uma mensagem a *A* cifrada com KU_a contendo N_1 e N_2
  7. *A* envia uma mensagem a *B* cifrada com KU_b contendo N_2

Distribuição de Chaves Públicas (7)

- Autoridade de chave pública (cont.)



Distribuição de Chaves Públicas (8)

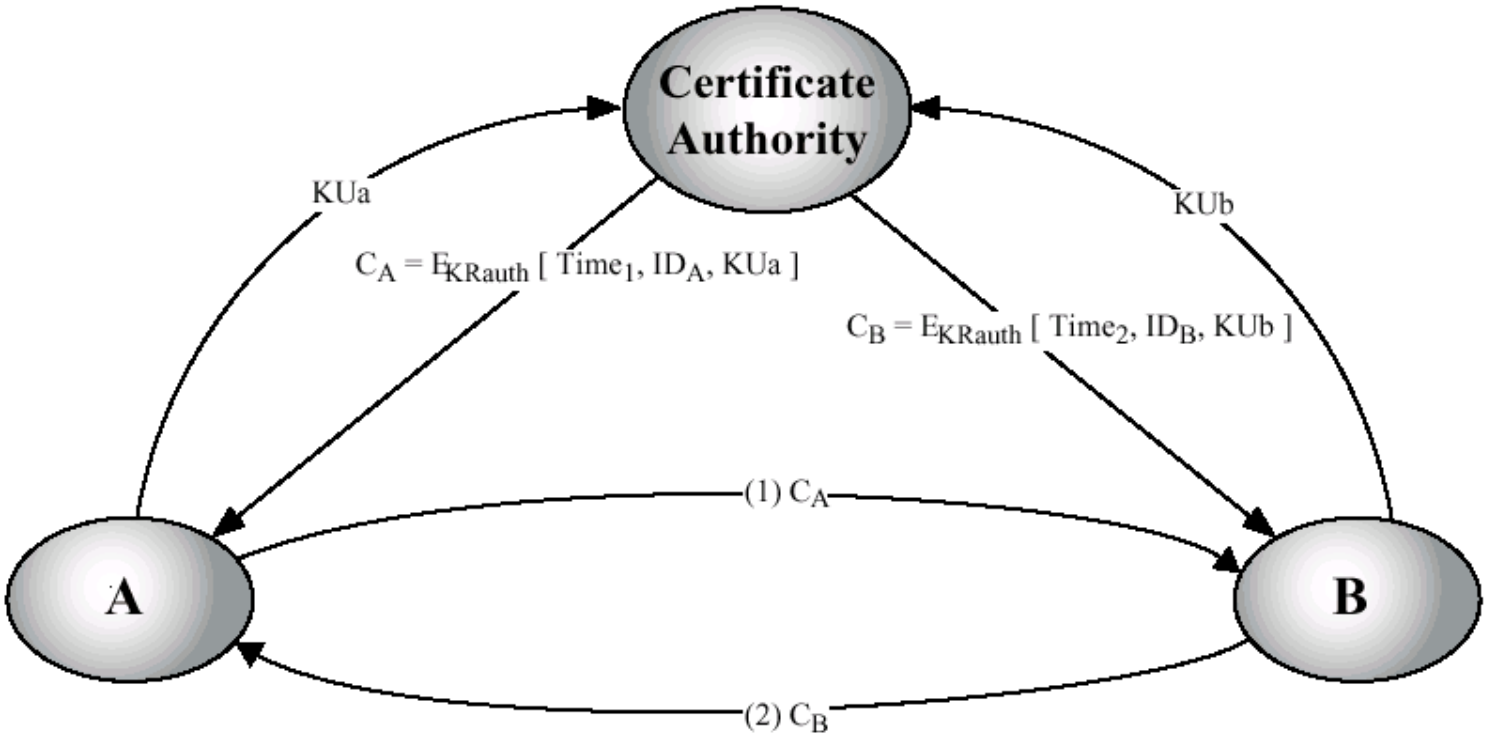
- Autoridade de chave pública (cont.)
  - Apesar de ser necessário 7 mensagens, as primeiras 4 ocorreram poucas vezes porque os intervenientes podem armazenar as chaves públicas
  - A *PKA* pode ser um ponto de engarrafamento
  - Se alguém conseguir obter a chave privada da *PKA*, esta fica comprometida.

Distribuição de Chaves Públicas (9)

- Certificados de chave pública (CA)
  1. Cada participante pode ler um certificado para determinar o nome e a chave pública do dono do certificado
  2. Cada participante pode verificar que um certificado foi originado na *CA* e não foi alterado
  3. Só a *CA* pode criar e actualizar certificados
- Uma chave privada comprometida é semelhante à perca de um cartão de crédito: o dono cancela o cartão, mas está em risco enquanto todas as comunicações não tiverem conhecimento do seu cancelamento
- O protocolo X.509 usa este tipo de distribuição de chaves

Distribuição de Chaves Públicas (10)

- Certificados de chave pública (cont.)



Conclusões

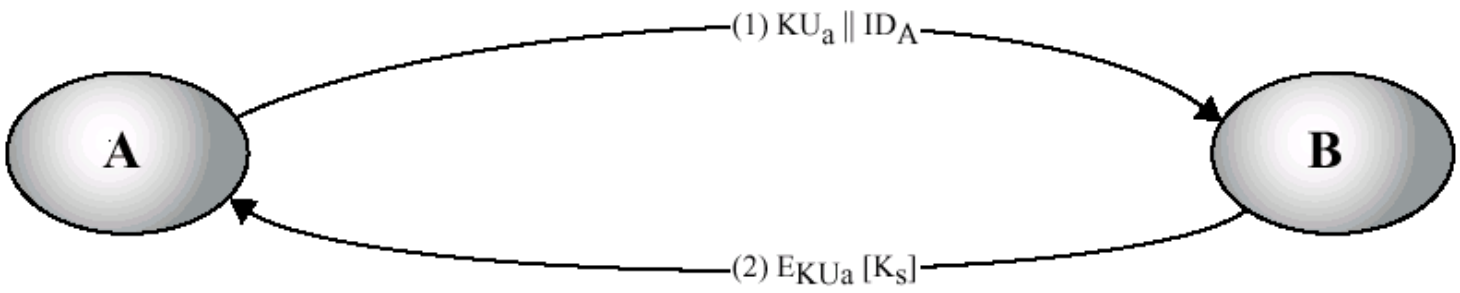
- Depois de distribuídas ou disponibilizadas as chaves, podem realizar-se comunicações seguras resistentes a ataques
- A utilização de técnicas de cifragem assimétrica são bastante pesadas, tornando pouco comum a sua utilização exclusiva
- As técnicas de cifragem assimétrica são vistas como um bom veículo de distribuição de chaves secretas utilizadas na criptografia convencional

Distribuição de Chaves Secretas (1)

- Técnicas de distribuição de chaves secretas:
  - Distribuição simples
  - Distribuição com confidencialidade e autenticidade
  - Esquema híbrido

Distribuição de Chaves Secretas (2)

- Distribuição simples
  1. *A* gera um par de chaves {KU_a, KR_a} e envia uma mensagem a *B* com KU_a e um identificador ID_A
  2. *B* gera uma chave secreta K_s e envia a *A* cifrada com KU_a
  – Este esquema é vulnerável a ataques *Man-in-the-middle*



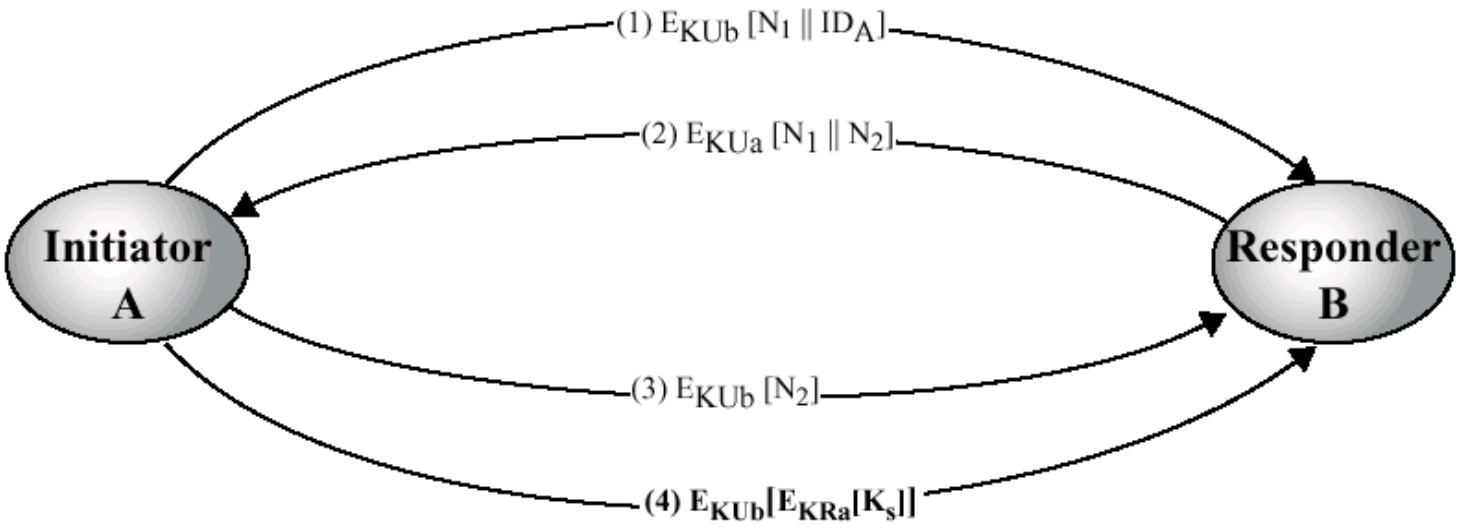
Distribuição de Chaves Secretas (3)

- Distribuição com confidencialidade e autenticidade
  - Troca de chaves públicas através de um dos esquemas anteriores

1. A cifra uma mensagem para B com KU_b contendo ID_A e N_1
2. B cifra uma mensagem para A com KU_a contendo N_1 e N_2
3. A cifra uma mensagem para B com KU_b contendo N_2
4. A escolhe K_s e envia $M=E_{KUb}[E_{KRa}[K_s]]$

Distribuição de Chaves Secretas (4)

- Distribuição com confidencialidade e autenticidade (cont.)



Distribuição de Chaves Secretas (5)

- Esquema Híbrido
  - Utilizado em mainframes da IBM
  - Mantém a utilização de 1 KDC
  - Partilha de chaves mestras com cifragem assimétrica
  - Melhorias alcançadas
    - Desempenho – em aplicações orientadas às transacções com trocas frequentes de chaves a distribuição de chaves através de cifras assimétricas torna-se pesada
    - Compatibilidade – garante a compatibilidade com sistemas de KDC existentes através de alguns ajustes nas aplicações