Cifragem Simétrica

Distribuição de Chaves

Distribuição de Chaves (1)

- Alternativas para a troca de chaves entre 2 intervenientes A e B:

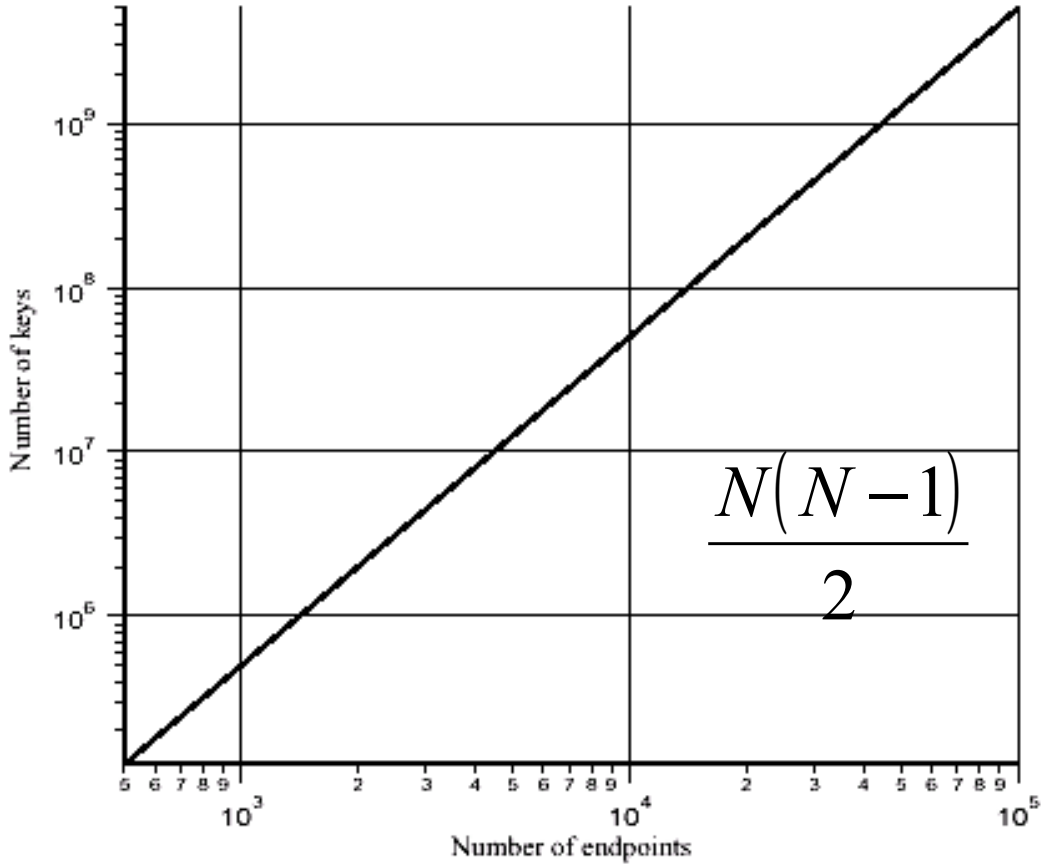
1. A escolhe a chave e entrega-a a B em mão
2. Um 3º interveniente escolhe a chave e entrega-a em mão a A e a B
3. Se A e B utilizaram recentemente uma chave comum, um deles pode escolher uma nova chave e enviá-la codificada com a anterior
4. Se A e B têm uma ligação segura para um 3º interveniente C, C pode entregar uma chave a A e a B através dos canais seguros existentes

Distribuição de Chaves (2)

1. A escolhe a chave e entrega-a a B em mão
2. Um 3º interveniente escolhe a chave e entrega-a em mão a A e a B
   - Opções razoáveis para a usar na cifragem do canal
   - Mas incomportável na cifragem ponto a ponto
     - Chaves diferentes para cada par comunicante (aplicações, equipamentos, utilizadores, ...)

Distribuição de Chaves (3)

- Número de chaves para ligações arbitrárias



Distribuição de Chaves (4)

1. Se A e B utilizaram recentemente uma chave comum, um deles pode escolher uma nova chave e enviá-la codificada com a anterior
   - Pode ser usado na cifragem do canal ou ponto-a-ponto
     - Mas se um atacante conseguir obter uma chave terá acesso a todas as chaves seguintes
     - O problema da distribuição de chaves mantém-se

Distribuição de Chaves (5)

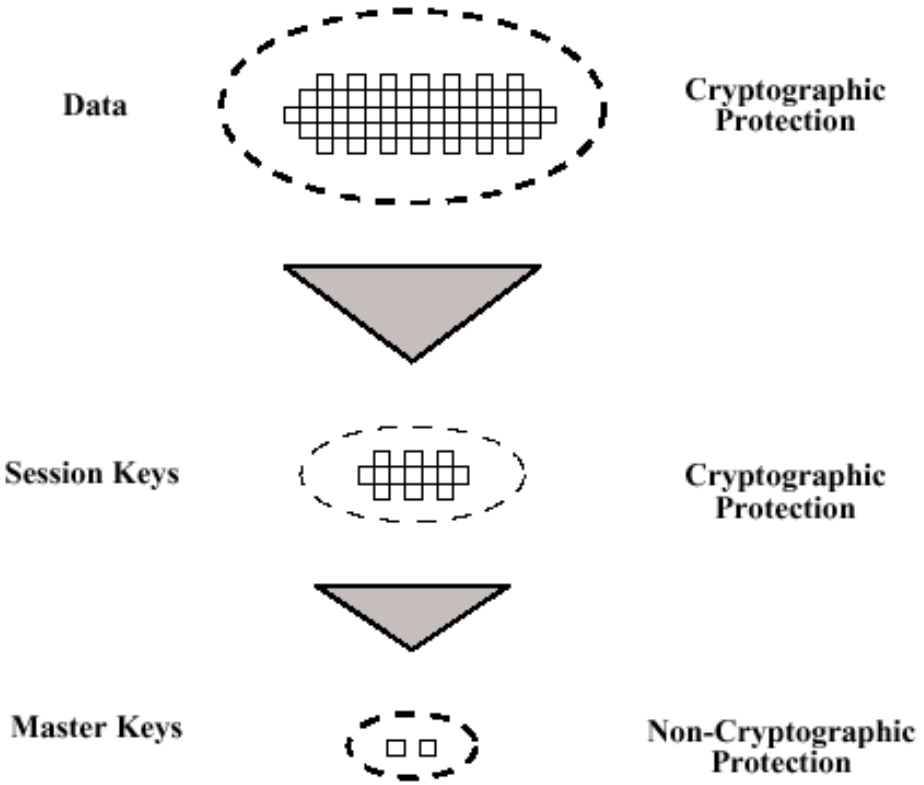
1. Se A e B têm uma ligação segura para um 3º interveniente C, C pode entregar uma chave a A e a B através dos canais seguros existentes
   - Esquema mais adoptado
   - O problema da distribuição das chaves é resolvido através de um centro de distribuição de chaves (3º interveniente)
   - Cada utilizador deve partilhar uma chave única com o centro de distribuição de chaves (KDC)

KDC (1)

- *Key Distribution Center* (KDC)
- Utilização baseada numa hierarquia de chaves com um mínimo de 2 níveis
  - *Session Key*: chave temporária usada para a comunicação entre sistemas finais. São distribuídas pelo próprio canal cifradas com a *Master Key*
  - *Master Key*: é partilhada entre o KDC e o sistema final (utilizador ou computador). Deve ser distribuída fisicamente e não cifrada.

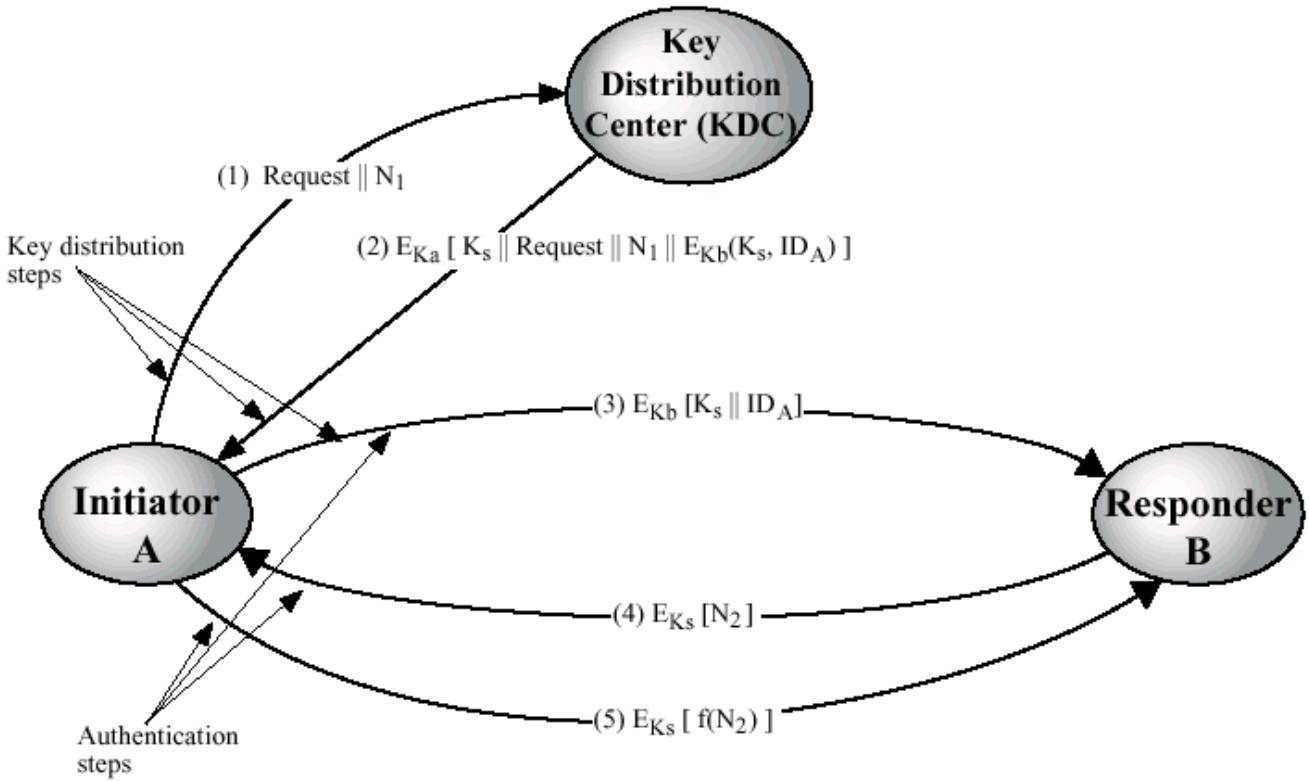
KDC (2)

- Utilização de uma hierarquia de chaves



KDC (3)

- Cenário típico de distribuição de chaves



KDC (4)

- *A* possui uma *Master Key* K_a
- *B* possui uma *Master Key* K_b
- Passos para a comunicação:

1. *A* pede uma *session key* ao KDC para comunicar com *B*. O pedido é identificado com N_1 (Um *nounce* que pode ser um nº aleatório, um *timestamp* ou um contador, desde que seja difícil de prever)
2. O KDC responde com uma mensagem cifrada com K_a. Essa mensagem contém o *nounce*, uma *session key* K_s e cifrado com K_b a K_s e ID_A para estabelecer a comunicação com B e provar a identidade de A

KDC (5)

1. *A* guarda a Ks e envia a B a informação originada pelo KDC: $E_{Kb}[K_s, ID_A]$. Neste momento a chave de sessão K_s já foi distribuída a A e a B de forma segura.
2. Usando K_s, B envia um N_2 a A
3. Usando K_s, A envia um valor $f(N_2)$ a B (por exemplo incrementar um valor a N_2)

KDC (6)

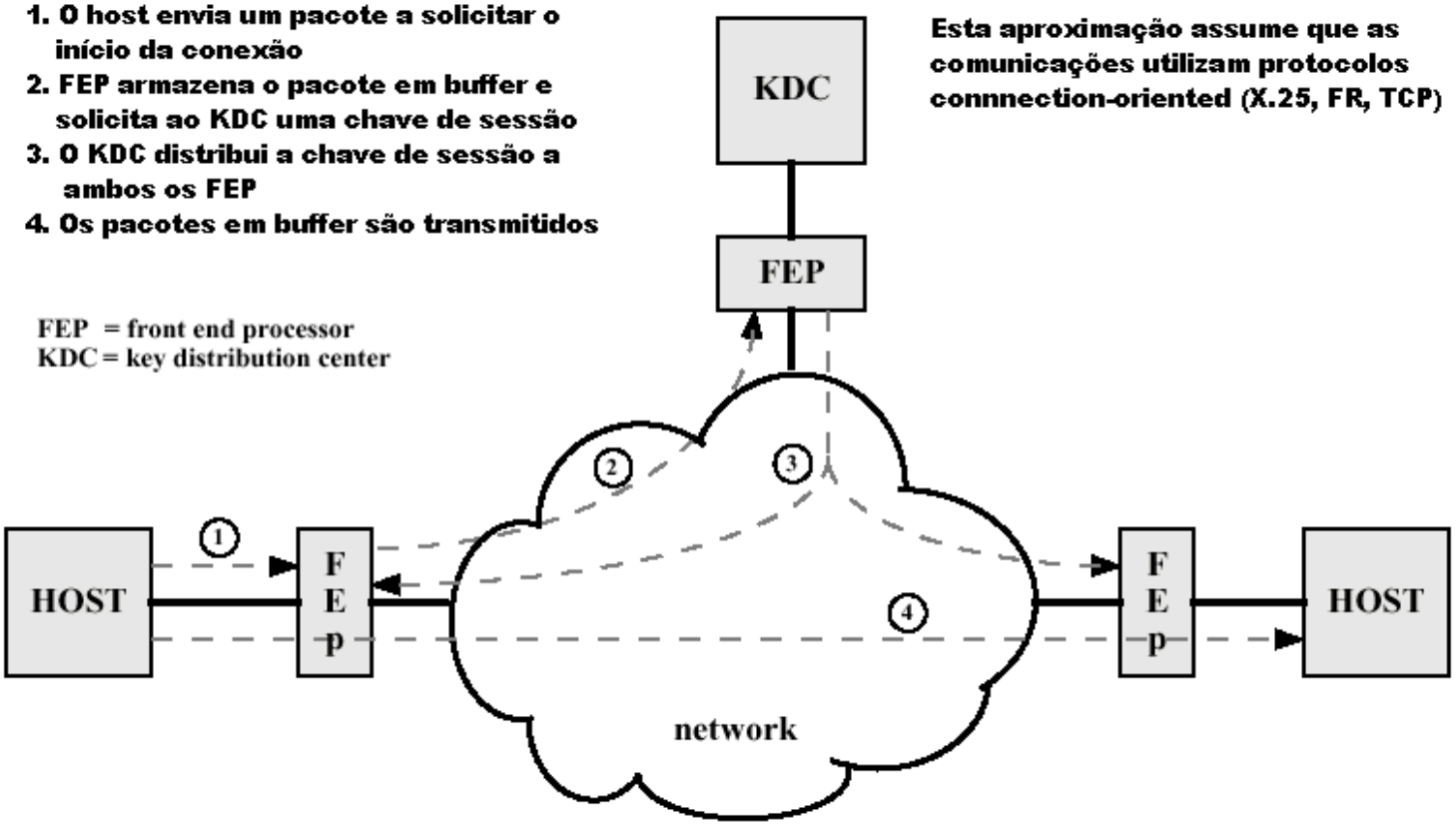
- Controle hierárquico de chaves
  - As funções de distribuição de chaves podem ser distribuídas por diversos KDC
  - Um KDC local pode ser responsável por uma LAN ou por 1 edifício
  - Quando se pretendem estabelecer comunicações não locais, os KDCs locais podem comunicar com um KDC global
  - Minimização do esforço de distribuição de chaves mestras

KDC (7)

- Duração das chaves de sessão
  - Compromisso entre Segurança (chaves frequentes) e Desempenho (chaves pouco frequentes)
  - Para protocolos *connection-oriented*
    - A escolha mais óbvia será a duração da ligação
    - Se a ligação for muito longa será prudente que a chave seja mudada periodicamente
  - Para protocolos *connection-less*
    - Não há início ou fim da comunicação explícitos
    - Utilização da mesma chave durante um determinado período temporal ou durante um determinado número de transacções

KDC (8)

- Esquema de controlo de chaves transparente



KDC (9)

- Controle de chaves descentralizado
  - Cada interveniente possui uma *master key* para cada potencial receptor
  - O número de *master keys* é N(N-1)/2, o que limita este esquema a um contexto local

KDC (10)

- Controle de chaves descentralizado