9. Segurança

Tópicos a serem abordados…

- Política de segurança.
- Criptografia.
- Comunicação segura: canal seguro, autenticação, autorização, integridade, confidencialidade.
- Certificados de segurança.

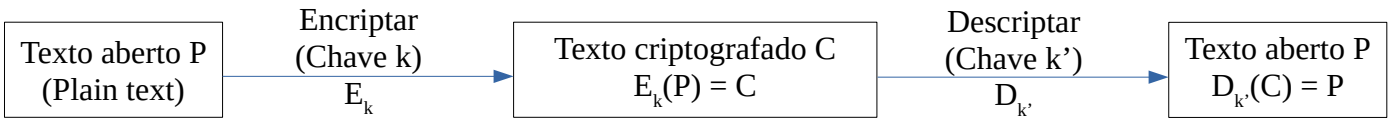
Principais mecanismos de segurança…

- Criptografia: os dados ficam ininteligíveis e inalteráveis aos intrusos.
- Autenticação: o usuário é realmente quem diz ser?
- Autorização: o usuário tem permissão para executar a ação solicitada.
- Auditoria: histórico de ações executadas e quem as executou.

A política de segurança deve se estender até, por exemplo, o banco de dados…

- Integridade referencial.
- Checked constraints.

Criptografia



$D_{k'}(E_k(P)) = P$

Na criptografia simétrica, k = k'
Na criptografia assimétrica, $k \neq k' \rightarrow$ Uma das chaves é privada, a outra é pública.

DES – Data Encryption Standard

Criptografia simétrica

Bloco de dados (64 bits) ===DES (Passo 1..16)===> Bloco criptografado (64 bits)

Passos:
$E_{k1}(P) = C1$
$E_{k2}(C1) = C2$
$E_{k3}(C2) = C3$
…
$E_{k16}(C15) = C16 = C$

Onde a chave k_i é derivada de uma chave mestra de 56 bits.

DES não é muito seguro.
DES triplo oferece uma segurança maior.

Vantagem: Rápido!

RSA – Rivest, Shamir e Adleman

Criptografia assimétrica

Base fundamental = Todo número inteiro pode ser escrito como um produto de números primos

Em RSA, a chave pública e privada é um número primo com centenas de dígitos decimais (número primo muito grande). Quebrar a chave significa encontrar esses dois números.

Desvantagem: Aproximadamente 100 a 1000 vezes mais lento que DES.
Solução: RSA para trocar chaves compartilhadas entre dois pontos de conexão e DES para cripitografar dados pelo canal de comunicação posteriormente.

MD5

h(mensagem) = número de 128 bits

h: funçao hash
número de 128 bits = resumo de mensagem

MD5 é uma função de hash para calcular um resumo de mensagem. Tipicamente utilizado para verificar a integridade dos dados ao se comparar o arquivo obtido com uma chave MD5 pública.

Canais seguros

Como tornar segura a comunicação entre dois computadores?

- Autenticar as partes comunicantes.
- Garantir a integridade e confidencialidade das mensagens.
- Controlar o acesso aos recursos: autorização.

Um canal seguro possui essas características e, portanto, protege as partes comunicantes contra:

- Interceptação (escuta) de mensagens, ou seja, proporciona garantia de confiabilidade.
- Modificação de mensagens.
- Injeção de mensagens.

Autenticação

Autenticação e integridade devem sempre estar presentes.

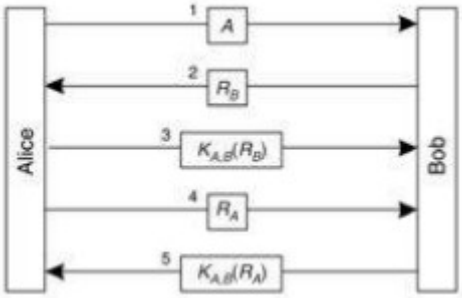
- De que vale uma mensagem autêntica se não se pode garantir que a mesma tenha sofrido alguma alteração durante a transmissão.

- De que vale uma mensagem íntegra se não se pode garantir sua autenticidade.

Uma vez que um canal de comunicação seguro tenha sido estabelecido entre dois pontos, uma chave de sessão (chave criptográfica) é utilizada para garantir a integridade e confidencialidade das mensagens. Ao término da sessão, a chave deve ser descartada de forma segura.

Autenticação baseada em uma chave secreta compartilhada

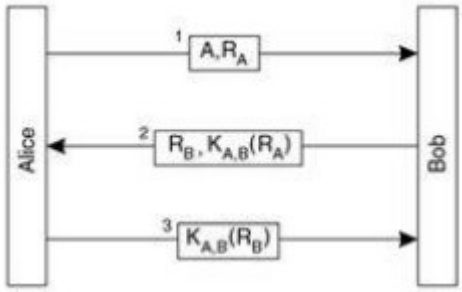
Alice ---------- $K_{A,B}$ ---------- Bob
(A) Chave compartilhada entre A e B (B)



A: Identidade de A
R_A: Desafio de A
R_B: Desafio de B

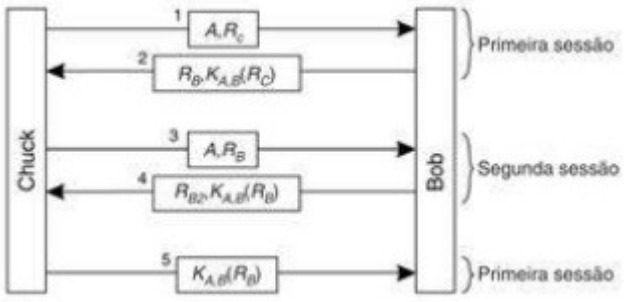
1. Eu sou Alice
2. Prove!
3. Eis a prova
4. Prove que você é Bob
5. Eis a prova

Uma possível otimização



Cuidado: Não funciona!

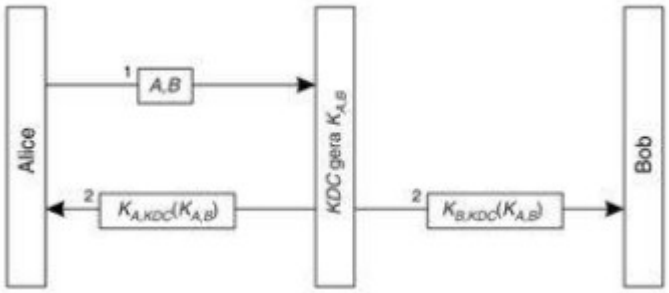
Motivo…



Desvantagem: Cada par comunicante possui sua própria chave compartilhada. Para *n* servidores, cada servidor deve manter *n* – 1 chaves.

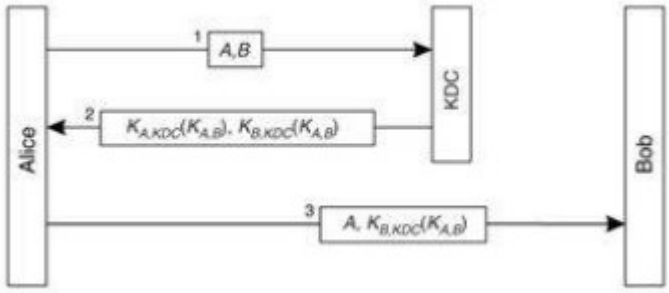
Autenticação que utiliza uma central de distribuição de chaves

A central compartilha uma chave secreta com cada um dos servidores, mas nenhum par comunicante precisa manter sua própria chave secreta. De fato, uma chave secreta é gerada para cada par comunicante sob demanda.



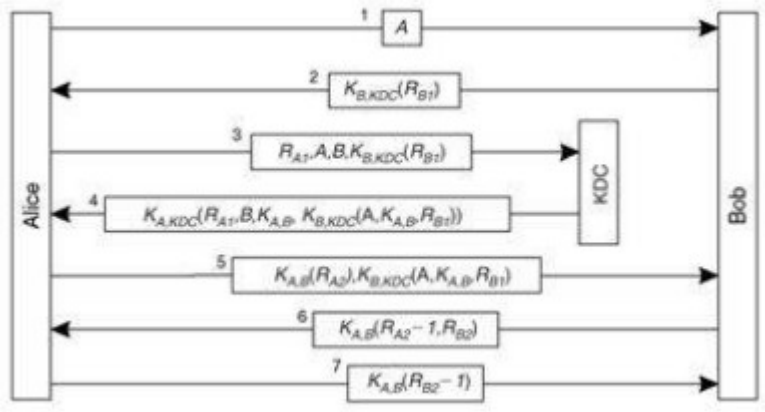
Mas há um problema, e se Bob ainda não recebeu a chave $K_{A,B}$ da central no momento em que Alice envia uma mensagem a ele?

Solução:



Alice recebe um tíquete e o envia a Bob em sua primeira mensagem.

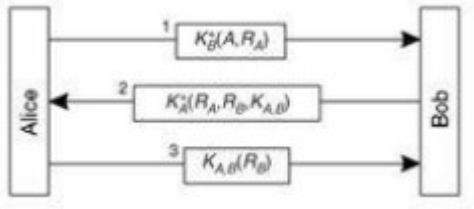
Protocolo de autenticação Needham-Schroeder



A_1, A_2, B_1, B_2: números aleatórios usados apenas uma vez (*nonce*). Servem como proteção contra re-utilização mal-intencionada de uma chave de sessão.

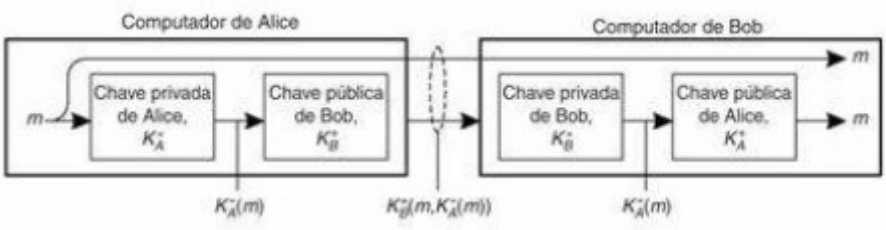
Autenticação usando criptografia de chave pública

Autenticação mútua…



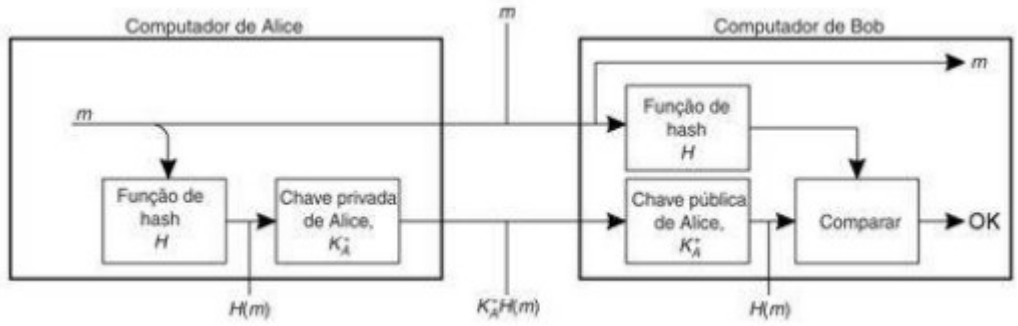
Integridade e confidencialidade de mensagens

Mensagem + Assinatura Digital => Garante a integridade e autenticidade da mensagem



Contudo, este é um processo computacionalmente custoso.

Solução: Utilizar um resumo de mensagem (por exemplo, MD5).



Por que usar uma chave de sessão temporária ao invés do próprio conjunto de chaves pública e privada?

- O uso frequente com grandes quantidades de dados torna mais fácil identificar a chave.

- Chaves de sessão limitam possíveis ataques a apenas aquela sessão.

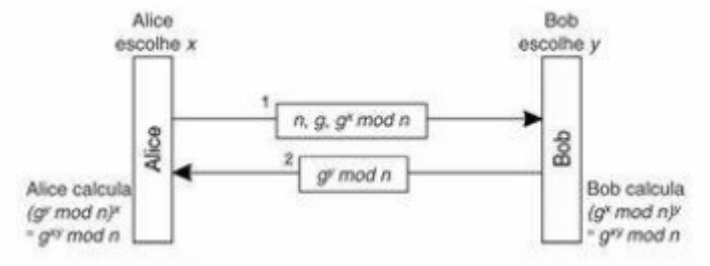
- Chaves de sessão são computacionalmente mais baratas.

E quanto ao gerenciamento de chaves? Como obter uma chave pública em um sistema criptográfico assimétrico?

- Usar uma entidade certificadora confiável (algumas já são pré-cadastradas nos browsers).

- Utilizar o protocolo de Diffie-Hellman para obter uma chave compartilhada por um canal inseguro.

Protocolo Diffie-Hellman…



x, y: números grandes aleatórios (atuam como chave privada)

1. Alice envia n, g e o resultado de g^x mod n.

É praticamente impossível para Bob calcular o valor de x.
Bob calcula $(g^x \bmod n)^y$, que é o mesmo que g^{xy} mod n. Essa será a chave compartilhada.

2. Bob envia g^y mod n.

Alice calcula $(g^y \bmod n)^x$, que é o mesmo que g^{xy} mod n. Esse é o valor da mesma chave computada por Bob.

Agora, apenas Alice e Bob tem um valor de chave em comum: uma chave secreta compartilhada por ambos.

Mesmo em um canal inseguro, caso tenha havido “escuta”, os valores de x e y não foram transmitidos na rede e, portanto, apenas Alice e Bob são capazes de computar o valor da chave.