Introdução aos Protocolos de Estabelecimento de Chave

Rafael Will Macedo de Araujo
(rwill@ime.usp.br)

DCC – IME – USP

Maio de 2011

CNPq no. 151134/2010-3

Objetivos

- Definir o que é protocolo de estabelecimento de chave

Objetivos

- Definir o que é protocolo de estabelecimento de chave
  - Como se dividem estes protocolos?
  - Quais as diferenças entre eles?

Objetivos

- Definir o que é protocolo de estabelecimento de chave
  - Como se dividem estes protocolos?
  - Quais as diferenças entre eles?
- Mostrar exemplos de protocolos

Objetivos

- Definir o que é protocolo de estabelecimento de chave
  - Como se dividem estes protocolos?
  - Quais as diferenças entre eles?
- Mostrar exemplos de protocolos
  - São necessárias muitas trocas de mensagens?
  - Permitem autenticação?

Objetivos

- Definir o que é protocolo de estabelecimento de chave
  - Como se dividem estes protocolos?
  - Quais as diferenças entre eles?
- Mostrar exemplos de protocolos
  - São necessárias muitas trocas de mensagens?
  - Permitem autenticação?
- Mostrar possíveis ataques

Roteiro

Definições

- **Protocolo:** É um algoritmo "multi-parte" (vários participantes), definido por uma sequência de passos precisos, que especificam as ações necessárias para que dois ou mais participantes possam atingir um objetivo específico. Em outras palavras, são as regras que "governam" sintaxe, semântica e sincronização da informação.

Definições

- **Participante ou entidade:** é alguém ou alguma coisa que envia, recebe ou manipula informação. Pode ser uma pessoa, um computador, etc.
  - Chamaremos de A e B.

Definições

- **Participante ou entidade:** é alguém ou alguma coisa que envia, recebe ou manipula informação. Pode ser uma pessoa, um computador, etc.
  - Chamaremos de A e B.
- **Adversário ou espião:** É uma entidade que não é nem o remetente nem o destinatário da informação que está sendo transmitida, e que tenta anular o serviço de segurança de informação estabelecido entre o remetente e o destinatário.
  - Chamaremos de C.

Definições

- **Linha (ou canal) de comunicação:** meio (linha telefônica, ondas de rádio, Internet, *Local Area Network*, etc) por onde trafegam as informações trocadas pelos participantes. Considera-se aqui que esta linha de comunicação é insegura, ou seja, existe uma ou mais pessoas má intencionadas (espiões) que podem grampear, alterar ou inserir dados, e até mesmo tentar forjar ser um participante legítimo do protocolo.

Definições

- **Autenticação de Entidade (entity authentication):** É o processo no qual um participante está seguro (através da aquisição de alguma evidência) da identidade de um segundo participante envolvido no protocolo.

Definições

- **Autenticação de Entidade (entity authentication):** É o processo no qual um participante está seguro (através da aquisição de alguma evidência) da identidade de um segundo participante envolvido no protocolo.
- **Confirmação de chave (key confirmation):** É a propriedade na qual um participante está seguro de que um segundo participante (identificado ou não) realmente tem a posse de determinada chave secreta.

Definições

- **Autenticação de chave implícita (implicit key authentication):** É a propriedade na qual um participante está seguro que nenhum outro participante, além de um segundo participante especificamente identificado, pode ter acesso a determinada chave secreta.

Definições

- **Autenticação de chave implícita (implicit key authentication):** É a propriedade na qual um participante está seguro que nenhum outro participante, além de um segundo participante especificamente identificado, pode ter acesso a determinada chave secreta.
- **Autenticação de chave explícita (explicit key authentication):** É a propriedade obtida quando é possível ter autenticação de chave implícita e confirmação de chave.

Estabelecimento de Chave (*Key Establishment*)

- É o processo ou protocolo no qual um **segredo compartilhado** torna-se disponível para dois ou mais participantes, para posterior uso criptográfico.
- Divide-se em dois subgrupos: transporte de chave (*key transport*) e acordo de chave (*key agreement*).

Motivação

- Problema de distribuição de chaves secretas.
  - Como Alice e Beto podem se comunicar de forma segura, sem a necessidade de um encontro para combinar uma chave secreta?

Motivação

- Problema de distribuição de chaves secretas.
  - Como Alice e Beto podem se comunicar de forma segura, sem a necessidade de um encontro para combinar uma chave secreta?
- Comprometimento de chaves secretas utilizadas por um longo período de tempo (*long-term key*), ou para troca de muitas mensagens.
  - É desejável que a troca de chaves secretas seja frequente (*key freshness*).

Problema do logaritmo discreto

- Sejam:
  - G: grupo cíclico finito (por exemplo $\mathbb{Z}_p^*$)
  - g: gerador de G
  - p: número primo (grande)

Problema do logaritmo discreto

- Sejam:
  - G: grupo cíclico finito (por exemplo $\mathbb{Z}_p^*$)
  - g: gerador de G
  - p: número primo (grande)
- Problema do Logaritmo Discreto (DLP):
  - Dados p, g e g^s mod p, encontrar s

Problema do logaritmo discreto

- Sejam:
  - G: grupo cíclico finito (por exemplo $\mathbb{Z}_p^*$)
  - g: gerador de G
  - p: número primo (grande)
- Problema do Logaritmo Discreto (DLP):
  - Dados p, g e g^s mod p, encontrar s
- Não se conhece um algoritmo capaz de encontrar s em tempo polinomial.

Roteiro

Acordo de Chave (*Key Agreement*)

- Protocolo ou mecanismo de estabelecimento de chave no qual dois ou mais participantes acordam uma chave secreta de maneira que ambos influenciam em seu resultado.

Acordo de Chave (*Key Agreement*)

- Protocolo ou mecanismo de estabelecimento de chave no qual dois ou mais participantes acordam uma chave secreta de maneira que ambos influenciam em seu resultado.
  - Nenhum participante pode controlar qual será o valor da chave secreta.

Acordo de Chave (*Key Agreement*)

- Protocolo ou mecanismo de estabelecimento de chave no qual dois ou mais participantes acordam uma chave secreta de maneira que ambos influenciam em seu resultado.
  - Nenhum participante pode controlar qual será o valor da chave secreta.
- Cada participante inicialmente contribui com uma "informação" que será utilizada pelos outros participantes para que posteriormente, todos possam calcular a chave. Todos os participantes devem chegar à mesma chave secreta K.

Acordo de Chave (*Key Agreement*)

- Protocolo ou mecanismo de estabelecimento de chave no qual dois ou mais participantes acordam uma chave secreta de maneira que ambos influenciam em seu resultado.
  - Nenhum participante pode controlar qual será o valor da chave secreta.
- Cada participante inicialmente contribui com uma "informação" que será utilizada pelos outros participantes para que posteriormente, todos possam calcular a chave. Todos os participantes devem chegar à mesma chave secreta K.
- Deseja-se que um espião não deva ser capaz de descobrir (calcular) a chave acordada pelos participantes do protocolo.

Alguns protocolos de acordo de chave baseados em técnicas assimétricas

Protocolo	**Autent. de chave**	**Autent. de entidade**	**Msgs. trocadas**
Diffie-Hellman	nenhuma	nenhuma	2
Acordo de chave ElGamal	unilateral	nenhuma	1
STS	mútua/explícita	mútua	3

Acordo de chave Diffie-Hellman (1976)

- Foi a primeira solução prática para o problema de distribuição de chaves, permitindo que dois participantes, que nunca se encontraram antes, pudessem compartilhar uma chave secreta através de trocas de mensagens em um canal de comunicação aberto.
- A segurança da chave secreta está na intratabilidade do problema do logaritmo discreto.

Acordo de chave Diffie-Hellman (1976)

Resumo: A e B enviam uma mensagem, cada um, em um canal público.
Resultado: Segredo compartilhado K conhecido por ambos os participantes A e B.

- Escolhe-se um primo p tal que a computação do problema do logaritmo discreto módulo p seja inviável, e um gerador g de $\mathbb{Z}_p^*$ (tal que $2 \leq g \leq p-2$). Tanto p quanto g são tornados públicos.
- A deve escolher um inteiro aleatório x, tal que $1 \leq x \leq p-2$. x é o segredo de A.
- B deve escolher um inteiro aleatório y, tal que $1 \leq y \leq p-2$. y é o segredo de B.

Acordo de chave Diffie-Hellman (1976)

1. $A \rightarrow$B:	g^x mod p
2. $B \rightarrow$A:	g^y mod p

- A recebeu $g^y \bmod p$ de B. Ele então calcula $(g^y)^x \bmod p$.
- B recebeu $g^x \bmod p$ de A. Ele então calcula $(g^x)^y \bmod p$.

Tem-se que: $(g^y)^x \bmod p = (g^x)^y \bmod p = g^{xy} \bmod p = K$.

Ataque do homem do meio (*man-in-the-middle*)

- Como não há autenticação, um espião C pode se passar por um participante legítimo do protocolo, sem que os outros desconfiem de sua verdadeira identidade.

1.	$A \rightarrow$C:	$g^x \bmod p$
2.	$C \rightarrow$A:	$g^z \bmod p$
3.	$C \rightarrow$B:	$g^z \bmod p$
4.	$B \rightarrow$C:	$g^y \bmod p$

$$K_{AC} = g^{xz} \bmod p$$
$$K_{BC} = g^{yz} \bmod p$$

$$A \Leftrightarrow K_{AC} \Leftrightarrow C \Leftrightarrow K_{BC} \Leftrightarrow B$$

Acordo de chave ElGamal (*half-certified Diffie-Hellman*)

Resumo: A envia para B uma única mensagem, em um canal público.
Resultado: Segredo compartilhado K conhecido por ambos os participantes A e B

- O participante B escolhe um primo p e um gerador g de $\mathbb{Z}_p^*$.
- B escolhe um inteiro aleatório b, $1 \leq b \leq p-2$, e calcula g^b mod p.
- B divulga sua chave pública (p, g, g^b), e guarda sua chave secreta b.
- A escolhe um inteiro aleatório x, $1 \leq x \leq p-2$. x é o segredo de A.

Acordo de chave ElGamal (*half-certified Diffie-Hellman*)

1. $A \rightarrow$B: $g^x \bmod p$

- A tem acesso a $g^b \bmod p$ (chave pública de B), então A calcula $(g^b)^x \bmod p = K$.
- B recebe $g^x \bmod p$ de A. B calcula $(g^x)^b \bmod p = K$.
- Ambos chegam à mesma chave secreta K.

Station-to-Station (STS)

Resumo: A e B trocam 3 mensagens em um canal público.
Resultado: Acordo de chave, autenticação de entidade mútua, autenticação de chave explícita.

- Sejam $S_A(m)$ e $S_B(m)$ assinaturas de A e B respectivamente, sobre uma mensagem m.
- Escolhe-se um primo p, e um gerador g de $\mathbb{Z}_p^*$, $2 \leq g \leq p-2$.
- Assumimos que cada participante tem cópias autênticas das chaves públicas das assinaturas dos outros participantes.

Station-to-Station (STS)

- A escolhe um inteiro aleatório x, tal que $1 \leq x \leq p-2$. x é o segredo de A.
- B escolhe um inteiro aleatório y, tal que $1 \leq y \leq p-2$. y é o segredo de B.

Station-to-Station (STS)

- A escolhe um inteiro aleatório x, tal que $1 \leq x \leq p-2$. x é o segredo de A.
- B escolhe um inteiro aleatório y, tal que $1 \leq y \leq p-2$. y é o segredo de B.

1. $A \rightarrow$B:	$g^x \bmod p$
2. $B \rightarrow$A:	$g^y \bmod p, \left\{\{g^y, g^x\}_{S_B}\right\}_k$
3. $A \rightarrow$B:	$\left\{\{g^x, g^y\}_{S_A}\right\}_k$

A chave secreta k é calculada por B na mensagem (2) e por A na mensagem (3).

$$k = g^{xy} \bmod p.$$

Roteiro

Transporte de Chave (*Key Transport*)

- Protocolo ou mecanismo no qual um dos participantes cria, ou outro obtem, uma chave secreta, e transfere para outros participantes de maneira segura.

Alguns protocolos de transporte de chave baseados em criptografia simétrica

Protocolo	**Tipo de servidor**	**Mensagens trocadas**
AKEP2	nenhum	3
Shamir's no-key protocol	nenhum	3
Kerberos	KDC	4
Needham-Schroeder	KDC	5

Authenticated Key Exchange Protocol 2 (AKEP2)

Resumo: A e B trocam 3 mensagens para derivar a chave de sessão W.
Resultado: Autenticação de entidade mútua, e autenticação de chave implícita de W.

- A e B compartilham duas chaves simétricas K e K', distintas. h_K é uma função de hash com chave, utilizada para autenticação de entidade. $h'_{K'}$ é uma função de hash com chave ou uma permutação pseudo-aleatória, utilizada para derivação da chave de sessão W.

Authenticated Key Exchange Protocol 2 (AKEP2)

Resumo: A e B trocam 3 mensagens para derivar a chave de sessão W.
Resultado: Autenticação de entidade mútua, e autenticação de chave implícita de W.

- A e B compartilham duas chaves simétricas K e K', distintas. h_K é uma função de hash com chave, utilizada para autenticação de entidade. $h'_{K'}$ é uma função de hash com chave ou uma permutação pseudo-aleatória, utilizada para derivação da chave de sessão W.

Seja $T = (B, A, r_A, r_B)$.

1.	$A \rightarrow$B:	r_A
2.	$B \rightarrow$A:	T, $\{T\}_{h_K}$
3.	$A \rightarrow$B:	(A, r_B), $\{A, r_B\}_{h_K}$

$W = \{r_B\}_{h'_{K'}}$

Shamir's no-key Protocol

Resumo: A e B trocam 3 mensagens em um canal público.
Resultado: A chave secreta K é transferida de forma segura, mas não há autenticação.

- Escolhe-se um primo p tal que a computação do problema do logaritmo discreto módulo p seja inviável. O valor de p é tornado público.
- A e B escolhem respectivamente dois números aleatórios a e b, tais que $1 \leq a, b \leq p-2$, e ambos coprimos a $p-1$. Calcular também a^{-1} e b^{-1} mod $p-1$.

Shamir's no-key Protocol

Resumo: A e B trocam 3 mensagens em um canal público.
Resultado: A chave secreta K é transferida de forma segura, mas não há autenticação.

- Escolhe-se um primo p tal que a computação do problema do logaritmo discreto módulo p seja inviável. O valor de p é tornado público.
- A e B escolhem respectivamente dois números aleatórios a e b, tais que $1 \leq a, b \leq p-2$, e ambos coprimos a $p-1$. Calcular também a^{-1} e b^{-1} mod $p-1$.

1.	$A \rightarrow$B:	$K^a \bmod p$
2.	$B \rightarrow$A:	$(K^a)^b \bmod p$
3.	$A \rightarrow$B:	$(K^{ab})^{a^{-1}} \bmod p$

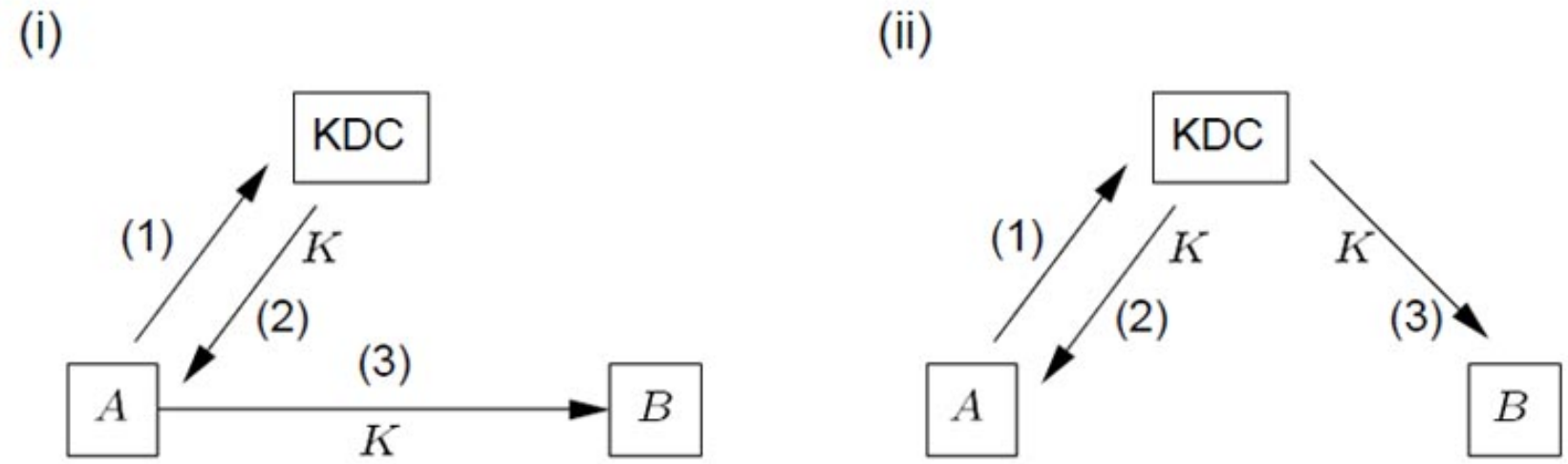
B pode então calcular $(K^b)^{b^{-1}}$ mod p, e assim obter a chave secreta compartilhada K.

Protocolos de Transporte de Chave baseados em Servidor

- Envolvem dois participantes, A e B, que desejam se comunicar, e um servidor confiável T, que compartilha uma chave secreta (*long-term secret key*) com cada participante *a priori*.
- O servidor pode ter o papel de um centro de distribuição de chave (*key distribution center* - KDC), ou de um centro de "tradução" de chave (*key translation center* - KTC).

Diagrama simplificado (KDC)

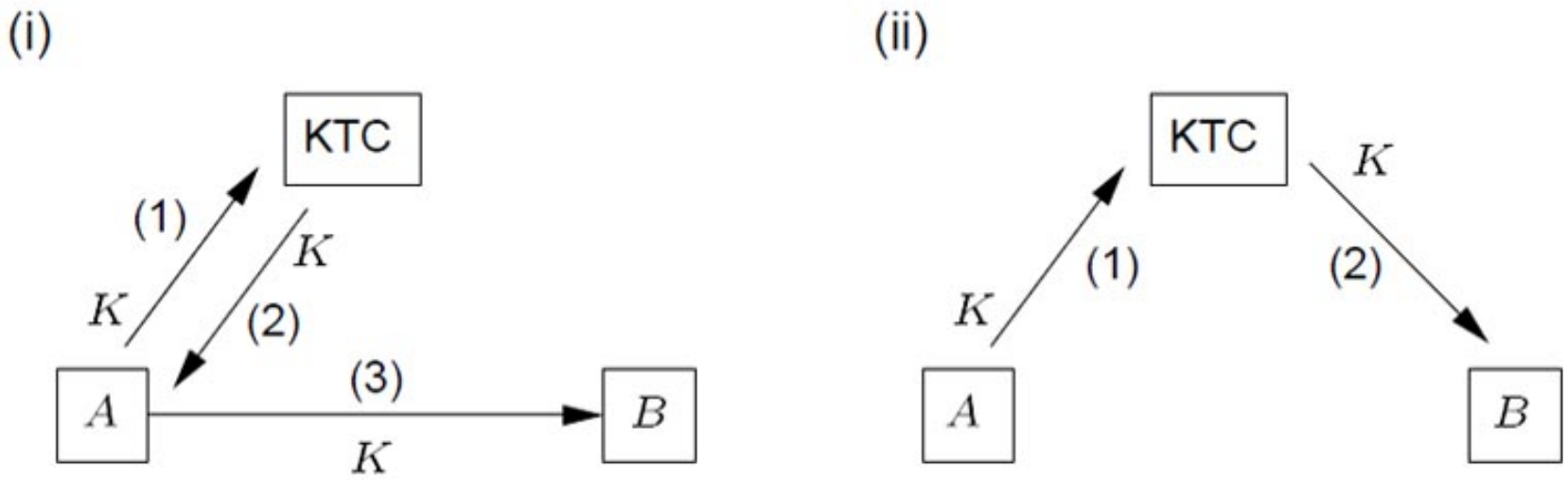
Key distribution center (KDC)



Objetivo: Fornecer uma chave de sessão para os participantes.

Diagrama simplificado (KTC)

Key translation center (KTC)



Objetivo: Tornar uma chave escolhida por um participante (suponha A) disponível para outro participante (suponha B), re-criptografando-a com a chave compartilhada entre o servidor T e o participante B.

Basic Kerberos authentication protocol

Resumo: A interage com o servidor T e o participante B.
Resultado: Autenticação de entidade de A para B.
Outras definições:

- N_A é um NONCE (*number used once*) escolhido por A.
- T_A é um *timestamp* do relógio de A.
- K_{AB} é a chave de sessão escolhida por T, que será compartilhada por A e B.
- L indica o período de validade ("*lifetime*").

Itens opcionais estão marcados com asterisco (*).

Basic Kerberos authentication protocol

- A e B compartilham respectivamente as chaves K_{AT} e K_{BT} com o servidor T.

Considere:
$ticket_B = \{K_{AB}, A, L\}_{K_{BT}}$, e $authenticator = \{A, T_A, A^*_{subkey}\}_{K_{AB}}$.

1.	$A \rightarrow$T:	A, B, N_A
2.	$T \rightarrow$A:	$\text{ticket}_B, \{K_{AB}, N_A, L, B\}_{K_{AT}}$
3.	$A \rightarrow$B:	$\text{ticket}_B, authenticator$
4.	$B \rightarrow$A:	$\{T_A, B^*_{subkey}\}_{K_{AB}}$

Os parâmetros opcionais A^*_{subkey} e B^*_{subkey} podem ser utilizados para transferência de uma chave secreta (diferente de K_{AB}) de A para B ou vice-versa, ou na computação de uma chave secreta combinada, através de alguma função $f(A_{subkey}, B_{subkey})$.

Protocolo Needham-Schroeder (1978)

Resumo: A interage com o servidor T e o participante B.
Resultado: Autenticação de entidade (A com B); estabelecimento de chave com confirmação de chave.

- A e B compartilham respectivamente as chaves K_{AT} e K_{BT} com o servidor T.

Protocolo Needham-Schroeder (1978)

Resumo: A interage com o servidor T e o participante B.
Resultado: Autenticação de entidade (A com B); estabelecimento de chave com confirmação de chave.

- A e B compartilham respectivamente as chaves K_{AT} e K_{BT} com o servidor T.

1.	$A \rightarrow$T:	A, B, N_A
2.	$T \rightarrow$A:	$\left\{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BT}}\right\}_{K_{AT}}$
3.	$A \rightarrow$B:	$\{K_{AB}, A\}_{K_{BT}}$
4.	$B \rightarrow$A:	$\{N_B\}_{K_{AB}}$
5.	$A \rightarrow$B:	$\{N_B - 1\}_{K_{AB}}$

Protocolo Needham-Schroeder (1978)

- Não existe um parâmetro indicando o período de validade da chave de sessão K_{AB}, como no Kerberos.
- A mensagem (3), que corresponde ao ticket do Kerberos, é criptografada duas vezes na mensagem (2) (desnecessário).
- O participante B não tem como verificar se a chave K_{AB} é recente. Em 1981, Denning e Sacco mostraram que é possível personificar A para B utilizando-se desse fato.

Protocolo Needham-Schroeder (1978)

- Um espião C pode armazenar mensagens antigas, criptografadas com chaves de sessão utilizadas anteriormente. Se uma dessas chaves de sessão (suponha K'_{AB}) for comprometida, C pode utilizar as mensagens trocadas com esta chave para personificar A.

1.	$A \rightarrow$T:	A, B, N_A
2.	$T \rightarrow$A:	$\left\{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BT}}\right\}_{K_{AT}}$
3.	$C \rightarrow$B:	$\{K'_{AB}, A\}_{K_{BT}}$
4.	$B \rightarrow$C:	$\{N_B\}_{K'_{AB}}$
5.	$C \rightarrow$B:	$\{N_B - 1\}_{K'_{AB}}$

"B acredita que está conversando com A, mas na verdade está conversando com C".

Roteiro

Tipos de ataques

- **Espionagem (eavesdropping):** O adversário captura informações enviadas pelo protocolo.
  - Muitos ataques sofisticados incluem a espionagem de execuções do protocolo como parte essencial.

Tipos de ataques

- **Negação de serviço (Denial of Service - DoS):** O adversário tenta impedir os usuários legítimos de completar o protocolo.
  - Muito difícil de prevenir.

Tipos de ataques

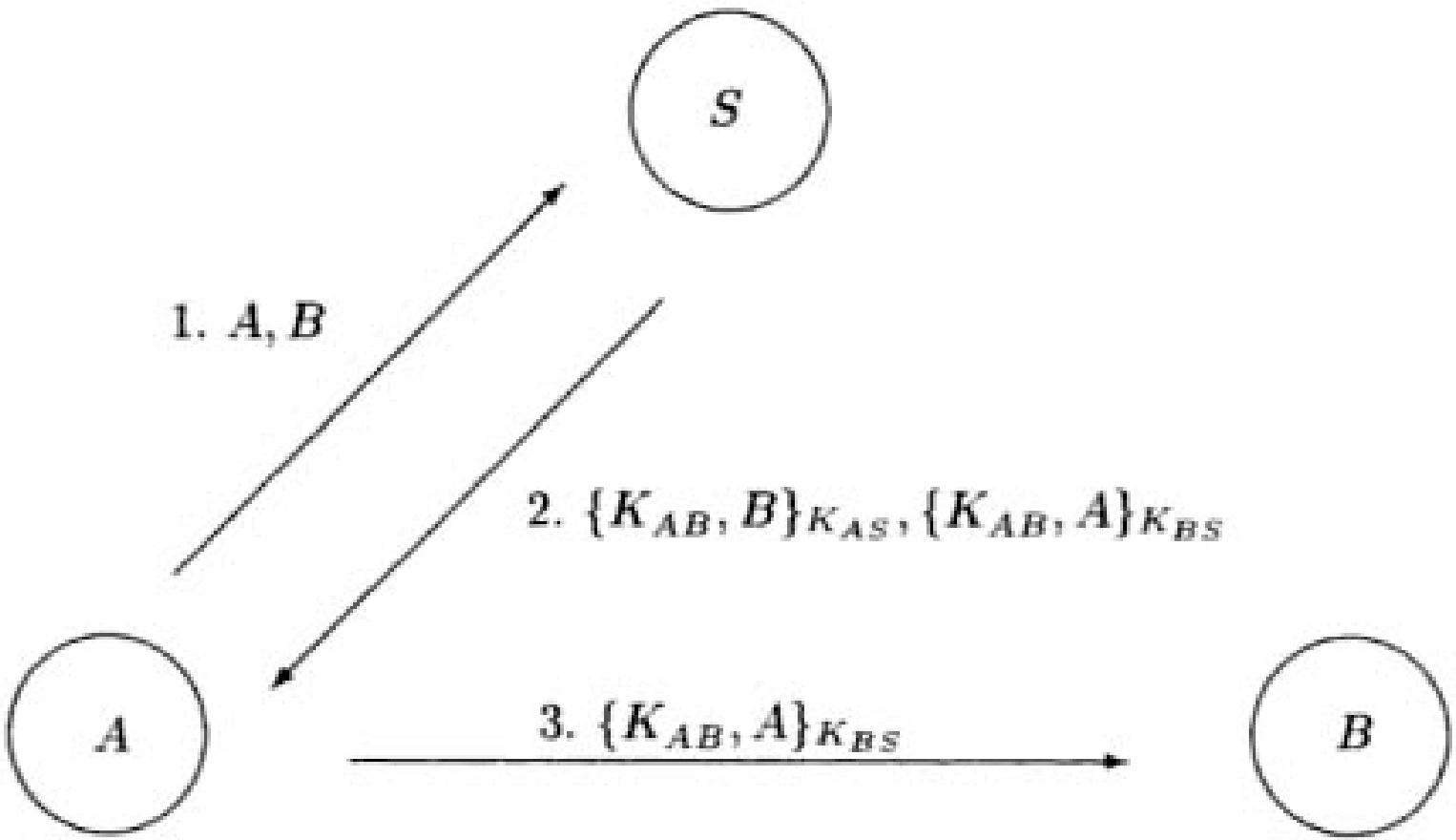
- **Criptoanálise:** O adversário ganha alguma vantagem útil do protocolo para ajudar na criptoanálise.
  - Mesmo sabendo que os algoritmos criptográficos utilizados são considerados imunes à criptoanálise, deve se levar em consideração se a chave secreta utilizada é fraca.

Tipos de ataques

- **Replay:** O adversário grava informações enviadas durante uma execução do protocolo, e depois as reenvia para o mesmo (ou outro) participante, em uma futura execução do protocolo.

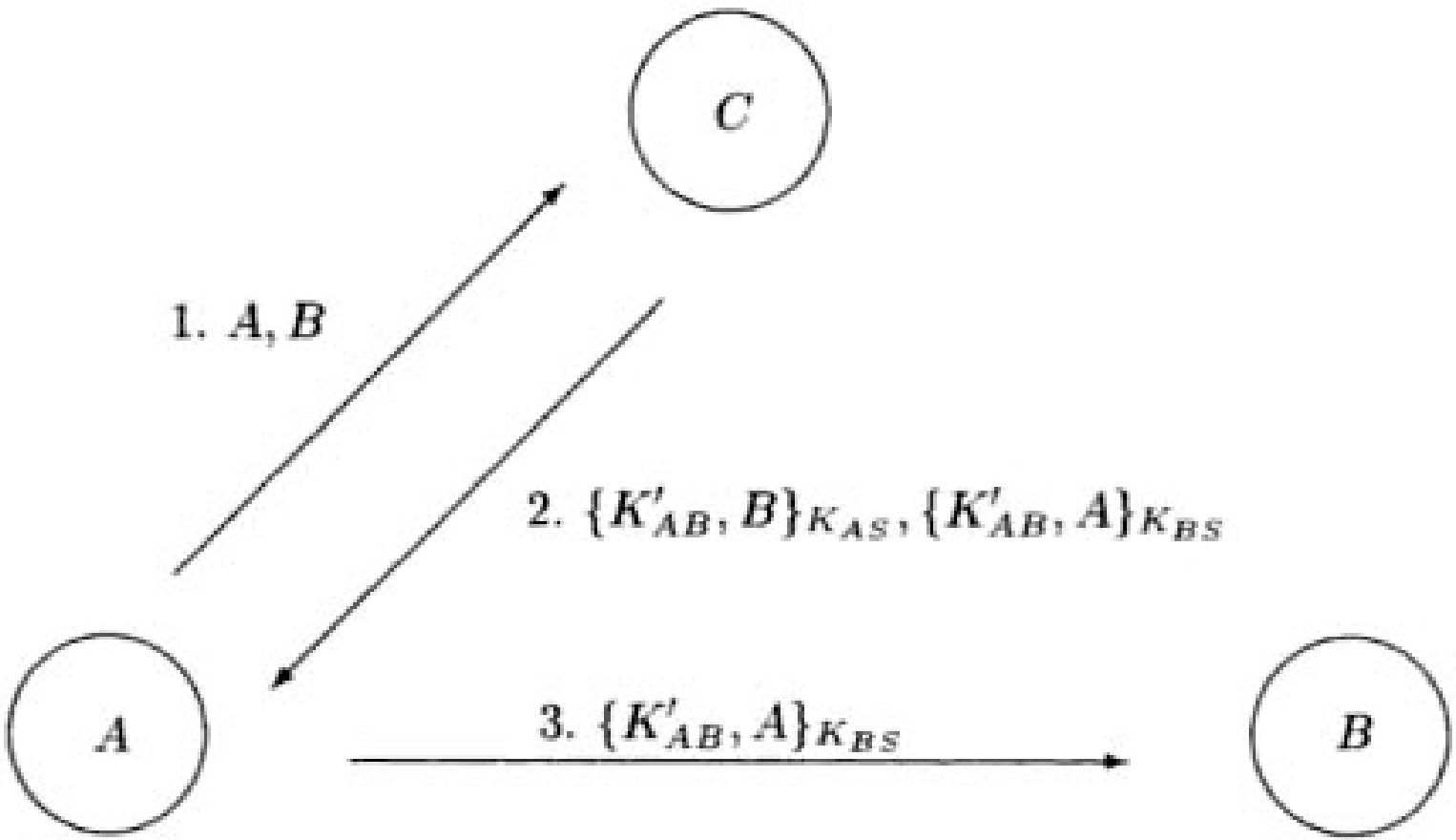
Tipos de ataques

- **Replay:** O adversário grava informações enviadas durante uma execução do protocolo, e depois as reenvia para o mesmo (ou outro) participante, em uma futura execução do protocolo.



Tipos de ataques

- **Replay:** O adversário grava informações enviadas durante uma execução do protocolo, e depois as reenvia para o mesmo (ou outro) participante, em uma futura execução do protocolo.



Tipos de ataques

- **Reflexão(reflection):** É um caso especial do ataque por *replay*. O adversário envia as mensagens do protocolo de volta para o participante que as enviou.

Tipos de ataques

- **Reflexão(reflection):** É um caso especial do ataque por *replay*. O adversário envia as mensagens do protocolo de volta para o participante que as enviou.

1.	$A \rightarrow$B:	$\{N_A\}_K$
2.	$B \rightarrow$A:	$\{N_B\}_K, N_A$
3.	$A \rightarrow$B:	N_B

O objetivo do protocolo (ingênuo) acima é a autenticação mútua de A e B.

Tipos de ataques

- O adversário pode iniciar várias execuções paralelas do protocolo.

Tipos de ataques

- O adversário pode iniciar várias execuções paralelas do protocolo.

1.	$A \rightarrow$C:	$\{N_A\}_K$
1'.	$C \rightarrow$A:	$\{N_A\}_K$
2'.	$A \rightarrow$C:	$\{N'_A\}_K, N_A$
2.	$C \rightarrow$A:	$\{N'_A\}_K, N_A$
3.	$A \rightarrow$C:	N'$_A$
3'.	$C \rightarrow$A:	N'$_A$

Referências Bibliográficas

- MENEZES. Alfred J., OORSCHOT, Paul C. van, VANSTONE, Scott A. **Handbook of Applied Cryptography**. CRC Press; 1 edition. 1996.
- BOYD. Colin, MATHURIA, Anish. **Protocols for Authentication and Key Establishment**. Springer-Verlag. 2003.

Perguntas?

Obrigado!