Lista de Exercícios 2

Esta lista é para preparação para a Prova 1. Procure realizar com cuidado, pois já é parte da Prova 1.

Prazo de realização e postagem no Moodle: de 25/04/2014 à 23/05/2014

Prazo de entrega impressa: 23/05/2014 (PROVA 1)

Protocolos Criptográficos

Criptografia Simétrica e Assimétrica

1. A figura 1 seguinte ilustra o caso de um protocolo entre um terminal de caixa bancário e um banco. Leia o protocolo no material na página sobre protocolos básicos.

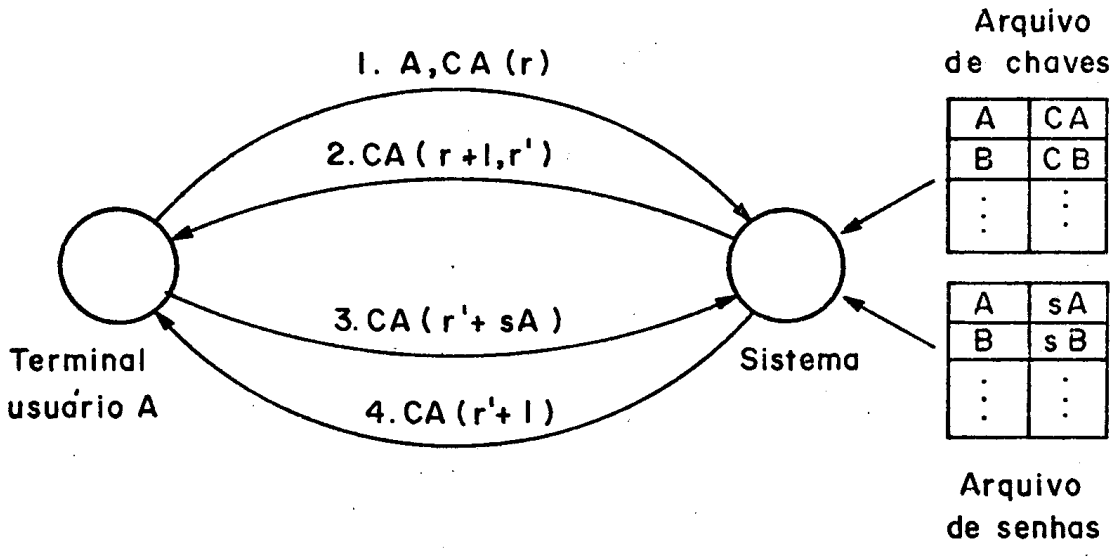


Figura 1. Um protocolo de autenticação de usuário.

O protocolo é o seguinte (figura 1):

1. O terminal envia ao sistema a identidade iA de A, juntamente com CA(r), onde r é gerado ao acaso pelo terminal.
2. O sistema, de posse de iA, determina CA, decifra CA(r) obtendo r, gera um outro valor aleatório r', envia ao terminal a mensagem CA(r+1,r').
3. O terminal decifra CA(r+1,r') obtendo r+1 (e também r'), e verifica que o resultado r+1 é um mais do que o aleatório r por ele gerado. Em seguida, o usuário envia ao sistema a mensagem CA(r'+sA) onde sA é a senha de A.

Procure responder as seguintes questões sobre um possível ataque. Procure ver os tipos de ataque citados no material sobre Autenticação de Mensagens. O que é um *nonce* ?

(a) Para que serve o número r usado no protocolo ?
Para que o Terminal T com o Usuário A autentique o sistema Banco. Assim o sistema Banco não pode se passar por outro sistema. A eliminação de r permite que um mau caráter se passar pelo sistema Banco.

(b) Para que existe o número r' usado no protocolo ?
Para que o sistema Banco autentique o Terminal T com o Usuário A. Assim, o Usuário A não pode se passar por outro usuário. A eliminação de r´ permite que um mau caráter se passar pelo Usuário A no terminal.

(c) Cite um ataque possível que pode ser evitado com o uso de r e r´.
Se r e r´são usados, isto ajuda na autenticação mútua entre as duas partes, Terminal e Sistema Banco, Um outro tipo de ataque é o conhecido por Ataque de Repetição, em que um oponente pode capturar uma mensagem , e posteriormente, caso não haja nenhuma proteção contra este tipo de ataque, reenviar a mensagem capturada, visando obter alguma vantagem, por exemplo, perante os sistema Banco.

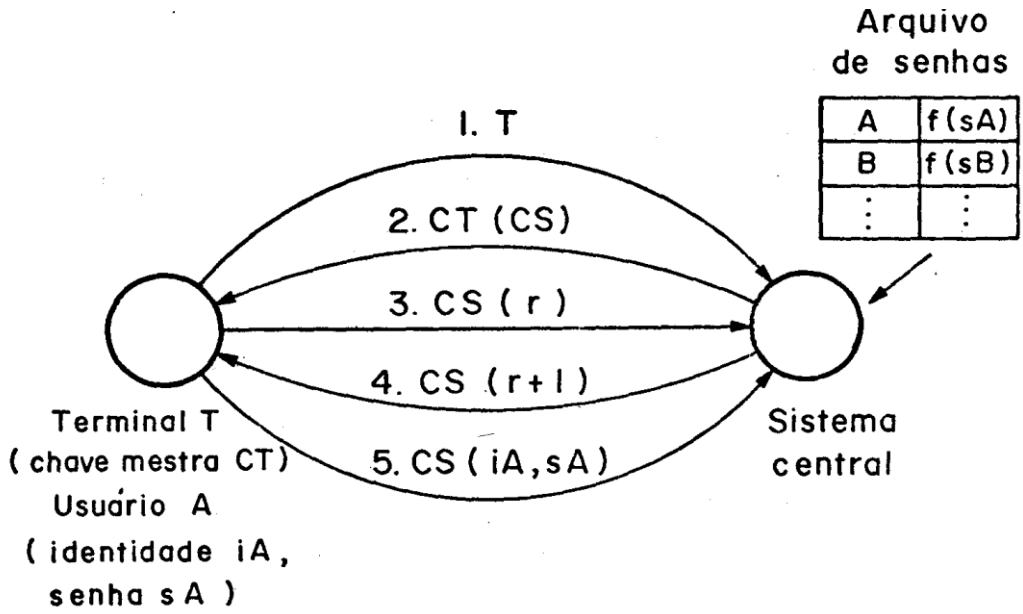
(d) Escreva, usando notação formal, o protocolo da figura 1.

1. T gera r aleatoriamente
2. T → B : IA || E_{CA} (r)
3. B decripta D_{CA} (r), B gera r´ , B calcula r+1
4. B → T : E_{CA} (r+1 || r´)
5. T decifra D_{CA} (r+1 || r´) , T obtém r´

6. T → B : E_{CA} (r´ || sA)
7. B decifra D_{CA} (r´ || sA) , obtém r´ e aS, e autentica Usuário A no seu arquivo de senhas.

---

2. Considere a figura 2 seguinte, um protocolo que mostra um procedimento de autenticação de um usuário de um terminal bancário. Suponha que um terminal bancário é uma entidade T e o sistema central (banco) uma entidade B. Considere para o terminal o par de chaves, pública e privada, (PU_T, PR_T) e para o sistema de autenticação em B, respectivamente, o par (PU_B, PR_B) de chave pública e chave privada. No protocolo da figura, a **criptografia simétrica**, com uma chave de sessão *CS* é usada no procedimento de autenticação.



Altere o protocolo acima, descrevendo formalmente suas etapas, para funcionar com criptografia de chave pública.

1. Considere que o sistema central (banco B) conheça as chaves públicas dos vários terminais *T* (PU_T). E que esses terminais T conheçam a chave pública do sistema central.

   B : PU_T *(por construção do sistema de segurança)* e (PU_B, PR_B)
   T : PU_B e (PU_T, PR_T)

2. Alguém está querendo usar o terminal T. O protocolo se inicia quando o terminal envia sua identificação *T* para o sistema central B.

   T → B : I_T (aqui, o identificador de T não está criptografado, mas se fóssemos fazer assim, usaríamos $PU_B(I_T)$, assumindo-se como acima que T conhece PU_B.

3. Pelo protocolo, o sistema central B deve enviar uma chave de sessão *CS* para o terminal *T* poder criptografar (usando criptografia simétrica com uma chave de sessão *CS*), através da chave mestra *CT*.

   B → T : *CT*(*CS*), neste caso, a chave mestra CT do terminal T criptografa a chave de sessão CS enviada pelo banco B para o terminal T.

4. Mas, para se usar criptografia de chave pública, o sistema central, agora, se utilizará da chave pública do terminal T (PU_T), enviando a chave de sessão *CS* criptografada para *T.* Com sua chave privada (PR_T), o terminal *T* decifra a chave de sessão *CS*.

   Para usar criptografia de chave pública, o banco B, agora substitui a chave CT por uma chave pública PU_T

   O uso da criptografia de chave pública, se faz aqui na etapa 4 e poderíamos ter:

   B → T : $PU_T(CS)$
   T : $PR_T(CS)$
   T : *CS*

5. Com *CS*, o terminal *T* pode cifrar os números *r* supostamente aleatórios gerados por *T* e enviá-los ao sistema central.

   T : $E_{CS}(r)$
   onde r é *nonce* gerado por T
   T → B : $E_{CS}(r)$
   B : $D_{CS}(r)$
   B : r

6. De posso do número *r*, o sistema central modifica esse número *r,* adicionando 1, cifrando-o com *CS* e enviando para *T*. O banco B envia *r+1* para T. Lembrem que os números *r* e *r+1* são usados apenas uma vez, para evitar ataques de repetição no procedimento de autenticação de um usuário do terminal *T*. Daí o termo *nonce*, em inglês, para denominar esses números.

   B : r+1
   B: $E_{CS}(r+1)$
   B → T : $E_{CS}(r+1)$
   T : $D_{CS}(r+1)$
   T : r+1

7. O terminal envia sua identificação *iA* e a senha *sA* para o sistema central poder autenticar usando o arquivo de senhas, contendo os valores *hash* das senhas dos usuários do sistema.

   O terminal T recebe o número *r+1* e assim, fica sabendo que o banco B recebeu seu número *r*, envoado anteriormente.

$T \rightarrow B : E_{CS}(I_A, SA)$,

onde I_A é o identificador de um usuário A e AS é a senha do usuário, Ambos os valores são enviados criptografados para o sistema do banco B.

---

3. Três amigos residentes em cidades distantes desejam trocar informações pela Internet de forma segura. Somente um deles, B possui um par chave pública/chave privada KR/KU . Proponha um protocolo para que os amigos possam trocar uma KS (chave simétrica) para ser utilizada pelos três na troca de mensagens sigilosas.

$$A : \text{Gera } KSa$$

$$A \rightarrow B : E_{KUb} (KSa)$$

$$B : D_{KRb} [E_{KUb} (KSa)]$$

$$C : \text{Gera } KSc$$

$$C \rightarrow B : E_{KUb} (KSc)$$

$$B : D_{KRb} [E_{KUb} (KSc)]$$

$$B : \text{Gera } KS$$

$$B \rightarrow A : E_{KSa} (KS)$$

$$B \rightarrow C : E_{KSc} (KS)$$

$$A,B,C \leftarrow E_{KS} (M) \rightarrow A,B,C$$

---

4. Suponha que para acessar a base de dados de notas da UFSC com prerrogativas de administrador, devem estar envolvidos **3** membros da comunidade acadêmica, entre professores e servidores administrativos da UFSC.
Sendo obrigatório o envolvimento de pelo menos 1 professor e de pelo menos

1 servidor. Para solucionar este problema foi definido que a senha de acesso KS, uma chave de sessão, deveria estar cifrada de forma a garantir a regra de segurança acima definida.

Defina o protocolo criptográfico para segurança e liberação da senha de acesso, sabendo que cada membro da comunidade acadêmica possui um par de chaves assimétricas. Como sugestão, lembre do significado do envelope digital, que usa criptografia simétrica para transmitir os dados cifrados e usa a criptografia de chave pública para distribuir com segurança a chave de sessão. Use a seguinte notação:

p – professores, pi – i-ésimo professor

a – servidor administrativo, ai – i-ésimo servidor administrativo

S : Gera KS, senha de acesso ao banco de dados

Para **segurança** de KS, deve-se cifrar KS com todas as combinações possíveis de servidores e professores, sempre utilizando-se a KU (chaves públicas) de pelo menos 1 servidor e 1 professor.

Para 2 professores e 1 servidor:

$$S : E_{KUpi} \{ E_{KUpi+1} [E_{KUai} (\mathbf{KS})] \} \quad e$$

$$S : E_{KUpi} \{ E_{KUpi+2} [E_{KUai} (\mathbf{KS})] \} \quad e$$

. . . . . .

$$S : E_{KUpi} \{ E_{KUp+n} [E_{KUai} (\mathbf{KS})] \}$$

Para 1 professor e 2 servidores:

$$S : E_{KUpi} \{ E_{KUai} [E_{KUai+1} (\mathbf{KS})] \} \quad e$$

. . . . . .

$$S : E_{KUpi} \{ E_{KUai} [E_{KUai+n} (\mathbf{KS})] \}$$

A **liberação** da senha de acesso somente será possível com a combinação de KR (chaves privadas) capazes de decifrar KS, ou seja, com a presença de: 2 professores e 1 servidor, ou, 1 professor e 2 servidores administrativos.

$$S : D_{KRpi} \{ D_{KRpi+1} [D_{KRai} (\mathbf{KS})] \} \quad ou$$

$S : D_{KRpi} \{ D_{KRai+1} [D_{KRai} (\mathbf{KS})] \}$ ou

. . . . . .

---

5. O protocolo seguinte ilustra o problema do "**Man-in-the-Middle Attack**". Mesmo que as chaves públicas de Alice e Bob estejam armazenadas em uma base de dados, este ataque funcionará. Explique o porquê.

Protocolos Básicos

Man-in-the-Middle Attack

$A \rightarrow B : KU_A$

$M : KU_A$; $M \rightarrow B : KU_M$

$B \rightarrow A : KU_B$

$M : KU_B$; $M \rightarrow B : KU_M$

$A \rightarrow B : E_{KU_M}(m)$ Alice pensa que tem uma KU_B

$M : E_{KU_M}(m)$; $M : D_{KU_M}(m)$; $M : m$; $M :> m'$

$M : E_{KU_B}(m')$; $M \rightarrow B : E_{KU_B}(m')$; $B : D_{KRB}(m')$; $B : m'$

$B \rightarrow A : E_{KU_M}(m'')$ Bob pensa que tem uma KU_A

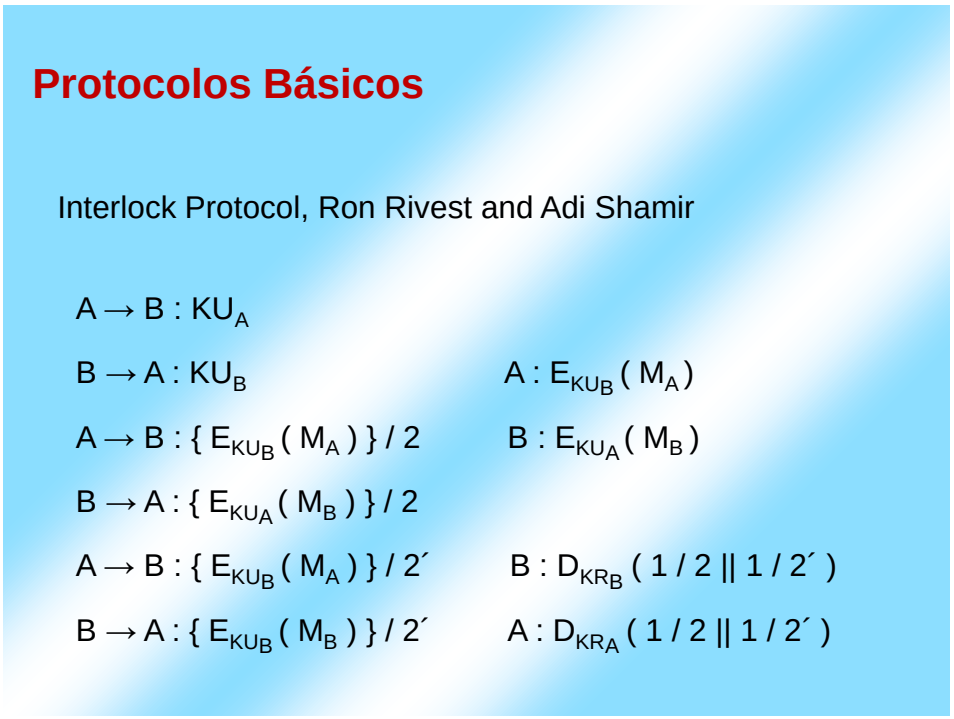
$M : E_{KU_M}(m'')$; $M : D_{KR_M}(m'')$; $M : m''$

$M : E_{KU_A}(m'')$; $M \rightarrow A : E_{KU_A}(m'')$

- Supõe que Mallory, o intruso, pode interceptar a consulta de Alice na base de dados e substituir sua própria chave-pública para Bob.
- Supõe que Mallory, o intruso, pode interceptar a consulta de Bob na base de dados e substituir sua própria chave-pública para Alice.
- Ou melhor ainda, supõe que, Mallory pode invadir a base de dados e substituir as chaves de Alice e Bob, pela chave dele.
- Então, Mallory simplesmente espera Alice e Bob se comunicarem, intercepta e modifica mensagens capturadas de forma bem sucedida.
- Este *Man-in-the-Middle Attack* funciona bem, porque Alice e Bob não tem nenhum meio para verificar que eles estão se comunicando.

- Assumindo que Mallory não causa nenhum atraso de rede notável, Alice e Bob não tem ideia que alguém situado entre eles está lendo tudo de sua supostamente comunicação secreta.

6. O protocolo seguinte, **Interlock Protocol**, foi criado por Ron Rivest, Adi Shamir (os mesmos que criaram o RSA, tem uma boa chance de frustar o *Man-in-the-Middle Attack*.



- O importante ponto aqui é que metade de mensagens não tem nenhuma utilidade sem a outra metade, ela não pode ser decifrada. Bob não pode ler qualquer parte da mensagem de Alice até a etapa (6) de concatenação de duas metades.
- Alice não pode ler qualquer parte da mensagem de Bob até a etapa (7), ou seja, até que Alice junte as duas metades e decifre com sua chave privada.
- Este protocolo **Interlock** causa um problema para Mallory. Explique porque.

Veja os slides em Protocolos Básicos sobre o Interlock Protocol:

Quando Mallory, o intruso, intercepta metade da mensagem de Alice em (3), ele não pode decriptá-la com sua chave privada e re-encriptá-la com a chave pública de Bob.

Quando Mallory, o intruso, intercepta metade da mensagem de Bob em (4), ele tem o mesmo problema.

7. O protocolo Needham-Schroeder, abaixo, pode apresentar um problema de segurança. Tente analisar e relatar qual problema de segurança você pode notar. O detalhe é sutil, mas tente verificar.

Needham-Schroeder (Chave Compartilhada)

$A \rightarrow T : ID_A \,||\, ID_B \,||\, N_A$
$T \rightarrow A : [\, E_{KA}(N_A \,||\, ID_B \,||\, K_S \;||\; E_{KB}(K_S \,||\, ID_A)) \,]$ (2)
$A \rightarrow B : E_{KB}(K_S \,||\, ID_A)$ (3)
$B \rightarrow A : E_{KS}(N_B)$
$A \rightarrow B : E_{KS}(N_B - 1)$ (5)

Que pode ser escrito também como a seguir, substituindo-se || por uma ",":

$A \rightarrow T : ID_A , ID_B , N_A$
$T \rightarrow A : [\; E_{KA}(N_A , ID_B , K_S \;,\; E_{KB}(K_S , ID_A)) \;]$ (2)
$A \rightarrow B : E_{KB}(K_S , ID_A)$ (3)
$B \rightarrow A : E_{KS}(N_B)$
$A \rightarrow B : E_{KS}(N_B - 1)$ (5)

Ou pode-se também usar esta notação como usada em **Isabelle**, onde $\{|\ \ldots\ |\}_K$ são usadas para denotar uma mensagem (...) criptografada por uma chave K.

$A \rightarrow T : ID_A , ID_B , N_A$
$T \rightarrow A : \{|\ N_A , ID_B , K_S \;,\; \{|\ K_S , ID_A\ |\}_{KB}\ |\}_{KA}$ (2)
$A \rightarrow B : \{|\ K_S , ID_A\ |\}_{KB}$ (3)

o que é mais interessante para um atacante é a comunicação entre A e B. Então, o oponente pode capturar esta mensagem $\{|\ K_S , ID_A\ |\}_{KB}$ e sem ter nenhum conhecimento do conteúdo desta mensagem, fazer a repetição, reenviando-a para B. Como resultado, B pode ser enganado a aceitar uma chave de sessão K_S velha, como se fosse recente ("fresca").

$B \rightarrow A : \{|\ N_B\ |\}_{KS}$
$A \rightarrow B : \{|\ N_B - 1\ |\}_{KS}$ (5)

Obs: Existe também o protocolo **Public-Key Needham-Schroeder**

1. $A \rightarrow B : \{|\ A, N_A\ |\}_{KUB}$
2. $B \rightarrow A : \{|\ N_B , N_A\ |\}_{KUA}$
3. $A \rightarrow B : \{|\ N_B\ |\}_{KUB}$

Neste protocolo existe um “middle-person attack” sobre o protocolo Needham-Schroeder de Chave Pública, o qual é um tanto sutil. Levou-se em torno de 15 anos para ser descoberto. E somente conseguiram detectar o possível ataque, após submeter o protocolo numa ferramenta de prova formal.

Gavim Low, um professor de Teoria da Computação da University of Oxford, mostrou que um atacante-espião pode explorar duas execuções intercaladas e interpor-se entre os pares A e B, de modo que B acredite que seu para é A, quando, ele, de fato, é o atacante-espião.

Veja a demonstração do ataque de Gavim Lowe nos slides da Palestra 2:
´´Métodos Formais Aplicados a Segurança da Informação´´
situados na página na Aula 9.

O protocolo Needham - Schroder Chave Pública é um sistema de autenticação para garantir a transmissão de dados através de redes. Gavin Lowe encontrou uma fraqueza neste protocolo e por isso foi redesenhado e agora é comumente conhecido como o Protocolo de Needham - Schroeder -Lowe .

Finalidade: O protocolo Needham Schroder Public Key usa criptografia de chave pública para permitir que dois pontos de entrar em uma conexão segura para provar a sua identidade. Um servidor de chaves distribui uma chave pública diferente para os participantes , em seguida, cada parte deve provar que detém a chave privada correspondente para decodificar qualquer mensagem criptografada pela chave pública correspondente , mostrando que eles são a parte que eles afirmam ser .

Ataque: Gavin Lowe detectou que o sistema Needham - Schroder era vulnerável a "man in the middle" ataques. Isso significa que alguém pode ouvir o processo de autenticação , passando -se “fora” como A para B e de B para A , capturando , reordenando e fazendo o encaminhamento de cada mensagem no diálogo . Isso permite que o impostor possa intervir e se disfarçar de uma ou ambas as partes envolvidas na troca.

Veja explicação, também em http://orium.pw/univ/mei/ssrc/2.5.2-Key-distribution-protocols-P2.pdf