Um Protocolo Criptográfico para Comunicação Anônima Segura em Grupo

Paulo Sérgio Ribeiro, Ricardo Felipe Custódio
Curso de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Catarina
88040-900 Florianópolis - SC
{*paulosr@telesc.com.br,custodio@inf.ufsc.br*}

Resumo: *A criptografia simétrica provê alguma autenticação, porém o receptor não tem como provar a um terceiro que esta mensagem é autêntica. Propõe-se um protocolo criptográfico que faz uso de criptografia de chaves públicas ao invés de chaves simétricas capaz de unir a confiabilidade oferecida pela assinatura digital com a segurança oferecida pelo anonimato*

Palavras Chaves: *segurança, protocolos criptográficos, anonimato*

Abstract: *The symmetric cryptography provides some authentication, but the receptor has no way of convincing a third part that the message is authentic. We will propose a cryptographic protocol using public key instead of symmetric key to join the reliability given for the digital signature with the security given for the anonymity.*

Keywords: *security, cryptographic protocols, anonymity*

1 INTRODUÇÃO

Em 1976, Diffie e Hellman [DIF 76] mudaram os rumos da criptografia com o que eles chamaram de **criptografia de chave pública**. Diferente da criptografia tradicional, que usa uma chave única para cifrar e decifrar mensagens, eles propuseram um esquema que usa duas chaves distintas, denominadas chaves assimétricas. Uma das chaves é publicada (chave pública) e a outra é mantida em segredo (chave privada). Estas chaves são usadas para cifrar mensagens, de maneira que uma mensagem cifrada com a chave privada somente poderá ser decifrada com a chave pública, e vice-versa. Nos dias atuais, um dos algoritmos criptográficos mais usados é o RSA [RIV 78], que é uma implementação dos conceitos de chaves assimétricas.

O algoritmo de chave pública não é um substituto para a criptografia simétrica [SCH 96]. Os algoritmos de chave pública são lentos e vulneráveis a alguns ataques. Na maioria das implementações práticas, a criptografia de chave pública é usada para a distribuição segura das chaves simétricas (chaves de seção), que serão usadas para cifrar as mensagens [KOH 78]. Esta técnica se baseia em o originador gerar uma chave K simétrica (chave de seção), cifrar esta chave usando a chave pública do receptor (chave assimétrica) e envia-la para o receptor. O receptor decifra a mensagem recuperando a chave K, e esta chave será usada para a comunicação entre ambos. Nosso protocolo fará uso deste tipo de técnica, porém com algumas características especiais. Iremos usar o conceito de chave de seção, porém nossa chave de seção não será mais simétrica e sim um par de chaves assimétricas. Nossa chave de seção assimétrica terá vida lon-

ga, quando comparado com a maneira usual de uso de chaves de seção. Uma última diferença é que nossa chave assimétrica de seção será gerada pelo receptor da mensagem e não mais pelo originador.

Uma outra característica importante no uso de chaves assimétricas foi a possibilidade de desenvolver novos conceitos de assinatura digital, que permite ao receptor identificar o originador da mensagem. O NIST (National Institute of Standards and Technology) publicou um padrão para o uso da assinatura digital, conhecido como DSS (Digital Signature), inicialmente proposto em 1991, usando criptografia assimétrica e funções resumo (Hash) que agrega uma garantia de integridade ao esquema. O DSS não garante a confidencialidade da informação. A assinatura digital é suficiente para convencer os outros da autenticidade da mensagem. Porém, assinando um documento digitalmente você será responsável pelo mesmo, devido à característica de não-repúdio da assinatura digital. Técnicas que garantem o anonimato pode resolver a necessidade de repudiar uma mensagem enviada, porém o anonimato nos coloca em um dilema: como confiar em uma mensagem cuja origem é desconhecida? Para resolver este impasse iremos propor um protocolo criptográfico.

Nosso protocolo será baseado no problema da autenticação da mensagem, como descrito abaixo:

Criptografia simétrica prove alguma autenticação, mas o receptor não tem como convencer um terceiro da autenticidade da mensagem. Bruce Schneier [SCH 96] falou sobre o problema da autenticação da mensagem: *"Criptografia simétrica provê alguma autenticação. Quando Bob recebe uma mensagem de Alice cifrada com a chave compartilhada entre eles, Bob sabe que a mensagem veio de Alice. Ninguém mais conhece a chave deles. No entanto, Bob não tem como convencer um terceiro sobre isso"*. Várias propostas foram apresentadas para solucionar o problema da autenticação. Neste artigo iremos usar esta característica, não mais como um problema.

Fazendo uso das técnicas descritas anteriormente iremos propor um protocolo criptográfico para resolver o seguinte problema: vamos supor que Alice queira enviar uma mensagem para Bob. Porém, Alice quer a garantia que, se Bob publicar esta mensagem, ele não terá como provar que foi Alice quem lhe enviou a mensagem, mesmo Bob estando certo de que foi Alice quem lhe enviou a mensagem.

Este artigo é organizado em seis seções. Na seção 2 faremos uma breve revisão sobre comunicação em grupo. Na seção 3, apresentaremos as notações a serem usadas na formalização do protocolo. Na seção 4, descreveremos o protocolo proposto. Na seção 5 será as considerações de segurança do protocolo proposto, e finalmente na seção 6 faremos nossas considerações finais.

2 COMUNICAÇÃO EM GRUPO

David Chaum [CHA 91] introduziu a idéia de assinatura em grupo, que possui as seguintes propriedades: apenas membros do grupo podem assinar mensagens; o receptor pode verificar se a assinatura é válida para o grupo; o receptor não pode identificar qual dos membros é o originador; e em caso de disputa, a identidade do originador pode ser revelada. Em 1999, Tseng e Jan [TSE 98] publicaram um artigo baseado na assinatura em grupo que garante o anonimato

para cada membro. As mensagens podem ser lidas por cada um dos membros, sem saber quem as enviou. Após um período estabelecido, a identidade de cada um dos membros pode ser divulgada para os outros. Nossa proposta difere-se das anteriores pelas seguintes características:

- O anonimato é algo bem definido, estando presente ou não. Na nossa proposta, o anonimato esta presente, exceto para um membro, para o qual a mensagem é direcionada;
- A idéia de comunicação em grupo esta existente pelo fato de a comunicação ser feita entre os elementos de um grupo de pessoas, que tenham passado por um processo de inicialização do sistema. Porém o grupo é de tamanho variável e indefinido, sendo que nenhum dos elementos terá conhecimento do grupo como um todo.

As propriedades de nossa proposta de comunicação são as seguintes: apenas membros do grupo podem assinar as mensagens; cada elemento tem seu subgrupo, mais nenhum deles conhece o grupo como um todo; apenas um elemento do grupo saberá quem é o emissor da mensagem; em caso de disputa, a identidade do emissor não tem como ser revelada.

Baseado no RSA, [CHA 83] propôs em 1982 o primeiro esquema de assinatura cega, cujo objetivo é o de unir a confiabilidade da assinatura digital com a segurança do anonimato. Esta proposta permite assinar um documento sem conhecer seu conteúdo, e teve absoluta importância no desenvolvimento de protocolos para eleição segura e dinheiro digital, entre outros. Em 2000, Fan, Chen e Yeh [FAN 00] publicaram uma proposta adicionando alguns benefícios à proposta original, adicionando um fator randômico para proteger contra ataques que tentam descobrir a identidade dos membros. A proposta de Chaum é a que mais se aproxima da solução para o problema proposto, porém, mesmo o receptor sabendo que a mensagem foi assinada por uma autoridade confiável, o mesmo não saberá a origem específica da mensagem. Identificar a origem da mensagem é uma necessidade para nossa proposta.

3 NOTAÇÃO

A tabela 1 descreve aa notação a ser usada na formalização do protocolo proposto.

Tabela 1: Notação

Alice (A): Originador da Mensagem.	*Bob (B)*: Receptor da mensagem.
Carol (C): Terceira pessoa do esquema, que irá tentar identificar a identidade de Alice.	*Mallory (M)*: Quarta pessoa que irá tentar burlar o esquema, maliciosamente.
Simon (S): Responsável em mascarar os endereços, dificultando os ataques de Mallory.	*Trent (T)*: Autoridade confiável de distribuição de chave pública.
$\rightarrow$: Sentido de encaminhamento da Mensagem.	$\triangleright$: Produz.
$\|\|$: Concatenação.	X: Texto plano.
Y: Texto cifrado.	E: Cifrar.
D: Decifrar.	K: Chave Simétrica.
$E_K(X) \triangleright Y$ e $D_K(Y) \triangleright X$.	i: membros A, B, C, M, S ou T.
KU_i: Chave pública de i.	KR_i: Chave privada de i.
$E_{KU_i}(X) \triangleright Y$ e $D_{KR_i}(Y) \triangleright X$.	$E_{KR_i}(X) \triangleright Y$ e $D_{KU_i}(Y) \triangleright X$.
K_1 e K_2: Par de chaves assimétricas.	$E_{K_1}(X) \triangleright Y$ e $D_{K_2}(Y) \triangleright X$.
N_i: Endereço físico de i.	M: Mensagem.
ID_i: Identidade de i.	$H(M)$: Função resumo da mensagem M.

4 PROTOCOLO PROPOSTO

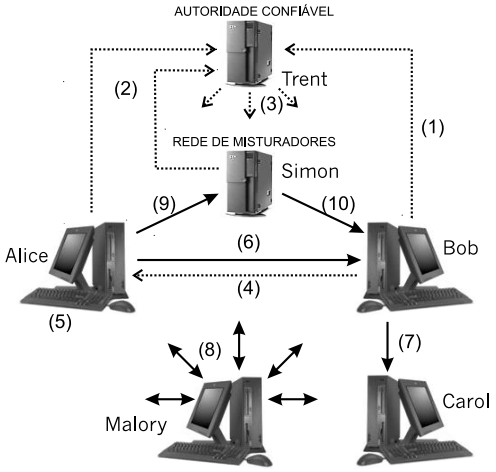

Figura 1: Protocolo Proposto

Na Figura 1 apresentamos os diversos elementos pertencentes ao nosso protocolo. Os elementos representados por computadores pessoais são os membros que participam do esquema. Os outros dois elementos, Trent e Simon, são os membros complementares, necessários no funcionamento do protocolo. As setas representam o fluxo de informação, sendo que as linhas tracejadas são informações de repasse de chaves. As linhas cheias representam a informação propriamente dita (mensagem). Os passos a serem seguidos estão representados pelos números entre parênteses. Detalhamos cada um destes passos a seguir:

Passo (1) : Bob gera um par de chaves assimétricas (KU_B e KR_B) e encaminha a chave pública KU_B com a sua identificação ID_B para Trent, por um canal seguro. Trent será responsável pela divulgação da chave KU_B. A chave KR_B é mantida em segredo por Bob. Trent tem a função de certificar se a chave informada por Bob realmente pertence a ele, pois cabe a ele, como sendo uma autoridade confiável de distribuição de chaves públicas. Uma maneira que Bob tem de entregar KU_B para Trent, é cifrar KU_B e sua identificação ID_B com a chave pública de Trent KU_T. Uma função resumo pode ser gerada sobre estes dados para garantia de integridade da informação. Formalmente temos:

$B \rightarrow T : E_{KU_T}(ID_B||KU_B||H(ID_B||KU_B))$

Passo (2) : analogamente ao passo (1), o mesmo procedimento é feito para divulgação da chave pública de Alice KU_A e de Simon KU_S. Formalmente teremos:

$A \rightarrow T : E_{KU_T}(ID_A||KU_A||H(ID_A||KU_A))$

$S \rightarrow T : E_{KU_T}(ID_S||KU_S||H(ID_S||KU_S))$

Passo (3) : Trent decifra as informações recebidas e divulga as chaves públicas KU_A, KU_B e KU_S para todos os elementos do esquema. Inclusive Mallory tem acesso a esta informação.

Esta fase inicial serve apenas para criarmos uma forma prática de possuirmos canais de comunicação confiáveis entre os elementos do sistema. O mesmo resultado pode ser ob-

tido usando certificados digitais. Neste caso, Trent seria uma Autoridade Certificadora. VeriSign, lider mundial de provisionamento de infraestrutira segura na Internet us esta técnica. Desta maneira, quando Bob quiser enviar uma informação de forma confiável para Alice, o mesmo poderá cifrar a mensagem com a chave KU_A, de maneira que somente Alice que possui a chave KR_A terá acesso a informação. A partir do passo (4) começa o nosso protocolo propriamente dito.

Passo (4) : Bob gera um novo par de chaves assimétricas K_1 e K_2, destinadas exclusivamente para a comunicação com Alice. A chave K_1 é encaminhada para Alice por um canal seguro, juntamente com a identidade de Bob ID_B. A chave K_2 é mantida em segurança por Bob.

$B \rightarrow A : E_{KU_A}(ID_B||K_1||H(ID_B||K_1))$

Estas fases até o passo (4) são as fases de inicialização, sendo executada uma única vez, no momento que o sistema é criado. A partir do passo (5) começa a comunicação propriamente dita.

As premissas que viabilizarão o protocolo a funcionar conforme a proposta inicail são:

- A chave K_1 é a maneira que Alice tem para se identificar perante Bob. Desta maneira Alice não tem interesse em divulgar K_1, pois uma terceira pessoa poderia enviar mensagens em seu nome para Bob.

- Bob não tem interesse em divulgar a chave K_1, pois divulgando-a Bob não teria mais como identificar quem é o emissor da mensagem.

Passo (5) : Alice quer enviar uma mensagem para Bob. Alice cifra a mensagem M com a chave K_1, de maneira que somente Bob que possui a chave K_2 poderá decifrar a mensagem. Uma função resumo pode ser inserida para garantia de integridade da informação.

$A \rightarrow B : E_{K_1}(M||H(M)) \triangleright Y$

Passo (6) : A mensagem cifrada Y é transmitida. Bob, recebendo a mensagem Y de Alice, decifra usando a chave K_2, recuperando a mensagem M. A única informação que identifica que a mensagem Y foi enviada por Alice é o fato da mesma ter sido cifrada com a chave K_1, pois somente Bob sabe que K_1 é de Alice.

Em $B : D_{K_2}(Y) \triangleright M||H(M)$

Recalculando a função resumo sobre a mensagem M, Bob certifica a integridade da mensagem recebido de Alice.

Passo (7) : Bob resolve repassar a mensagem para Carol, e tem todo o direito de faze-lo, porém Bob não tem como provar que o mesmo foi originado por Alice. Bob pode até dizer que foi Alice quem lhe enviou a mensagem, mas não tem como provar.

Passo (8) : Mallory representa uma pessoa maliciosa tentando burlar o esquema. Mallory pode ser qualquer elemento que esteja usando de todos os artifícios para tentar descobrir a identidade de Alice, exceto ALice e Bob. Escutando os canais de comunicação, identificando o endereço de origem das mensagens, Mallory pode saber que Alice esta se comunicando com Bob. Desta maneira, para aumentarmos ainda mais a garantia do anonimato de Alice,

dificultando as ações de Mallory. Vamos inserir o elemento chamado Simon, responsável por mascarar os dados de endereçamento bem como, eliminar qualquer relação estatística entre o tamanho das mensagem recebidas e encaminhadas. Uma estrutura criptográfica chamada *"Rede de Misturadores"* [CHA 81] pode ser usada. A Rede de Misturadores habilita um grupo de usuários trocar mensagens, eliminando qualquer relação entre os dados recebido e reenviados. Simon é um elemento de confiança, sem muita inteligência, cuja função fundamental é a de reencaminhar as mensagens em fragmentos. Desta maneira, ao invés de Alice encaminhar a mensagem diretamente para Bob, ela encaminha para Simon que repassa a mensagem para Bob. Simon não terá acesso à mensagem, pois esta cifrado com a chave K_1.

Passo (9) : Alice envia a mensagem M cifrado com a chave K_1 juntamente com o endereço físico N_B de Bob para Simon, por um canal seguro, cifrando com a chave pública de Simon KU_S. A função resumo pode ser novamente usada.

$A \rightarrow S : E_{KU_S}(N_B||H(N_B)E_{K_1}(M||H(M)))$

Passo (10) : Simon decifra a primeira parte da mensagem recebida de Alice com sua chave KR_S e encaminha a outra parte, $E_{K_1}(M||H(M))$, para o endereço N_B. Simon, recebe diversas mensagens de tamanho variável, e encaminha fragmentos da mensagem, de tamanho fixo para o endereço N_B, dificultando qualquer associação entre o tamanho dos pacotes de entrada originados por Alice e o tamanho dos pacotes de saída encaminhados para Bob. Mais uma vez, a única informação que certifica que a mensagem veio de Alice é o fato de Bob saber que a chave K_1 é exclusiva de Alice. Nem mesmo Bob poderá associar a mensagem recebido com o endereço de origem da mensagem recebida, pois todas as mensagens estão vindo de Simon. Desta maneira, Bob sabe que a mensagem veio de Alice, mas não tem como provar.

5 CONSIDERAÇÕES DE SEGURANÇA

Analisaremos aqui os diversos aspectos de segurança do protocolo acima descrito.

Bob gera um par de chaves para comunicação com Alice. Bob envia a chave K_1 para Alice, que não deve divulgar esta chave para ninguém, pois é com esta chave que Alice se identificará perante Bob.

a) O que acontece se Alice divulgar a chave K_1?

- *Com Alice*: Alice não terá mais como se autenticar perante Bob. É como se Alice tivesse passado uma procuração para um terceiro, que responderá por Alice frente a Bob.

- *Com Bob*: Bob pensará que toda informação cifrada com a chave K_1 veio de Alice. Porém nada impede que Alice divulgue sua chave, e Bob não tem como saber quando isso ocorrer.

O interesse de Alice está no fato que Bob vai acreditar que toda mensagem cifrado com a chave de Alice é proveniente da mesma, mesmo não tendo como provar. Alice precisa deste tipo de comunicação com Bob. Nem mesmo Alice terá acesso à mensagem enviado

por um terceiro que teve acesso a chave K_1, pois somente Bob possui a chave K_2 capaz de decifrar a mensagem. Isso poderia desqualificar Alice em relação a Bob.

b) O que acontece se Bob entregar a chave K_1 de Alice para um terceiro?

É de interesse de Bob que somente Alice possua a chave K_1, pois é a única maneira que Bob tem de saber que a mensagem veio de Alice. Divulgando a chave K_1, Bob não vai saber quem encaminhou a mensagem. Como Bob não tem como provar que a mensagem veio de Alice, o mesmo não teria motivos para tal.

c) O que acontece se Bob divulgar a chave K_2?

Se Bob divulgar a chave K_2, todas as pessoas que possuírem esta chave poderão ler a mensagem enviado por Alice, porém somente Bob saberá que a mensagem veio de Alice. Bob pode até dizer que a mensagem veio de Alice, mas não tem como provar. Em condições normais somente Bob terá acesso a informação e saberá que veio de Alice.

d) O que acontece se Bob enviar uma outra chave K_1' para Alice, diferente de sua chave K_1?

Um terceiro elemento, a exemplo de Carol, em comum acordo com Bob, poderia gerar um par de chaves K_1' e K_2' e enviar K_1' para Bob. Bob, tentando revelar a identidade de Alice para Carol, envia a chave K_1' como sendo sua chave K_1. De qualquer maneira Bob não teria como provar para Carol que a chave K_1' foi repassada para Alice. Como consequencia, somente Carol que possuia a chave K_2' teria acesso a informação enviada por Alice, porém Carol não terá como se certificar se a mensagem veio realmente de Alice.

Desta maneira, a proposta inicial se satisfaz, pois a identidade de Alice estará resguardada em qualquer situação. Ninguém, além de Bob, saberá a origem da informação.

6 CONSIDERAÇÕES FINAIS

No processo de inicialização, passo (4), Mallory pode tentar encaminhar uma mensagem divulgando uma chave K_1' como sendo a chave K_1 de Bob, tentando se passar por Bob. Desta maneira Alice encaminharia mensagens para Mallory pensando estar enviando para Bob. Um processo de assinatura digital pode ser usado para que Alice tenha certeza que foi Bob quem lhe enviou a informação. Cifrando a função resumo com sua chave KR_B, Bob prova para Alice ser ele o emissor da mensagem. A mensagem toda deve ser cifrada com a chave KU_A de Alice, de maneira que somente Alice tenha acesso a informação, como a seguir:

$B \rightarrow A : E_{KU_A}(ID_B||K_1||E_{KR_B}(H(ID_B||K_1)))$

Assim Alice se certificará que Bob é o emissor. Como conseqüência, Alice tem como provar que Bob também tem conhecimento da chave K_1. Com isso, Alice poderá comprovar que Bob conhece a mensagem por ela enviada. Não é de interesse de Alice faze-lo, pois estaria confessando ser ela mesma a fonte da informação. É de interesse de Alice manter seu anonimato na mensagem enviada para Bob. Este passo é de fundamental importância no funcionamento do protocolo.

Ainda no passo (4), onde Bob gera o par de chaves assimétricas K_1 e K_2, poderia ser usado uma chave simétrica K única, a ser divulgada para Alice. Os princípios do protocolo se mantém,

a menos do seguinte problema. Alice, em posse da chave K pode querer divulga-la para um terceiro. Fazendo-o, Alice terá acesso as mensagens encaminhadas por este terceiro para Bob, o que daria a Alice uma maior segurança para divulgar a chave K. Isto poderia vir a desqualificar o protocolo. Usando-se chaves assimétricas, se Alice divulgar a chave K_1 recebida de Bob, nem mesmo Alice terá acesso as informações enviadas para Bob em seu nome, o que dá uma maior segurança ao protocolo.

O protocolo descrito é baseado no ”princípio do interesse mútuo”, e se isso acontecer, teremos uma forma interessante de comunicação. Um terceiro, tal como Carol, pode vir a ter acesso ao mensagem, mediante uma traição de Bob. Porém Bob não tem como provar que foi Alice quem lhe enviou o mensagem, deixando Carol na incerteza da origem da informação. O anonimato de Alice esta garantido de qualquer maneira, exceto para Bob, atendendo o propósito do protocolo.

A implementação deste protocolo é relativamente simples, por se tratar de técnicas consagradas, e mesmo sendo técnicas bastante difundidas, esta proposta trás um enfoque diferente ao tema em questão, mostrando um detalhamento e uma análise nunca antes visto.

Referências Bibliográficas

[CHA 81] CHAUM, D. Untraceable electronic mail, return addresses, and digital pseudonyms. **EUROCRYPT'91**, [S.l.], 1981.

[CHA 83] CHAUM, D. Blind signatures for untraceable payments. **CRYPTO'82**, [S.l.], 1983.

[CHA 91] CHAUM, D. Group signatures. **EUROCRYPT'91**, [S.l.], 1991.

[DIF 76] DIFFIE, W.; HELLMAN, M. New directions in cryptography. **IEEE Transations on Informations Theory**, [S.l.], v.22, n.6, p.644–654, 1976.

[FAN 00] FAN, C.-I.; CHEN, W.-K.; YEH, Y.-S. Randomization enhaced chaum's blind signature scheme. **Computer Communications**, [S.l.], v.23, p.1677–1680, 2000.

[KOH 78] KOHNFELDER, L. **Towards a Practical Public-Key Cryptosystem**. M.I.T., May, 1978. Tese de Doutorado.

[RIV 78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public key cryptosystems. **Communications of the ACM**, [S.l.], v.21, n.2, p.120–126, 1978.

[SCH 96] SCHNEIER, B. **Apllied Cryptography**. United States of America: John Wiley Sons, Inc., 1996.

[TSE 98] TSENG, Y.-M.; JAN, J.-K. A novel id-based group signature. **Information Science**, [S.l.], v.120, p.131–141, jul, 1998.