Plano de Estudos

MAC 5701 – TÓPICOS EM CIÊNCIA DA COMPUTAÇÃO

Aluno:	Waldyr Dias Benits Júnior
Nº USP:	3772327
Orientador:	prof. Dr. Routo Terada
Área de interesse:	Criptografia – Sistemas Criptográficos baseados em identidade

1- Introdução

Este documento tem como objetivo detalhar um plano de estudos a ser seguido no primeiro semestre de 2003, constando de levantamento bibliográfico e resumo de artigos relacionados à área de interesse, a fim de contribuir para a elaboração da dissertação de Mestrado.

2- A área de Estudo

Nos dias de hoje, diversas operações, como compras e transações bancárias de pequena e grande monta, podem ser feitas através da Internet. Isto possibilita um compartilhamento de recursos, o que, por sua vez, propicia um ganho de economia em escala. Infelizmente, as informações que circulam na grande rede podem ser facilmente observadas por terceiros, nem sempre bem-intencionados. Faz-se necessário, portanto, uma preocupação constante com a segurança no transporte e armazenamento de informações sensíveis. É impensável se falar em "ambiente seguro" se as informações não estiverem protegidas por uma criptografia forte e outros mecanismos de segurança, como assinatura digital.

Atualmente, podemos fazer uso da criptografia simétrica ou assimétrica para garantirmos a segurança necessária, mas cada uma delas apresenta certas desvantagens. No caso da criptografia simétrica, temos a necessidade de estabelecer um canal seguro para troca das chaves, e, uma vez trocadas, é preciso que haja um gerenciamento das mesmas, a fim de proporcionar um armazenamento seguro. O problema se agrava a medida que aumenta o número de participantes na comunicação, tendo em vista que o número de chaves necessárias cresce numa ordem de grandeza proporcional ao quadrado do número de participantes. Já na criptografia assimétrica, além dos algoritmos conhecidos serem bem mais lentos do que os de criptografia simétrica, há a exigência de uma infraestrutura para armazenamento das chaves públicas, bem como a preocupação em se garantir a autenticidade destas, o que é conseguido através de certificados digitais. Estes certificados, por sua vez, têm que ser verificados, o que envolve um custo computacional adicional para cada verificação.

Mais recentemente, as curvas elípticas permitiram o desenvolvimento de uma criptografia assimétrica em que a chave pública de um usuário não é uma cadeia aleatória de *bits* e sim um identificador que caracteriza este usuário de forma única, como por exemplo seu número de CPF ou seu endereço eletrônico (*e-mail*). Tal fato possibilitou que se estabeleça uma comunicação segura sem troca de segredos, sem troca de certificados digitais e sem a necessidade de se manter um diretório público de chaves. Desta forma, podemos conceber uma troca de mensagens da mesma maneira em que ocorre no correio físico: se você conhece o endereço de uma pessoa, você pode enviar uma correspondência que, teoricamente, somente ela poderá abrir. Este esquema de criptografia assimétrica é hoje conhecido como criptografia baseada em identidade (IBE - *Identity-Based Encryption*), e por não ter nenhuma literatura em língua portuguesa sobre este assunto, motivou seu estudo e nos servirá de ponto de partida como tema para a dissertação de Mestrado.

3- Trabalhos Relacionados

Os conceitos fundamentais de criptografia e a sua terminologia, que será utilizada no decorrer deste trabalho, podem ser estudados nos livros [1], [2], [3] e [4].

A criptografia de chave pública - em que são utilizadas duas chaves, sendo uma de domínio público, usada para cifrar mensagens e verificar assinaturas e outra de conhecimento exclusivo de seu detentor, chamada de chave privada, e que é usada para decifrar e assinar mensagens - foi proposta pela primeira vez em 1976, no artigo [5], de Diffie e Hellman. Mais tarde, R.Rivest, A. Shamir e L. Adleman desenvolveram e publicaram o algoritmo RSA, primeiro algoritmo de chave pública [6].

As curvas elípticas, com suas propriedades, permitiram que se pudesse mapear um conjunto de bits em pontos de uma curva, e a partir daí, trabalhar com estes pontos na criptografia. A aritmética das

curvas elípticas pode ser estudada no livro [7]. A aplicação de curvas elípticas em criptografia é tratada nos artigos [8] e [9].

O conceito de Sistemas Criptográficos baseados em identidade surgiu com A. Shamir, em 1984 [10], e a sua principal característica é que, diferentemente da criptografia assimétrica padrão, temos como chave pública alguma característica que identifique o usuário de forma única, como por exemplo seu endereço eletrônico (*e-mail*) e, com isso, não há mais a necessidade de se fazer um mapeamento entre o usuário e sua chave pública através de certificados digitais, haja vista que a chave pública identifica o próprio usuário. A partir deste artigo de Shamir, vários pesquisadores trataram do assunto, como [11], [12].

As *Short Signatures*, ou assinaturas curtas, baseadas no *Weil Pairing*, foram introduzidas em [13] e, apesar de não serem sistemas baseados em identidade, utilizam as propriedades das curvas elípticas, sendo muito utilizadas em conjunto com os sistemas baseados em identidade, e por isso, serão incluídas neste trabalho. Existem, ainda, diversos esquemas de assinaturas baseadas em identidade, como pode ser visto em [14], [15] e [16].

O artigo [17] traz uma importante contribuição com a transformação de sistemas *one-way encryption* (ID-OWE - nível mais baixo de segurança) em sistemas seguros contra ataque adaptativo a texto ilegível escolhido (ID-CCA - nível mais elevado); o artigo [18] define os sistemas SPKI, que servirão de ponto de partida para estudarmos toda a infraestrutura de chaves públicas (PKI) e o artigo [19] traz o conceito de hierarquia de certificados baseados em identidade.

Podemos ver implementações do *Tate Pairing*, uma função bilinear utilizada em curvas elípticas e que é muito empregada nos esquemas baseados em identidade, nos artigos [20] e [21].

O esquema de assinatura & criptografia em um único passo (*signcryption*), em que se consegue sigilo e autenticidade de uma mensagem em um único passo, é uma forma otimizada do tradicional "assinar-e-depois-cifrar", e pode ser visto no artigo [22].

Finalmente, o artigo [23], em que nos baseamos para escolher o tema da dissertação, apresenta uma revisão de criptografia e assinatura baseadas em identidade, além de um modelo híbrido de certificação PKI/ IBE e mostra diversas aplicações relacionadas com Sistemas Criptográficos baseados em identidade.

4- O Plano de Estudos

O objetivo de nosso trabalho é desenvolver uma pesquisa na área de Sistemas Criptográficos baseados em identidade, apresentando os esquemas de criptografia e assinatura *ID-Based,* e suas principais aplicações, além de um estudo na tradicional infraestrutura de chaves públicas (PKI), mostrando suas principais desvantagens e vulnerabilidades. Mostraremos, ainda, como poderemos conseguir uma hierarquia de certificação de chaves públicas baseadas em identidade. Na fase final da dissertação, fase esta que transcorrerá após a conclusão deste trabalho, procuraremos fazer uma comparação destes esquemas baseados em identidade com os tradicionais esquemas de chave pública padrão, com base nos critérios de desempenho, segurança e facilidade de implementação. Deveremos seguir o seguinte cronograma:

JAN e FEV 2003	Pesquisa bibliográfica de artigos relacionados
MAR 2003	Continuação da pesquisa e apresentação de seminários internos sobre o tema proposto, visando ampliar conhecimentos
ABR 2003	Continuação dos seminários
MAI 2003	Início da elaboração do resumo final
JUN 2003	Conclusão do resumo final, a ser entregue como relatório desta disciplina
JUL 2003	Exame de qualificação, submetendo como trabalho o relatório apresentado nesta Disciplina
AGO 2003	Continuação do trabalho de pesquisa visando a fase final da dissertação

5- Conclusão

Por se tratar de um assunto recente na área de criptografia, certamente ainda surgirão diversos trabalhos relacionados, o que contribuirá para enriquecer cada vez mais nossa pesquisa. Pretendemos que o relatório a ser apresentado sirva de ponto de partida para o texto final da dissertação de Mestrado, e nos permita um pleno entendimento do assunto, nos dando a maior parte dos elementos necessários a uma comparação o mais completa possível. Esta dissertação, depois de concluída, poderá servir de motivação para uma Tese de Doutorado, seja na busca de outros aspectos para comparação, na descoberta de novas vulnerabilidades nos sistemas comparados, ou mesmo em implementações de Sistemas Criptográficos baseados em identidade.

6- Referências Bibliográficas Atuais

[1] R. Terada. *Segurança de Dados- Criptografia em Redes de Computador*. 1ª ed. Edgard Blücher, 2000.

[2] D. Stinson. *Cryptography – Theory and Practice*. 2nd ed. Chapman & Hall, 2002.

[3] A. Menezes, P. Oorschot and S. Vanstone. *Handbook of Applied Cryptography*. 1st ed. CRC, 1997.

[4] W. Stallings. *Cryptography and Network Security – Principles and Practice*. 3th ed. Prentice Hall, 2002.

[5] W. Diffie e M. Hellman. *New Directions in Cryptography*. IEEE Transactions on Information Theory, v. IT-22, nº 6, Nov 1976, pp. 644-654.

[6] R. Rivest, A. Shamir e L. Adleman. *A Method for Obtaining Digital Signatures and Public Key Cryotosystems*. Communications of the ACM, v. 21, nº 2, Feb 1978, pp. 120-126.

[7] J. Silverman. *The Arithmetic of Elliptic Curves*. 1st ed. Springer Verlac. 1986.

[8] P. Barreto. *Curvas Elípticas e Criptografia: Conceitos e Algoritmos*. Disponível em <http://planeta.terra.com.br/informatica/paulobarreto>. 1999.Acesso em 25/03/2003.

[9] S. Galbraith. *Supersingular Curves in Cryptography*. ASIACRYPT 2001, pp. 495-513.

[10] A. Shamir. *Identity Based Cryptosystems and Signature Schemes*. Advances in Cryptology – CRYPTO'84, Springer-Verlag, LNCS 196, pp. 47-53, 1985.

[11] D. Boneh e M. Franklin. *Identity Based Encryption from the Weil Pairing*. Advances in Cryptology – CRYOTO'2001, Springer-Verlag, LNCS 2139, pp. 213-229, 2001.

[12] C. Cocks. *An Identity Based Encryption Scheme Based on Quadratic Residues*. Cryptology and Coding, Springer Verlag, LNCS 2260, pp. 360-363, 2001.

[13] D. Boneh, B. Lynn e H. Shacham. *Short Signature from the Weil Pairing*. Advances in Cryptology – ASIACRYPT'2001, Springer-Verlag, LNCS 2248, pp. 514-532, 2001.

[14] J.C. Cha e J.H. Cheon. *An Identity-based Signature from gap Diffie-Hellman groups*. Preprint, 2002.

[15] F. Hess. *Efficient Identity Based Signature Schemes Based on Pairings*. To appear Selected Areas in Cryptography - 2002.

[16] K. Paterson. *ID-Based Signatures from Pairings on Elliptic Curves*. Preprint, 2002.

[17] E. Fujisaki e T. Okamoto. *Secure Integration of Asymmetric and Symmetric Encryption Schemes*. Advances in Cryptology – CRYPTO'1999, Springer-Verlag LNCS 1666, pp. 537-554, 1999.

[18] C. Ellison e B. Frantz. *SPKI Certificate Theory*. Internet RFC 2693, 1999.

[19] J. Horowitz e B. Lynn. *Hierarchical Identity-Based Encryption*. Advances in Cryptology – EUROCRYPT'2002, Springer-Verlag LNCS 2332, pp. 466-481, 2002.

[20] P. Barreto, H. Kim, B. Lynn e M. Scott. *Efficient Algorithms for Pairing-Based Cryptosystems*. Advances in Cryptology – Crypto'2002, Lecture Notes in Computer Science 2442, Springer-Verlag (2002), pp. 354--368.

[21] S. Galbraith, K. Harrison, D. Soldera. *Implementing the Tate Pairing*. ANTS 2002, pp.324-337.

[22] D. Nalla e K.C. Reddy. *Signcryption scheme for Identity-based Cryptosystems.* Disponível em <http://eprint.iacr.org/2003/044/>. 2002. Acesso em 13/03/2003.

[23] L. Chen, K. Harrison, A. Moss, D. Soldera e N.P. Smart. *Certification of Public Keys within an Identity-Based System*. 5th International Security Conference, ISC 2002, LNCS 2433, pp. 322-333, 2002.