APLICAÇÃO DE TÉCNICAS CRIPTOGRÁFICAS NA PROTEÇÃO DE UMA REDE CORPORATIVA DE COMPUTADORES

Kátia G. Pinto

Quartel do Comando Geral
Polícia Militar de Pernambuco
Praça do Derby, Recife, PE
katia@fisepe.pe.gov.br

*Valdemar C. da Rocha Jr.**

Grupo de Pesquisa em Comunicações
Depto. de Eletrônica e Sistemas - UFPE
CP 7800, CEP 50711-970 Recife, PE
vcr@npd.ufpe.br

RESUMO

Este trabalho foi motivado pela preocupação em utilizar criptografia para salvaguardar informações sigilosas que transitam em rede nos diversos setores da Polícia Militar de Pernambuco, principalmente após a implantação da Rede Corporativa, em função do papel estratégico desta. É apresentada uma aplicação da cifra SAFER, proposta pelo Prof. James Massey, associada à técnica de geração pública de chaves secretas de Diffie e Hellman. Foram investigadas as propriedades, a forma de emprego e o sistema de gerenciamento de chaves. Um protótipo do sistema foi implementado em *software*, possibilitando demonstração do seu funcionamento.

1. INTRODUÇÃO

A fusão dos computadores e das telecomunicações teve uma profunda influência sobre a forma como os computadores são organizados atualmente. O velho modelo de um único computador servindo a todas as necessidades computacionais da organização vem sendo rapidamente substituído por outro no qual um grande número de computadores, separados fisicamente mas ligados em rede, executam a tarefa. Aliada a toda esta tecnologia, surge uma nova preocupação referente à segurança das informações que trafegam em uma rede de computadores. Assim como uma rede provê uma série de facilidades e dinamismo aos serviços executados, ela pode também ser alvo de ameaças relacionadas à segurança. A ausência de uma política de segurança pode fazer com que uma Organização se torne vulnerável a ataques às informações sigilosas, os quais poderão deixá-la em uma situação altamente embaraçosa e causar imensos prejuízos.

*O trabalho deste autor foi financiado parcialmente pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Projeto 304214/77 – 9

Ante o exposto e tendo em vista a implantação da Rede Corporativa na Polícia Militar de Pernambuco (PMPE), foi desenvolvida uma dissertação de mestrado [1] abordando técnicas criptográficas e gerenciamento de chaves. Além da utilização de técnicas criptográficas, este trabalho visou também a investigação científica e a disseminação do conhecimento acumulado sobre o tema, ou seja, visou melhorar o nível geral de competência técnica na PMPE, dedicando tempo e recursos a essa tarefa. Por meio de um planejamento cuidadoso e testando as soluções propostas, foi possível disponibilizarmos benefícios das telecomunicações para a Corporação, de uma maneira segura e prudente.

Na Seção 2, introduzimos conceitos básicos sobre Segurança de Redes e Criptografia. Dentro desse contexto temos os conceitos sobre ameaças e ataques, política de segurança, serviços de segurança e os mecanismos de segurança. Na Seção 3, apresentamos o projeto de implementação de uma técnica criptográfica, o SAFER (Secure And Fast Encryption Routine), como uma das medidas adotadas na política de segurança na rede de computadores da PMPE, em que descrevemos, inicialmente, o pressuposto norteador dessa escolha entre tantas técnicas criptográficas existentes e, a seguir, suas propriedades, seu funcionamento, suas vantagens e sua disponibilização. Descrevemos, ainda, um sistema de gerenciamento de chaves, que foi desenvolvido para aplicação direta na PMPE, usando programação em Visual Basic e, por meio de exemplo, apresentamos o emprego do SAFER.

2. SEGURANÇA EM REDES E CRIPTOGRAFIA

Nesta seção abordaremos alguns conceitos básicos sobre segurança em redes de computadores, bem como criptografia, tendo em vista a importância da utilização de técnicas criptográficas como um dos instrumentos

de segurança em redes. Os serviços de segurança em uma rede de computadores têm como função a confidencialidade, que consiste em proteger os dados contra leitura por pessoas não autorizadas, e a integridade dos dados, que consiste em evitar que pessoas não autorizadas insiram, excluam ou modifiquem mensagens. A autenticação das partes envolvidas consiste em verificar o transmissor de cada mensagem e tornar possível aos usuários o envio de documentos eletronicamente assinados.

2.1. Integridade de dados

Para garantir a integridade dos dados, podem ser usadas técnicas de detecção de modificação, normalmente associadas com a detecção de erros em *bits*, em blocos, ou erros de seqüência introduzidos por enlaces e redes de comunicação. Entretanto se os cabeçalhos e fechos carregando informações de controle não forem protegidos contra modificações, um intruso, que conheça as técnicas usadas pode contornar a verificação.

2.2. Criptografia

Segurança é uma propriedade complexa, difícil de modelar e otimizar. Na verdade, trata-se de um conceito o qual se baseia em quanto se está protegido de um possível oponente. Projetar um sistema de segurança significa analisar o potencial do possível adversário e desenvolver uma estratégia que consiga neutralizar seus "ataques". Segurança de dados visa a proteção de dados em sistemas de comunicação, envolvendo armazenamento e transmissão. Dentre os tipos de proteção utilizados em segurança de dados destaca-se como o principal deles a criptografia. A criptografia surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis, ou seja, em meios em que não é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura (intruso passivo) ou para modificá-lo (intruso ativo). A forma de proteção encontrada baseia-se na utilização de um método para modificar o texto original de uma mensagem a ser transmitida (texto claro), gerando um texto criptografado na origem, através de um processo de cifragem definido por um método de criptografia, garantindo, assim, a confidencialidade (podendo também vir a garantir a autenticidade) da informação armazenada ou transmitida. Os objetivos da criptografia, que são essencialmente, sigilo e autenticidade, são na verdade conceitos completamente independentes. Xuejia Lai, pesquisador chinês radicado na Suíça, deu talvez a melhor regra para distinguir entre sigilo e autenticidade. Uma técnica provê sigilo se ela determina quem pode receber a mensagem; ela provê autenticidade se determina quem pode ter enviado a mensagem [2]. Para cifrarmos ou decifrarmos uma mensagem, necessitamos de informações confidenciais geralmente associadas a uma quantidade denominada chave. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para cifrar como para decifrar mensagens, enquanto outros mecanismos utilizam chaves distintas para cifragem e decifragem [3]. Os processos criptográficos atuais fornecem mecanismos para implementarmos autenticidade e sigilo. Esses mecanismos podem ser usados para controlar, por exemplo, acessos a discos rígidos compartilhados, ou controlar canais de TV pagos por tempo de uso, etc.. As possibilidades de aplicações para o campo da criptografia são muito amplas. Com algumas ferramentas básicas é possível elaborar esquemas e protocolos que nos permitam o uso de dinheiro eletrônico, ou provar que se tem acesso a certa informação sem a necessidade de revelá-la, ou, então, compartilhar um segredo de modo que, digamos por exemplo não menos que 3, de um grupo de 5 pessoas, possam reconstruí-lo [4].

2.3. Sistemas criptográficos

A maioria dos sistemas criptográficos, usados na prática, baseia-se não na impossibilidade de serem quebrados mas sim na dificulade de tal quebra. Segurança contra um inimigo, que tem uma certa limitação de tempo e de poder de computação disponíveis para seu ataque, é chamada de segurança computacional; Shannon usou a terminologia segurança "prática" [4], [5].

3. A CIFRA SAFER

Apresentamos a técnica criptográfica SAFER (Secure And Fast Encryption Routine) nesta seção, como sugestão para implementação na rede de computadores da PMPE, bem como o pressuposto norteador dessa escolha. Os detalhes técnicos quanto às suas propriedades, seu funcionamento, suas vantagens e sua disponibilização estão descritos em [6]. Abordaremos, ainda, o sistema de gerenciamento de chaves, o qual foi desenvolvido na linguagem Visual Basic para aplicabilidade na PMPE [1].

3.1. Pressupostos norteadores

Considerando todo o levantamento realizado através do estudo exploratório, foi verificada a necessidade da implementação de uma política de segurança na rede corporativa da PMPE, pois o trânsito de informações, nos mais diversos setores da polícia é, em grande parte, classificado como sigiloso devido à peculiaridade da atividade policial militar. Para resguardar estas informa-

ções do acesso por pessoas não autorizadas, apresentamos como sugestão a utilização da técnica criptográfica denominada SAFER. A escolha do SAFER, entre tantas outras técnicas criptográficas, foi motivada pelo fato desta cifra ter um rastro de segurança desde seu lançamento em 1993 e por ser consignada ao domínio público. A seu favor a cifra SAFER tem ainda os fatos de ter recentemente participado do rol das técnicas concorrentes à substituição do DES (Data Encryption Standard), que atualmente ainda é o padrão norte-americano de cifragem, e de ter sido adotada para esquema de autenticação do protocolo Bluetooth para comunicações sem fio [7].

3.2. SAFER K-64

Descreveremos, a seguir, alguns aspectos importantes da cifra não proprietária SAFER (Secure And Fast Encryption Routine), criada pelo Prof. James Massey [6] para a Cylink Corporation (Santa Clara, CA, USA), em 1993. O SAFER K-64 é um algoritmo de cifragem de bloco orientado a *byte*. Nele, tanto o texto claro quanto o texto cifrado têm comprimento de 64 *bits* (8 *bytes*). A chave selecionada pelo usuário também tem comprimento de 64 *bits* (8 *bytes*). Uma diferença importante entre o SAFER e outras cifras de bloco é o fato da cifragem e da decifragem não diferirem apenas na reversão da construção das sub-chaves [6]. São usadas apenas operações com *bytes* nos processos de cifragem e de decifragem. Esta propriedade é particularmente útil em aplicações como *smart cards*, em que o poder de processamento disponível é muito limitado. A fim de alcançar a segurança desejada, foram explorados dois novos conceitos criptográficos. São eles: 1) uso de Transformação Linear Não-Ortodoxa (Pseudo-Transformada de Hadamard), para realizar difusão tanto do texto claro como da chave, sobre o texto cifrado e 2) uso de Polarização Aditiva de Chaves, para eliminar chaves fracas.

SAFER K-64 é uma cifra iterativa, isto é, a cifragem é realizada aplicando-se 6 rodadas (valor recomendado) de uma mesma transformação, e então aplicando uma transformação de saída. Cada iteração usa duas subchaves (8 *bytes* cada), derivadas da chave secreta pelo algoritmo de subchaves. No SAFER K-64 a decifragem consiste numa transformação de entrada, seguida por r rodadas idênticas. A transformação de entrada é formada por operações de ou-exclusivo e subtração módulo 256. O projeto do SAFER K-64 foi feito obedecendo aos princípios de Shannon, da confusão e da difusão, para a obtenção de segurança nas cifras de chave privada. As operações de transformações empregadas provocam a confusão necessária para fazer com que a estatística do texto cifrado dependa, de maneira complicada, da estatística do texto claro, dado que pequenas mudanças se difundem rapidamente através da cifra. A fim de garantir a difusão desejada foi criada uma nova e não ortodoxa transformada, a Pseudo-Transformada de Hadamard, que faz com que um dado *byte* de entrada afete cada *byte* de saída, isto é, a Pseudo-Transformada de Hadamard proporciona completa e garantida difusão em cada camada linear. A rápida difusão proporcionada pela Pseudo-Transformada de Hadamard é a principal razão pela qual a escolha de $r = 6$ é suficiente para fazer com que o SAFER K-64 seja resistente a "quebras" [8].

Foi mostrado em [8] como o SAFER K-64 alcança tanto boa confusão quanto boa difusão, as quais são dois atributos básicos para que uma cifra de bloco iterativa seja segura. Atualmente, a melhor ferramenta para a medição da segurança proporcionada por uma cifra iterativa é a resistência da mesma à criptoanálise diferencial. Muitos testes foram feitos por criptoanalistas contratados pela Cylink Corporation, os quais não tinham nenhum vínculo com o projeto. Além dos testes envolvendo ataques por criptoanálise diferencial, também foram feitos extensivos estudos estatísticos da cifra, com o objetivo de encontrar alguma fraqueza na mesma. Concluiu-se, com tais testes, que o SAFER K-64 com 6 rodadas é resistente à criptoanálise diferencial e tambám que nenhum tipo de fraqueza foi encontrada no mesmo [9].

3.3. SAFER K-128

Logo após o anúncio do SAFER K-64, surgiram pedidos para uma versão com chave de comprimento 128 *bits*, selecionada pelo usuário. Tal pedido foi atendido pelo *Special Projects Team of the Ministry of Home Affairs*, Singapura, que tomou a iniciativa de criar um novo algoritmo para a geração das subchaves, a partir da chave selecionada pelo usuário, agora com 128 *bits* [8].

O SAFER K-128 é uma cifra com estrutura iterativa, empregando transformação de saída e chaves de polarização idênticas ao SAFER K-64, porém o comprimento da chave selecionada pelo usuário é de 128 *bits*. Recomenda-se, nesta implementação, a utilização de 10 iterações ($r = 10$) sem, no entanto, utilizar mais que 12 rodadas. O SAFER K-128 é compatível com o SAFER K-64. Esta característica tornou o algoritmo bastante atrativo. O usuário que possua a implementação SAFER K-128 pode utilizá-la como SAFER K-64, para cifrar ou decifrar quando desejado. A cifra SAFER K-128 é também uma cifra não proprietária.

3.4. SAFER +

Faremos uma breve exposição sobre o SAFER +, esclarecendo que em princípio o sistema que será adotado inicialmente na PMPE será o SAFER K-128. O SAFER + foi a proposta da Cylink Corporation, para o Advanced Encryption Standard e que foi adotado, como mencionado acima, para esquema de autenticação do protocolo Bluetooth [7] . Os inventores do algoritmo são James L. Massey, Gurgen H. Khachatrian e Melsik K. Kuregian. A Cylink abre mão de todos seus direitos proprietários sobre o SAFER + e consigna este algoritmo ao domínio público. O SAFER + é baseado na família de cifras SAFER existentes, a qual compreende as cifras SAFER K-64, SAFER K-128, SAFER SK-64, SAFER SK-128, e SAFER SK-40. O comprimento de bloco de todas as cifras da atual família SAFER é de 64 *bits*, enquanto que o comprimento da chave é de 40 ou 64 ou 128 *bits* conforme indicado no nome da cifra, ou seja diferem da SAFER K-64 apenas nos esquemas da chave e no número de iterações usado. A estrutura de cifragem do SAFER + utiliza um comprimento de bloco de 16 *bytes* (128 *bits*), com comprimento da chave de 128 ou 192 ou 256 *bits*, devendo ter um número de 8, 12 ou 16 iterações respectivamente, conforme o comprimento da chave utilizada. A estrutura de decifragem é muito semelhante à de cifragem, com os mesmos comprimentos de bloco e de chave, porém não são operações idênticas.

SAFER+ não é nem uma cifra de Feistel nem uma cifra de permutação-substituição, mas sim uma cifra de substituição/transformação linear. Observa-se que a estrutura de iterações do SAFER + obedece a mesma estrutura da família SAFER K-64, onde a Transformação Linear Inversível é baseada também, na Pseudo-Transformada de Handamard (PHT), sendo empregado o *Embaralhamento Armênio*, que consiste numa permutação particular de coordenadas. Um estudo exaustivo do SAFER + mostrou que todas as características de 5 iterações têm probabilidade de quebra significativamente menor que 2^{-128} (porém este não é o caso para apenas 4 iterações) contra um ataque. O SAFER + com seis ou mais iterações (mas nunca menos) é seguro contra criptoanálise diferencial, mas para uma margem de segurança desejável, escolheu-se 8 iterações para o SAFER + com o esquema de chave de 128 bits, que provêem uma enorme margem de segurança, inclusive contra a criptoanálise linear [10].

3.5. O SAFER em *software*

Este pacote de *software* é uma implementação do algoritmo de cifra de bloco orientado a *byte*. Quatro versões do algoritmo são implementadas, a saber: SAFER K-64, SAFER K-128, SAFER SK-64 e SAFER SK-128. Os numerais 64 e 128 correspondem ao comprimento da chave selecionada pelo usuário. A letra "K" é associada à palavra chave (em inglês *key*), e nas novas versões implementadas "SK" significa *fortalecimento da chave*. A *interface* com o usuário é também fornecida para os sistemas UNIX, MS-DOS, VMS e outros. Qualquer compilador baseado em ANSI C ou C++ pode ser usado para compilar o código fonte. Além disso, o comportamento da entrada-saída dos programas executáveis é idêntico, isto é, o comando do usuário da função 'safer' é compatível em qualquer computador [12]. O código fonte pertence ao domínio público.

3.6. Sistema de gerenciamento de chaves

Apresentaremos nesta seção, o Sistema de Gerenciamento de Chaves (SGC), desenvolvido para a PMPE, cujo objetivo principal é o armazenamento de chaves públicas em um banco de dados denominado Catálogo Público Custodiado (CPC), o qual fornece subsídio para a computação de uma chave secreta comum, necessária para efetivar a troca sigilosa de mensagens entre quaisquer dois usuários de uma rede, através da utilização da cifra SAFER. Para tanto, daremos um enfoque inicial nas definições de funções unidirecionais e sistema de distribuição pública de chaves de Diffie-Hellman [11], que foram os princípios utilizados para a criação do SGC.

3.6.1. O sistema de distribuição pública de chaves de Diffie-Hellman

O sistema sugerido por Diffie-Hellman para a criação de uma chave secreta comum, foi bastante original e inteligente, pois através deste sistema pode-se trocar chaves secretas sem a necessidade de um canal seguro, e baseia-se na (conjecturada) propriedade unidirecional da exponenciação discreta [11]. Sua segurança consiste na dificuldade de se calcular logaritmos discretos em corpos finitos, comparado com a facilidade de se calcular exponenciais no mesmo corpo finito. Suponhamos que $f(x) = \alpha^x \bmod p$, onde p é um número primo grande (com pelo menos 100 dígitos decimais), e α um elemento primitivo do grupo multiplicativo de $GF(p)$, onde $f(x) = y$ é uma função *verdadeiramente* unidirecional e de conhecimento de todos os usuários autorizados a acessar o sistema.

Diffie e Hellman postularam a existência de um CPC, contendo um banco de informações autênticas, com os valores de $f(x) = y$ não-confidenciais, que está disponível para todos os usuários cadastrados. Digamos que temos dois usuários, A e B, autorizados a acessar o sistema. Após a identificação ao SGC e o

respectivo *login*, cada usuário escolhe uma chave privada, sejam elas x_A e x_B respectivamente, para computar cada um o valor da sua chave pública. Estas chaves públicas são, então, armazenadas no CPC, como os pares (A, y_A) e (B, y_B), correspondendo respectivamente aos usuários A e B. Suponhamos, ainda, que os usuários A e B desejam se comunicar secretamente, então

1. O usuário A consulta no CPC a chave pública de B, y_B e , vice-versa, o usuário B consulta no CPC a chave pública de A, y_A.

2. O usuário A irá computar a chave secreta comum K, elevando a chave pública de B, y_B , a um expoente igual a sua chave privada x_A. De modo análogo, o usuário B procede para computar a chave comum usando y_A e x_B.

Este número computado da chave K, que tanto o usuário A como o usuário B podem calcular, é a chave secreta comum de ambos, a qual eles podem agora usar como a chave secreta em um criptosistema convencional de chave secreta. O que o esquema de Diffie-Hellman fornece é portanto um modo público de distribuir chaves secretas, e este esquema é usualmente chamado de Sistema de Diffie-Hellman de Distribuição Pública de Chaves. Um ataque a este sistema é inviável se a exponenciação discreta for realmente unidirecional. Ainda não se tem notícia de um ataque ao sistema de Diffie-Hellman que não fosse computacionalmente equivalente a computar logaritmos discretos, nem alguém conseguiu ainda provar que todos ataques a este sistema são computacionalmente equivalentes a computar logaritmos discretos. Este é, portanto, geralmente considerado como um dos melhores sistemas [2], [5].

4. RESULTADO EXPERIMENTAL

Apresentaremos, agora, através de um exemplo, a funcionalidade do SGC, que foi desenvolvido, para aplicabilidade na PMPE. O SGC, tem por função a criação de uma chave pública dos usuários cadastrados e autorizados a acessar o sistema, gerando conseqüentemente um banco de dados onde são armazenados os pares Usuário e Chave-Pública correspondente, o qual denominaremos de Catálogo Público Custodiado (CPC). A chave pública, gerada e armazenada no CPC, deve sofrer atualizações periódicas, conforme determinação do gerente do sistema (administrador). O administrador do sistema é o único responsável pelo cadastro (inclusão e exclusão) dos usuários, e pela alteração dos valores das constantes α e p para o cálculo da função $f(x) = y$. No CPC estão disponíveis as chaves públicas, $y = \alpha^x \mathrm{mod} p$, dos usuários. Se um usuário A deseja se comunicar com o usuário B; A precisa recuperar a chave pública de B e gerar a sua chave secreta comum. A pode, então, cifrar uma mensagem, através do SAFER, com a chave secreta comum e enviá-la para B. B pode recuperar a chave pública de A no CPC, e gerar a sua chave secreta comum. Cada usuário deve ter uma única chave privada, e nenhuma comunicação prévia é necessria para o envio da mensagem. Temos, ainda no SGC, um *link* com o SAFER, facilitando o transporte dos dados obtidos da chave secreta comum para o SAFER. O SGC, obedece os princípios formulados por Diffie e Hellman em seu sistema de distribuição pública de chaves. Utilizamos a função, $f(x) = y = \alpha^x \mod p$, onde x é o valor da chave-privada escolhida secretamente pelo usuário; y é o valor da chave-pública obtida pelo cálculo de $f(x)$; α é a raiz primitiva, geradora de todos os elementos não-nulos do grupo multiplicativo do corpo finito $GF(p)$; p é um número primo grande (com pelo menos 100 dígitos decimais) e $(p-1)/2$ também é um número primo [11]. Os valores de α e p são fixos, variando apenas o valor da chave privada x do usuário. No entanto, em períodos predeterminados, os valores de α e p devem ser alterados pelo administrador do sistema dificultando, assim, possíveis ataques.

4.1. Utilização do gerenciamento de chaves

1. Inicialmente, solicitamos a entrada no SGC.

2. Em seguida, o sistema solicita a matrícula e a senha do usuário, que caso já esteja cadastrado, possibilitará ser executado o seu *login*. No nosso exemplo, o acesso será do próprio administrador a fim de ilustrarmos melhor os recursos disponíveis.

3. Após efetuar o *login* no SGC, acessamos a tela principal do sistema, onde temos disponíveis as opções de Cadastro, CPC, SAFER, Chave Secreta, MAPLE e Administração.

4. Os recursos disponíveis do administrador são o cadastro de usuários e a possibilidade de alteração das constantes α e p da função $f(x) = \alpha^x \mod p$.

5. Temos ainda no cadastro de usuários um campo de pesquisa para controle do administrador, com as opções de exclusão, inclusão e alteração, o nível estipulado no cadastro para o administrador é 1, enquanto para os demais usuários é 2.

6. Suponhamos agora, que Adriana deseje enviar uma mensagem cifrada para Bruno. O procedi-

mento inicial é Adriana buscar no CPC, o valor da chave pública de Bruno. Assim que for localizada a chave pública, Adriana a seleciona e o sistema executa um *link* para a tela da chave secreta, ou se preferir, pode-se clicar no menu, campo chave secreta. Caso o nome de Bruno seja clicado no CPC, é realizado um *link* para a Chave Secreta, com o transporte respectivo do nome; Adriana digita, então, a sua chave privada e em seguida clica em calcular, obtendo assim o valor da chave secreta comum, necessária para cifrar a mensagem no SAFER.

7. Já tendo selecionado o arquivo da mensagem confidencial, o qual Adriana deseja cifrar e enviar a Bruno, o sistema faz um *link* para o SAFER, e executa o comando [12] necessário para cifrar a mensagem:

   $C: \ SAFER > safer - e - ecb$

   $-k \ \ 9,13438523331814E+46$

   $COPOM.doc \quad COPOM.cry$

8. Para decifrar o arquivo COPOM.cry e recuperar o texto original, executamos o seguinte comando no SAFER:

   $C: \ SAFER > safer \ -d$

   $-k \ \ 9,13438523331814E+46$

   $COPOM.cry \ \ COPOM.ori$

   onde a chave secreta comum para decifragem foi calculada pelo receptor da mensagem, Bruno, ao verificar no CPC o valor da chave pública de Adriana e computar a chave secreta através da exponenciação discreta realizada pelo sistema, em que a chave pública de Adriana é "elevada" à chave privada de Bruno.

5. REFERÊNCIAS

[1] K. G. Pinto, *Proteção criptográfica na rede de computadores da Polícia Militar de Pernambuco, um estudo de caso*, Dissertação de Mestrado, Departamento de Eletrônica e Sistemas, UFPE, agosto de 2000.

[2] J. L. Massey, *Cryptography: Fundamentals and Applications*. ATS Seminars, Zurich, 1997.

[3] B. Schneier, *Applied Cryptography*. John Wiley & Sons, 2a edição, 1996.

[4] J. L. Massey, "An Introduction to Contemporary Cryptology". Proceeding of the IEEE, vol. 76, n. 5, pp. 533-549, May 1988.

[5] V. C. da Rocha Jr., *Uma Introdução à Criptografia*. XI Simpósio Brasileiro de Telecomunicações, Texto de Minicurso. Natal, RN, setembro, 1993.

[6] J. L. Massey, "SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm". R. Anderson, editor, Fast Software Encryption, Lecture Notes in Computer Science, No. 809, pages 1-17, New York: Springer, Jan. 1994.

[7] J. L. Massey, G. Khachatrian e M. Kuregian, "Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity and Encryption (NESSIE), 26 September 2000.

[8] J. L. Massey, "SAFER K-64: One Year Later". B. Preneel, editor, Fast Software Encryption, Lecture Notes in Computer Science, No. 1008, pages 212-241, Heidelberg and New York, 1995. Springer.

[9] J. L. Massey, "Announcement of a Strengthened Key Schedule for the Cipher SAFER". ETH Zurich, Set., 1995.

[10] V. C. da Rocha Jr., "SAFER +" , Seminário do Grupo de Pesquisa em Comunicações - CODEC, Depto. de Eletrônica e Sistemas - UFPE, 1999.

[11] W. Diffie e M. Hellman, "Privacy and Authentication: An Introduction to Cryptography", Proc. IEEE, vol. 67 (3) pp. 397-427, Mar. 1979.

[12] R. Demoliner, "Software implementation of SAFER". ETH, Zurich, 1995.