SISTEMAS DE CHAVE PÚBLICA: A CRIPTOGRAFIA DOS ANOS 80

Inhaúma Neves Ferraz

Na década de 1980 duas tecnologias extremamente dinâmicas, a das telecomunicações e a da computação, começaram a se unir dando surgimento a uma terceira, a teleinformática. As conseqüências desse processo vêm sendo chamadas de "informatização da sociedade", tendo sido precisamente analisadas no célebre "Rapport Nora".[1]

Nessa ocasião, projetaram-se as redes públicas de comunicações de dados. O escopo destas redes abrangia ligações computador-computador, computador-usuário e usuário-usuário. O impacto dessas redes na vista pública e privada tende a revolucionar a vida das comunidades.

Como exemplos de mensagens a fluir por estas redes pode-se citar contatos e contratos comerciais entre usuários que não se conheciam anteriormente, cotações de produtos e serviços, ordens de pagamento, consultas médicas, catálogos de produtos, correspondência pessoal etc.

As redes públicas de comunicações de dados foram projetadas para alguns milhares de usuários, podendo este número chegar a casa dos milhões. Além disso a transmissão por microondas deveria ser utilizada em larga escala. Desde que, muito embora a intercepção de transmissão por fio seja considerada criminosa em todo o mundo, a rádio-escuta não é atividade ilegal, os projetistas daquelas redes defrontavam-se com graves problemas de confiabilidade. As comunicações deveriam apresentar condições de ser sigilosas e permitir autenticação de mensagens evitando o "trote" e a sabotagem digital.

Problemas de tal tipo têm sido enfrentados, há séculos, por meio de técnicas criptográficas. Muito embora algumas dessas técnicas sejam de inegável eficiência, elas têm se valido da rígida estrutura hierárquica das corporações

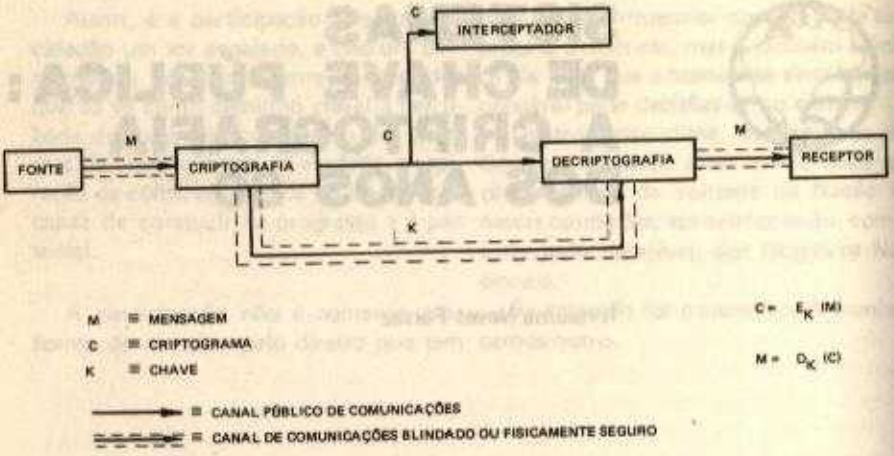

FIGURA 1

FLUXO DE INFORMAÇÕES EM UM SISTEMA DE PRIVACIDADE CRIPTOGRÁFICA

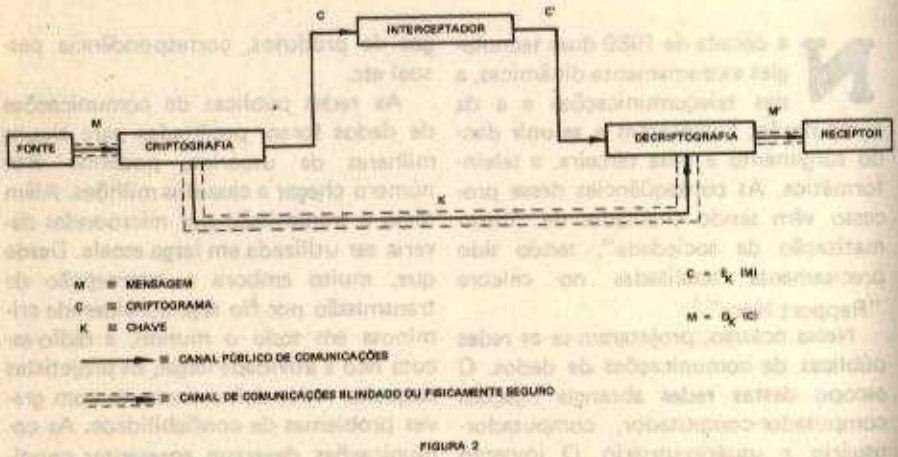

FIGURA 2

FLUXO DE INFORMAÇÕES EM UM SISTEMA DE AUTENTICAÇÃO CRIPTOGRÁFICA

que as utilizam (Governos, Forças Armadas, grandes empresas etc). A aplicação das técnicas criptográficas tradicionais, no caso em epígrafe, seria inviável pela enorme complexidade dos problemas administrativos de gerenciamento de chaves para milhares (ou milhões) de assinantes da rede.

Diversos centros de pesquisa norte-americanos dedicaram-se ao estudo da segurança das informações em redes públicas em comunicações de dados. Em

1976 dois pesquisadores da Universidade de Stanford[2] conseguiram formalizar o problema matemático envolvido. Deste trabalho e de outros, nascia a criptografia de chave pública, o maior avanço conceitual no campo da criptografia desde o surgimento da substituição polialfabética da Renascença [3, pg 153]*.

SISTEMAS CRIPTOGRÁFICOS

Um sistema criptográfico é uma coleção de pares consistindo cada um deles de uma função criptográfica E_K e de uma função decriptográfica D_K. A primeira delas transforma mensagens em criptogramas e a última transforma criptogramas em mensagens. Denomina-se chave o parâmetro K que seleciona a transformação a ser empregada. Chamando de M uma mensagem e de C o criptograma correspondente, os pares E_K e D_K devem ser tais que

$$C = E_K\ (M)$$

$$D_K\ (C) = D_K(E_K(M)) = M$$

para toda mensagem M e toda chave K.

Os processos criptográficos clássicos caracterizam-se por um canal seguro de comunicações (representado por um portador de confiança ou por correspondência registrada, por exemplo) unindo as partes que se comunicam. Por este canal era feita a distribuição de chaves. A partir daí, a comunicação processava-se através de canais inseguros. As figuras 1 e 2 ilustram um sistema criptográfico clássico assegurando privacidade e autenticação, respectivamente.

As funções E_K e D_K são de tal natureza que, uma vez conhecida uma delas, a outra é facilmente computável.

A existência de um canal seguro de comunicações era incompatível com a filosofia das redes públicas de comunicações de dados.

A característica marcante dos sistemas criptográficos de chave pública [4, pg 131] consiste no fato de cada usuário da rede revelar *publicamente*, por meio de um catálogo, sua função criptográfica e manter secreta sua função decriptográfica. Quando o usuário A desejar remeter sigilosamente a mensagem M ao usuário B deve transmitir o criptograma.

$$C = E_B\ (M)$$

Todos os usuários (e os eventuais interceptadores) conhecem E_B, porém, só o usuário B conhece D_B podendo fazer

$$D_B(C) = D_B\ (E_B\ (M)) = M$$

A essência das autenticações (ou assinaturas) é que todas as pessoas podem reconhecê-las, porém, só a pessoa autorizada poderá produzi-las.

Supondo que o usuário A desejasse autenticar uma mensagem M, destinada a qualquer usuário, obtendo uma mensagem assinada S, deveria fazer

$$S = D_A\ (M)$$

A autenticidade de tal mensagem assinada provém do fato de D_A ser privativa do usuário A.

A figura 3 ilustra um sistema criptográfico de chave pública.

Com a formulação matemática do problema começa a sua solução. Com a formalização do problema metade do caminho está percorrida. A formalização do problema caracterizou as seguintes propriedades necessárias às funções E_K e D_K para os sistemas em tela [2, pg 648] [5, pg 15].

* *Refere-se ao nº da página de obra citada na Bibliografia.*

FIGURA 3

FLUXO DE INFORMAÇÕES EM UM SISTEMA DE PRIVACIDADE CRIPTOGRÁFICA UTILIZANDO SISTEMAS DE CHAVE PÚBLICA

1) Para cada $K \in [K]$ (espaço de chaves) D_K é a "inversa à esquerda" de E_K, ou seja $D_K(E_K(M)) = M$
2) Para cada $K \in [K]$ e $M \in [M]$ (espaço de mensagens) os valores $E_K(M)$ e $D_K(M)$ são de fácil computação.
3) Para quase todo $K \in [K]$ é computacionalmente impraticável obter um algoritmo de fácil computação que, a partir de E_K, determine o equivalente a D_K.

4) Para todo $K \in [K]$ é possível gerar o par de funções inversas E_K e D_K.

Quando se deseja autenticar mensagens o sistema deve ainda possuir a característica abaixo.

5) Para cada $K \in [K]$, E_K é a inversa à esquerda de D_K, ou seja

$$E_K(D_K(M)) = m$$

Para que atenda à propriedade 3 é preciso que uma função seja de mão única [2, pg 650]. Tais funções podem ser facilmente computáveis, porém, suas inversas são de computação inviável (no mesmo sentido em que a trajetória avião-solo, de um pára-quedista, não tem inversa viável: não há quem possa, da observação da queda de um pára-quedista aprender a saltar do solo para um avião em vôo).

O estudo de tais funções e sua classificação pertence a um ramo da ciência denominado Teoria da Complexidade Computacional.

Uma vez tendo sido formalizadas as propriedades características dos sistemas criptográficos, a concepção de novos sistemas deixou de ser assunto esotérico ou de engenhosidade e passou a ser tema de pesquisa bibliográfica. Surgiram, então, os sistemas de Rivest, Shamir e Adleman[6], de Merkle e Hellman[7], de Mc Eliece[8] e vários outros. Uma característica comum a estes sistemas é que exigem, para criptoanálise exaustiva de uma intercepção, o processamento constante dos mais rápidos computadores hoje existentes, pelo período mínimo de centenas (ou milhares) de anos, mesmo conhecendo a função E_K utilizada!

SITUAÇÃO ATUAL

A inerente dificuldade de atendimento dos requisitos criptográficos formalizados, a ousadia dos esquemas propostos e a sua elegância vêm atraindo para a criptografia razoável número de matemáticos de alto nível.

Existe hoje, pela primeira vez na História, uma rede informal de cientistas, fora do Governo, que podem "fazer criptografia" de primeira linha e que trocam informações entre si de tal forma que os estudos crescem de maneira acelerada [3, pg 154].

Os sistemas criptográficos mais destacados deste século (máquinas de rotor, sistema de Vernam, sistemas tipo Lúcifer e sistemas criptográficos de chave pública) foram criados por amadores. É de se esperar que este fenômeno tenda a se ampliar.

Estes estudiosos são obstinados inimigos do sigilo. Baseiam-se em proposições formais que demonstram, desde 1881, que a segurança da chave é a única que importa [9, pg 235] e em exemplos históricos de que a homologação de sistemas criptográficos mantidos secretos significa apenas que os projetistas daqueles sistemas não conseguiram (ou não desejaram) quebrá-los [10, pg 421]. É famoso o caso da máquina ENIGMA, tida como segura pelo Dr. Vauk, do OKW alemão, e decifrada pelas máquinas de Alan Turing [11, pg 382].

Uma das assertivas fundamentais de tal grupo é que a criptografia não é mais um monopólio do Governo [3, pg 158].

Tal ponto de vista tem irritado os profissionais. Considerando que, antes do advento da chave pública e do sistema DES, praticamente todas as funções criptográficas eram de mão dupla, bastava conhecer a chave para quebrar o sistema ou, ainda mais, bastava conhecer tipo de sistema para começar a quebrá-lo. Nestas circunstâncias o sigilo era vital e o próprio recrutamento profissional baseava-se mais no gosto pelo sigilo e na discreção dos candidatos do que na sua habilidade para lidar com algoritmos.

Não seria natural que tais pessoas vissem com bons olhos a invasão de sua seara por irreverentes esgrimistas de teoremas.

Em 1979 o Almirante Bobby Inman, então Diretor da NSA, foi o primeiro diretor daquela Agência a buscar uma forma de diálogo com a comunidade acadêmica. Embora reconhecendo que a criptografia não era mais monopólio do Governo, buscava disciplinar a disseminação das informações técnicas criptográficas não-governamentais[12].

ESTUDOS CRIPTOGRÁFICOS NO INSTITUTO MILITAR DE ENGENHARIA

O Instituto Militar de Engenharia não tem, e nunca teve, missões criptográficas. Ocorre que tem por missão formar Engenheiros de Sistemas e, dentre as matérias preconizadas pela Association for Computing Machinery para a formação em Computação, estão a Álgebra de Estruturas Discretas, a Teoria da Informação e a Teoria da Codificação. Pela natural vocação profissional dos alunos militares, vem o Instituto Militar de Engenharia estudando criptografia, sempre através de literatura ostensiva vendida *livremente* no mercado norte-americano.

CONCLUSÕES

O presente trabalho pretende divulgar, no âmbito militar, algumas notícias

sobre o que se está fazendo hoje em dia no campo da criptografia não-governamental.

Procurou-se mostrar que houve uma mudança de enfoque, tendo a Matemática ocupado grande parte da área onde dominavam a engenhosidade e o sigilo convencional.

Muito embora as necessidades militares transcendam as necessidades comerciais, o grau de sigilo dos esquemas discutidos é tremendamente superior ao proporcionado, atualmente, pelos sistemas empregados nos pequenos e médios escalões da maioria dos Exércitos e, portanto, merece a nossa consideração.

BIBLIOGRAFIA

1. Nora, Simon e Minc, Alain — L'Informatisation de la Societé — Relatório do Inspetor Geral das Finanças de França ao Presidente da República Francesa — Paris — Janeiro de 1978.
2. Diffie, Whitfield e Hellmann, Martin E. — New directions in cryptography — IEEE Transactions on Information Theory, Vol IT-22, nº 6, pgs 644-654.
3. Kahn, David — Cryptology goes public — Foreign Affairs, 58, nº 1 — pgs 141-159, 1979.
4. Hellman, Martin E. — The mathematics of public-key cryptography — Scientific American — Vol 241, nº 2, pgs 130-140. Agosto de 1979.
5. Ferraz, I. N. e Barbosa, Maria Regina S. — Introdução aos Sistemas Criptográficos de Chave Pública — Anais do 7º Seminário Integrado de Software e Hardware Nacionais, pgs 13-18 — Campinas — Julho de 1980.
6. Rivest, Ronald L., Shamir, Adi e Adleman, E. — On digital signatures and public key cryptosystems — Communications ACM, Vol 21, pgs 120-126. Fevereiro de 1978.
7. Merkle, R. C. e Hellmann, Martin E. — Hiding information and signatures in trapdoor knapsacks — IEEE Transactions on Information Theory — Vol IT-24, nº 5, pgs 525-530 — Setembro de 1978.
8. Mc Eliece, R. J. — A Public-key Cryptosystem Based On Algebraic Coding Theory — DSN Progress Report — pgs 114-116 — Fevereiro de 1978.
9. Kahn, David — The codebreakers, the story of secret writing — Mc Millan — New York — 1967.
10. Diffie, Whitfield e Hellmann, Martin E. — Privacy and authentication: an introduction to cryptography — Proceedings IEEE — Vol 67, nº 3, pgs 397-427. Março de 1979.
11. Deavours, C. A. e Reeds, James — The enigma — Part I: Historical Perspectives — Cryptologia — Vol, nº 1 — Albion College — Albion — 1979.
12. Inman, B. R. — The NSA Perspective on Telecommunications Protection in the Governmental Sector — Cryptologia — Vol 3, nº 3 — Albion College — Albion — Julho de 1979 (republicação de SIGNAL, The Official Journal of the Armed Services Communications and Electronic Association — Março de 1979).

O Maj Inhaúma Neves Ferraz foi declarado Aspirante a Oficial da Arma de Engenharia em 1961. Em 1967 formou-se Engenheiro de Construção no Instituto Militar de Engenharia. É licenciado em Matemática pela Faculdade de Filosofia da Universidade Federal do Rio de Janeiro, Mestre em Ciências em Engenharia Mecânica pela Escola Federal de Engenharia de Itajubá, Mestre em Engenharia de Sistemas (Informática) pelo Instituto Militar de Engenharia e está em tese de doutoramento pelo Instituto Tecnológico de Aeronáutica. É Oficial do Quadro de Engenheiros Militares estando comissionado como Professor do Instituto Militar de Engenharia. Atualmente leciona Estruturas de Informação e chefia o Centro de Processamento de Dados do Instituto Militar de Engenharia.