Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Especialização em Gestão de Segurança da Informação e Comunicações

EDILSON FERNANDES DA CRUZ

A CRIPTOGRAFIA E SEU PAPEL NA SEGURANÇA DA INFORMÇÃO E DAS COMUNICAÇÕES (SIC) – RETROSPECTIVA, ATUALIDADE E PERSPECTIVA

Orientador: Professor João José Costa Gondim

Brasília/DF, Julho de 2009.

A CRIPTOGRAFIA E SEU PAPEL NA SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES (SIC) – RETROSPECTIVA, ATUALIDADE E PERSPECTIVA

EDILSON FERNANDES DA CRUZ

Monografia de Especialização submetida e aprovada pela Universidade de Brasília como parte do requisito parcial para obtenção do certificado de Especialista em Ciência da Computação: Gestão de Segurança da Informação e Comunicações.

Professor João José Costa Gondim (Orientador), Mestre
Universidade de Brasília

Professor Jorge Henrique Cabral Fernandes, Doutor
Universidade de Brasília

Professora Priscila A. S. M. Barreto, Doutora
Universidade de Brasília

Brasília, Julho de 2009

A minha esposa Jackie e meu filho Felipinhu,
modelos de desvelo e dedicação, razões de
uma existência.

AGRADECIMENTOS

Muitos depositaram em mim sua confiança e contribuíram para que este trabalho adquirisse forma e se materializasse a contento. Sou-lhes grato a todos, profundamente.

Contudo, até por dever de consciência, não poderia deixar de manifestar meu reconhecimento, minha gratidão e meu apreço especiais ao meu caríssimo irmão, Nilson Fernandes da Cruz, e aos meus prezados amigos Marlos Ribas Lima e Luiz Fernando da Cunha, todos Oficiais de Inteligência. Sua confiança e seu incentivo incondicionais impulsionaram mais esta incursão na infinda escalada rumo ao conhecimento.

Em particular, meus agradecimentos também ao Gabinete de Segurança Institucional da Presidência da República (GSIPR), nas figuras da Agência Brasileira de Inteligência (Abin) e da Secretaria de Acompanhamento e Estudos Institucionais (Saei), que me permitiram mais esta oportunidade de especialização profissional, aperfeiçoamento intelectual e crescimento espiritual.

Tributo especial ao Oficial de Inteligência Wilson Roberto Trezza, diretor-geral em exercício da Abin neste momento em que redijo, cujo apoio despertou novo ânimo e incentivou a jornada até aqui e adiante.

Se hoje sou ou estou uma pessoa melhor, ou pelo menos mais esclarecida, devo-lhes a todos.

"Assim como a informação se constitui em um bem cada vez mais valioso, e na medida em que a revolução das comunicações muda a sociedade, também o processo de codificação de mensagens, conhecido como criptografia, desempenha papel cada vez mais importante na nossa vida diária."[1]

Adaptado de Simon Singh
(*The Code Book*, 1999)

[1] "*As information becomes an increasingly valuable commodity, and as the communications revolution changes society, so the process of encoding messages, known as encryption, will play an increasing role in everyday life*."

RESUMO

Esta monografia apresenta um estudo sobre a Criptografia e seu papel na Segurança da Informação e das Comunicações (SIC) – retrospectiva, atualidade e perspectiva. Começa pela definição de criptografia, na tentativa de explicar o que vem a ser essa técnica. A seguir, apresenta breve história da criptografia e discute a sua evolução, desde as mais remotas origens. Também mostra a importância da criptografia para a segurança da informação e das comunicações. Na seqüência, analisa os tipos de criptografia em uso nos dias de hoje e examina onde e como estão sendo usados. Finalmente, apresenta a evolução da criptografia no Brasil e, antes de concluir, investiga o que o futuro reserva para a criptografia e que avanços ainda pode incorporar.

Palavras-chave: cifra, código, criptoanálise, criptografia, escrita secreta, espionagem, esteganografia, segurança da informação e das comunicações, sigilo.

ABSTRACT

This monography presents a study about Cryptography and its role in Information and Communications Security – historical aspects, actuality and perspective. It begins by the definition of cryptography, trying to explain what this technique means. Afterwards, it presents a brief history of cryptography and discusses its evolution, since the most remote origins. It also shows the importance of cryptography for information and communications secutiry. Subsequently, it analyzes the types of cryptography that are in use today and examines where and how they are being used. Finally It presents the evolution of cryptography in Brazil and, before concluding, it investigates what the future reserves for cryptography and what advances it may still incorporate.

Key words: cipher/cypher, code, confidentiality, cryptanalysis, cryptography, espionage, information and communications security, secrecy, secret writing, stenography.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

1 **ABIN**: Agência Brasileira de Inteligência.

2 **ABNT**: Agência Brasileira de Normas Técnicas.

3 **AC-RAIZ**: Autoridade Certificadora Raiz.

4 **AES**: *Advanced Encryption Standard* (Padrão Avançado de Criptografia).

5 **APF**: Administração Pública Federal.

6 **ATIS**: *Alliance for Telecommunications Industry Solutions* (Aliança para Soluções da Indústria de Telecomunicações).

7 **CDN**: Conselho de Defesa Nacional.

8 **CEPESC**: Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações.

9 **CERT.br**: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

10 **CGIBR**: Comitê Gestor da Internet no Brasil.

11 **CG-ICP**: Comitê Gestor da ICP-Brasil.

12 **CNSS**: *Committee on National Security Systems* (Comitê sobre Sistemas de Segurança Nacional).

13 **CPB**: Código Penal Brasileiro.

14 **CPQD**: Centro de Pesquisa e Desenvolvimento em Telecomunicações.

15 **CREDN**: Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, República Federativa do Brasil.

16 **DES**: *Data Encryption Standard* (Padrão de Criptografia de Dados).

17 **DICA**: Disponibilidade, Integridade, Confidencialidade e Autenticidade.

18 **DISA**: Disponibilidade, Integridade, Sigilo e Autenticidade.

19 **DSIC**: Departamento de Segurança da Informação e Comunicações.

20 **ESNI**: Escola Nacional de Informações.

21 **EUA**: Estados Unidos da América.

22 **GC&CS**: *Government Codes and Cypher School* (Escola Governamental de

Códigos e Cifras).

GSIPR: Gabinete de Segurança Institucional da Presidência da República.

IA: *Information Assurance* (Garantia da Informação).

ICP Brasil: Infra-Estrutura de Chaves Públicas Brasileira.

INFOSEC: *Information Systems Security* (Segurança de Sistemas de Informação).

ITI: Instituto Nacional de Tecnologia da Informação.

ITS: *Institute for Telecommunication Sciences* (Instituto de Ciências de Telecomunicação).

MI-5: *Military Intelligence 5* (5ª Seção da Inteligência Militar), o Serviço de Segurança e Contra-Inteligência do Reino Unido.

MI-6: *Military Intelligence 6* (6ª Seção da Inteligência Militar), o SIS.

MRE: Ministério das Relações Exteriores.

NIST: *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia).

NSA: *National Security Agency* (Agência de Segurança Nacional).

NTIA: *National Telecommunications and Information Administration* (Administração Nacional de Informação e Telecomunicações).

PNPC: Programa Nacional de Proteção ao Conhecimento.

RENASIC: Rede Nacional de Segurança da Informação e Criptografia.

RSAS: Regulamento para Salvaguarda de Assuntos Sigilosos.

RSISN: Regulamento para a Salvaguarda das Informações que Interessam à Segurança Nacional.

SI: Segurança da Informação.

SIC: Segurança da Informação e das Comunicações.

SIS: *Secret Intelligence Service* (Serviço de Inteligência Secreto), o MI-6.

SNI: Serviço Nacional de Informações.

TI: Tecnologia da informação.

TIC: Tecnologia(s) de Informação e Comunicações.

TSE: Tribunal Superior Eleitoral.

UNB: Universidade de Brasília.

VoIP: Voz sobre IP (*Internet Protocol*).

VOLP: Vocabulário Ortográfico da Língua Portuguesa.

GLOSSÁRIO

Assinatura Digital: transformação matemática de uma mensagem por meio da utilização de uma função matemática e da criptografia assimétrica do resultado desta com a chave privada da entidade assinante.

Autenticação: processo utilizado para confirmar a identidade de uma pessoa ou entidade, ou para garantir a fonte de uma mensagem. A autenticidade visa a assegurar a veracidade e consistência de dados e/ou informações, assim como a identidade e fidedignidade da fonte e do usuário, ou do emissor e do receptor.

Autoridade Certificadora – AC: entidade que emite certificados de acordo com as práticas definidas.

Certificado de Chave Pública: declaração assinada digitalmente por uma AC, contendo, no mínimo:

- o nome distinto (DN – *Distinguished Name*) de uma AC, que emitiu o certificado;
- o nome distinto de um assinante para quem o certificado foi emitido;
- a Chave Pública do assinante;
- o período de validade operacional do certificado;
- o número de série do certificado, único dentro da AC; e
- uma assinatura digital da AC que emitiu o certificado com todas as informações citadas acima.

Chave Privada: chave de um par de chaves mantida secreta pelo seu dono e usada no sentido de criar assinaturas para cifrar e decifrar mensagens com as Chaves Públicas correspondentes.

Chave Pública: chave de um par de chaves criptográficas que é divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente ou, dependendo do algoritmo criptográfico assimétrico utilizado, para cifrar e decifrar mensagens.

Cifração: processo de transformação de um texto original ("*plaintext*") em uma forma incompreensível ("*ciphertext*") usando um algoritmo criptográfico e uma chave criptográfica.

Confidencialidade: vide “sigilo”.

Criptografia: técnica ou conjunto de técnicas que possibilita, com o emprego de chave cifradora/decifradora, tornar ininteligíveis textos em claro e, inversamente, tornar inteligíveis textos cifrados, de forma a proteger a informação contra acesso não autorizado ao seu conteúdo.

Criptografia assimétrica, ou de chave pública: tipo de criptografia que usa um par de chaves criptográficas matematicamente relacionadas. As Chaves Públicas podem ficar disponíveis para qualquer um que queira cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente. A chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.

Criptografia simétrica, ou de chave privada: sistema que usa uma mesma chave para cifrar e decifrar a mensagem. Essa chave, portanto, deve ser de conhecimento tanto do emissor quanto do receptor.

Disponibilidade: garantia de que dados e/ou informações possam ser acessados e usados de forma ágil, confiável e oportuna. Inclui proteção contra negação de serviço.

Função *hash* criptográfico, ou **função resumo**: espécie de função randômica (aleatória), em que a entrada (*input*) é maior do que a saída (*output*). Em outras palavras, é o processo pelo qual se transformam grandes quantidades de dados em quantidades menores, por processos algorítmicos. Dessa forma, não permite que, a partir de determinados valores, se retorne à informação original. Em outras palavras, a mensagem é resumida.

Gestão de documentos: de acordo com a Política Nacional de Arquivos é o conjunto de procedimentos e operações técnicas para produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

Infra-Estrutura de Chaves Públicas – ICP: arquitetura, organização, técnicas, práticas e procedimentos que suportam, em conjunto, a implementação e a operação de um sistema de certificação baseado em criptografia de chaves públicas.

Integridade: garantia de que a mensagem não seja alterada durante a sua transferência, do emissor da mensagem para o seu receptor. Tem por fundamento evitar corrupção ou modificação não-autorizada de dados e/ou informações, em todas as suas fases de existência, isto é, geração ou produção, difusão e tramitação, uso, avaliação e destinação final (arquivamento ou eliminação).

Mensagem: registro contendo uma representação digital da informação, como um dado criado, enviado, recebido e guardado em forma eletrônica.

Não-repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria de uma mensagem ou participação em uma transação, controlada pela existência da assinatura digital que somente ele pode gerar.

Par de Chaves: chaves privada e pública de um sistema criptográfico assimétrico. A Chave Privada e sua Chave Pública são matematicamente relacionadas e possuem certas propriedades, entre elas a de que é impossível a dedução da Chave Privada a partir da Chave Pública conhecida. A Chave Pública pode ser usada para verificação de uma assinatura digital que a Chave Privada correspondente tenha criado ou a Chave Privada pode decifrar a uma mensagem cifrada a partir da sua correspondente Chave Pública.

Política de Certificação – PC: documento que estabelece o nível de segurança de um determinado certificado.

Redes: referem-se a sistemas de transmissão e podem incluir sistemas computacionais, servidores, *switches* e roteadores, além de outros recursos que permitam tráfego de sinais por fio, rádio e meios ópticos ou outros eletromagnéticos, incluindo redes de satélites, redes terrestres fixas e móveis, redes usadas para radiodifusão e televisão tradicional ou a cabo.

Registro: informação registrada em um meio tangível (um documento) ou armazenada em um meio eletrônico ou qualquer outro meio perceptível.

Segurança da Informação e das Comunicações (SIC): capacidade de um sistema de

informação, uma rede ou um sistema de gestão documental resistir a eventos acidentais e/ou ações ilícitas e/ou maliciosas que possam comprometer as características de dados/informações armazenados, processados ou em trânsito, assim como de serviços relacionados que possam ser oferecidos por esses sistemas.

Sigilo (*Confidentiality*): condição na qual dados e informações sensíveis são mantidos em segredo e divulgados apenas para as partes autorizadas e que tenham necessidade de conhecer. Pode incluir “privacidade” e se destina a prevenir/evitar revelação não-autorizada ou acidental de dados e/ou informações, garantindo que apenas os usuários reais tenham acesso ao seu conteúdo ou significado.

Sistema de informação: abrange redes de computadores e de comunicações eletrônicas, bem como dados armazenados, processados, recuperados ou transmitidos por meio dessas redes, ou que sejam essenciais a sua operação, uso, proteção e manutenção.

* * *

SUMÁRIO

1. INTRODUÇÃO

"O estudo, a busca da verdade e da beleza são domínios em que nos é consentido sermos crianças por toda a vida."

Albert Einstein

Existem parcos registros oficiais disponíveis acerca da evolução do uso da criptografia em organizações públicas no Brasil, a não ser no seio da Atividade de Inteligência, pioneira nesse ramo, que acabou se estendendo ao âmbito das Relações Exteriores e das Forças Armadas. Isto dificulta o estudo e a avaliação da matéria e, conseqüentemente, prejudica ações de diagnose, planejamento e implementação de melhorias.

Na iniciativa privada e em entidades paraestatais, há escassas informações disponíveis sobre o emprego da criptografia. Entidades que lidam com dados sensíveis à sua sobrevivência, como bancos, outras organizações econômicas ou financeiras e empresas de telecomunicações, despontam nesse setor, mas não disponibilizam esses dados, até por constituírem segredo comercial ou industrial.

Como resultado, verifica-se prejuízo à segurança da informação em termos nacionais.

Ademais, constata-se que o Estado brasileiro não utiliza criptografia de forma adequada ou no volume necessário. Não há políticas específicas a esse respeito. Como conseqüência, a gestão da segurança da informação e das comunicações nas organizações, particularmente de caráter público, tem sido prejudicada. Maior atenção é necessária.

Sem história é difícil realizar levantamento situacional, planejamento e melhoria. Uma análise histórica fornece subsídios úteis para disciplinar e estimular o uso correto dessa ferramenta. A avaliação do passado permite executar o presente e planejar o futuro.

A investigação pretérita e presente da criptografia determina que há necessidade de se adotarem ações no sentido de estimular o seu uso nos órgãos da Administração Pública Federal (APF), também a servir de exemplo para a iniciativa privada naquilo que se considerar de interesse da segurança da sociedade e do Estado.

Esforços nesse sentido iniciam-se pela sensibilização e conscientização,

independemente de grau ou nível hierárquico ou de vínculo empregatício dentro das organizações.

No presente trabalho, discorre-se sobre o surgimento e a evolução da criptografia. Aqui, busca-se explicar a importância dessa técnica para a segurança da informação e das comunicações e a necessidade de adotá-la como estratégia para auferir eficiência e eficácia na garantia de integridade, sigilo e autenticidade de dados e informações, tanto na área governamental quanto na iniciativa privada.

Durante a redação do presente trabalho, buscou-se purismo rigidamente escrupuloso na conservação da pureza do idioma pátrio, de forma a rejeitar meras transformações de caráter regencial ou sintático ou simples empréstimos de estrangeirismos, práticas comuns na área de Tecnologia(s) de Informação e Comunicações (TIC), pródiga em importar jargões e produzir neologismos por vezes ininteligíveis ou de significado dúbio ou duvidoso.

A área técnica não se preocupa com questões de redação. Costuma importar estrangeirismos, com termos esdrúxulos cujo entendimento o cidadão comum, o leigo, não consegue captar.

Procurou-se ser mais acessível. Por isso, até uma certa extravagância na colocação de ilustrações, para apresentar um visual atrativo e tornar a leitura agradável. Muitas imagens falam por si só e substituem inúmeras palavras. A intelecção é mais fácil e tranquila.

Buscaram-se, também, simplicidade e clareza, os dois pilares da redação de inteligência, de forma que a mensagem aqui transmitida seja entendida e absorvida pelo público mais diverso possível. Assim, busca-se apresentar a história e os fundamentos da criptografia, no intuito de ilustrar/instruir até os mais leigos. O objetivo principal é alertar para a importância dessa ferramenta para a proteção das informações e das comunicações, sejam governamentais ou particulares.

Durante a redação, na medida do possível, levou-se em consideração a norma culta da Língua Portuguesa, de modo que não houvesse agressão ou afronta ao que preconizam as regras gramaticais do idioma pátrio.

Incluindo esta introdução, a monografia estrutura-se em nove capítulos, além das Referências Bibliográficas ao final.

O Capítulo 2 apresenta os requisitos e pré-requisitos, traçando o objetivo, mostrando a

metodologia e apresentando as justificativas do trabalho.

O Capítulo 3 define Criptografia, após se efetuarem estudos sobre experiências nacionais e estrageiras relevantes sobre a questão.

O Capítulo 4, faz uma retrospectiva histórica da Criptografia, desde o surgimento da escrita, da qual se originou a escrita secreta, possível com o emprego de esteganografia, codificação ou da criptografia propriamente dita. Procede-se também a um breve relato sobre o secretismo que sempre cercou a criptografia e como esse fator influiu na produção literária.

O Capítulo 5 discorre sobre a Segurança da Informação e das Comunicações (SIC) e mostra a importância da Criptografia no seu contexto.

O Capítulo 6 apresenta os tipos de aplicações criptográficas.

O Capítulo 7 mostra como a Criptografia evoluiu no Brasil nos últimos 35 anos, fazendo referência às principais instituições envolvidas e programas desenvolvidos até o momento atual.

No Capítulo 8 discute-se tudo o que foi visto no trabalho, apresentando algumas sugestões, inclusive parte delas basedas em experiência profissional própria, obviamente sem fugir ao que se retrata no texto.

No Capítulo 9, procede-se à conclusão e sugerem-se soluções por meio de trabalhos futuros.

Por fim, no desfecho, as Referências Bibliográficas que foram consultadas e enriqueceram a execução deste trabalho.

2. REQUISITOS PRÉ-PESQUISA

OBJETIVO

Esta monografia objetiva, primordialmente, explicar a importância da criptografia para a segurança da informação e das comunicações e a necessidade de se adotarem estratégias e táticas criptográficas para assegurar, de forma eficiente e eficaz, integridade, sigilo e autenticidade de dados e informações, especialmente na área governamental.

Ademais, buscam-se apresentar subsídios que sirvam de instrumento de sensibilização e conscientização quanto à necessidade de adoção de sistema de gestão de segurança da informação e das comunicações, com foco no uso da criptografia para a proteção das informações e comunicações governamentais, particularmente as consideradas sensíveis e aquelas cujo sigilo seja de interesse da segurança da sociedade e do Estado.

Tendo em vista que, no âmbito da Administração Pública Federal (APF) — à qual se dirige o curso que ora concluímos —, o encarregado de coordenar as atividades de segurança da informação é o Gabinete de Segurança Institucional da Presidência da República (GSIPR), pretende-se, também, que este trabalho constitua instrumento útil ao exercício de suas atribuições, pelo menos do ponto de vista cultural e educativo quanto à importância da criptografia.

Como desdobramento, esta pesquisa visa a constituir instrumento de sensibilização e conscientização até mesmo do cidadão comum, quanto à importância da criptografia para o resguardo da inviolabilidade de informações relativas à intimidade, à vida privada, à honra e à imagem das pessoas.

METODOLOGIA

A pesquisa desenvolvida utilizou como metodologias principais a revisão bibliográfica e a análise documental, além de algumas entrevistas esporádicas feitas junto a determinados especialistas sobre assuntos específicos.

JUSTIFICATIVA

Embora este trabalho esteja focado primeiramente na criptografia, esta seria apenas parte de uma política de segurança da informação e das comunicações abrangente. Sem tal política, de longo alcance e independente de grau hierárquico ou posição funcional, qualquer alteração no estado de coisas da criptografia seria inócua ou teria pouco impacto operacional.

Além da APF, por competência legal, cabe ao governo desenvolver mecanismos no sentido de promover a segurança da informação e das comunicações também no setor privado. Os próprio órgãos governamentais não estão bem organizados para enfrentar os desafios representados pela sociedade da informação e o ambiente cibernético. Ademais, nenhuma agência governamental tem responsabilidade para promover segurança da informação e das comunicações no setor privado.

É importante que se estruturem ações integradas entre governos federal, estaduais e municipais, sem esquecer da iniciativa privada e da academia, de modo a estabelecer metas comuns para equacionar os principais problemas nas áreas de criptografia e segurança da informação e das comunicações. Atenção especial merecem itens e instalações que tenham dano potencial associado, em face da sua sensibilidade. Esses envolvem infraestruturas críticas, de segurança pública, energia, água, economia e finanças e malhas de comunicação por terra, mar e ar.

O Governo Federal tem papel fundamental no sentido de promover ativamente a segurança dos sistemas de informação e redes críticas necessárias ao bem estar da Nação. Como o Governo não dispõe de recursos humanos nem financeiros suficientes para atender às necessidades do País em termos de pesquisa e desenvolvimento, seria importante parceria com a academia e a iniciativa privada, adotando-se as devidas cautelas de segurança e sigilo. Em outros setores, caberia ao governo prover experiência, apoio e informações.

Ademais, verifica-se que no Brasil o arcabouço legal referente à criptografia é

extremamente limitado e resume-se a alguns decretos do Executivo que se restringem a fazer mera alusão a equipamentos criptográficos. Não há políticas específicas que determinem normas e regras, atribuam responsabilidades e imponham sanções quando necessárias.

Por fim, tendo em vista que criptografia constitui ferramenta de uso dual (militar e civil), há que se ter em mente que, além de servir aos interesses da segurança nacional, também pode prestar-se a atividades escusas ou ilegais. Deve-se até atentar para o fato de que surgiu da necessidade de se protegerem informações de intrusão/intromissão em assuntos particulares/privados, no terreno da espionagem. Atualmente, elementos maliciosos, como hackers, ladrões de senhas e mesmo organizações a serviço do crime organizado e terroristas, também se utilizam dessa ferramenta para trocar informações de forma sigilosa, no desenvolvimento de suas ações criminosas. O Brasil também carece de mecanismos eficazes que pelo menos minimizem tais ameaças, como, por exemplo, controle de *sofwares* criptográficos que sejam livremente disponibilizados no mercado e mecanismos de quebra de sigilo computacional.

Feitas essas considerações, no capítulo seguinte se procederá à definição de criptografia.

3. DEFINIÇÃO DE CRIPTOGRAFIA

"Definições, assim como perguntas e metáforas, são instrumentos para fazer pensar. Sua autoridade reside inteiramente na sua utilidade, não na sua correção. Usamos definições a fim de delinear problemas que desejamos investigar, ou favorecer interesses que queremos promover. Em outras palavras, inventamos definições e as descartamos na medida em que servem aos nossos propósitos."[2]

Adaptado de Neil Postman
[*Language Education in a Knowledge Context* (1980)]

Existem inúmeras definições de **criptografia** e não caberia aqui citá-las todas. Apenas para se ter idéia, levantamento estatístico feito na internet sem qualquer preocupação de "refinar a busca", com o objetivo apenas de verificar quantas vezes os vocábulos "criptografia" e seu correspondente em inglês "*cryptography*" são citados, apresentou o seguinte resultado:

Buscador / Entrada	*AOL*	globo.com	*Google*	MSN	*Yahoo*
Criptografia	310.000	206.000	1.020.000	775.000	6.790.000
Cryptography	221.000	92.100.000	5.900.000	4.290.000	30.400.000

Figura 1
Número de citações na internet de "criptografia" e "*cryptography*", por ferramenta de busca.
(Pesquisa em: 5 dez. 2008.)

Entretanto, alguns exemplos e opiniões em particular merecem menção, para situar

[2] "*Definitions, like questions and metaphors, are instruments for thinking. Their authority rests entirely on their usefulness, not their correctness. We use definitions in order to delineate problems we wish to investigate, or to further interests we wish to promote. In other words, we invent definitions and discard them as suits our purpose*s."

adequadamente a nossa linha de raciocínio e prover a fundamentação teórica necessária ao estudo que ora se apresenta.

Do ponto de vista lexicográfico, Houaiss (2007) ensina que o termo **criptografia**[3] deriva do latim moderno ***cryptographia***, formado de ***cript(o)***, do grego ***kruptós*** ("oculto, secreto, obscuro, ininteligível") mais ***-grafia***, do grego ***-graphía***, com o sentido de "escrita", do verbo grego *gráphó* ("escrever"). Segundo ele, criptografia significa, então,

> "conjunto de princípios e técnicas empr. para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; [...] em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções". (HOUAISS, 2007)

Dos Estados Unidos da América (EUA), onde a criptografia é objeto de especial atenção e assunto de interesse da segurança nacional, emanam importantes exemplos:

A *Alliance for Telecommunications Industry Solutions* (ATIS) entende que a criptografia[4] determina os métodos usados para cifração e decifração e, além disso, constitui (ATIS, 2007):

a) a arte ou ciência que se preocupa com os princípios, meios e métodos de tornar ininteligível a informação, ou de restaurar a informação cifrada, tornando-a inteligível; e

b) a disciplina que incorpora princípios, meios e métodos de transformação de dados, a fim de ocultar o conteúdo da informação, prevenir sua modificação clandestina e/ou prevenir seu uso não-autorizado;

Antes da ATIS, porém, o *Institute for Telecommunication Sciences* (ITS), ramo de pesquisa e desenvolvimento da *National Telecommunications and Information*

---

[3] CRIPTOGRAFIA. In: HOUAISS, Antonio. **Dicionário Eletrônico da Língua Portuguesa**. 2. ed. São Paulo: Ed. Objetiva, 2007. Datação do vocábulo: 1844.

[4] *CRYPTOGRAPHY*: In: ATIS Committee PRQC. ***ATIS Telecom Glossary 2007***. Estados Unidos. Disponível em: <http://www.atis.org/glossary/definition.aspx?id=6815>. Acesso em: 15 ago. 2008.

Administration (NTIA), do Departamento de Comércio, já defendia que criptografia[5] compreende os princípios, meios e métodos de tornar ininteligível a informação em claro e de restaurar a informação cifrada para uma forma inteligível (ITS, 1996);

Na mídia digital especializada, a *PC Magazine* explica que criptografia[6] é a conversão de dados em um código secreto, para transmissão através de rede pública. Segundo a revista (PC MAGANIZE, s.d.), o texto original, ou *plaintext*, é convertido em um equivalente codificado, denominado *ciphertext*, por meio de um algoritmo criptográfico. Depois, o texto cifrado é decodificado (decifrado ou decriptografado) no terminal receptor e recuperado na sua forma original, ou *plaintext*; e

De cima de toda a sua autoridade, a organização responsável pela segurança dos sistemas de informação do Governo dos EUA, a Agência de Segurança Nacional (*National Security Agency* – NSA[7]), por meio do seu Comitê sobre Sistemas de Segurança Nacional (*Committee on National Security Systems* – CNSS), estabelece, objetivamente, que criptografia[8] "é a arte ou ciência que se preocupa com os princípios, meios e métodos de tornar ininteligível um texto em claro e, inversamente, tornar legíveis informações criptografadas" (CNSS, 2006, p. 19).

Dos setores especializados brasileiros — apesar da constatação de que só recentemente esforços voltados à definição de criptografia passaram a se desenvolver com maior profundidade —, também emanam contribuições dignas de atenção:

---

[5] *CRYPTOGRAPHY*. In: Institute for Telecommunications Sciences – ITS. *Federal Standard 1037C – **Telecommunications: Glossary of Telecommunication Terms***. Boulder, Colorado, EUA: 1996. Disponível em: <http://www.its.bldrdoc.gov/fs-1037/>. Acesso em: 15 ago. 2008.

[6] *CRYPTOGRAPHY*. In: PC Magazine. ***PCMAG.COM Encyclopedia***. Estados Unidos. Disponível em: <http://www.pcmag.com/encyclopedia_term/0,2542,t=cryptography&i=40522,00.asp>. Acesso em: 1° nov 2008.

[7] A NSA, definida no seu próprio site (disponível em <http://www.nsa.gov/about/index.cfm>, acessado em 19 jul. 2008) como a "organização criptológica da América", coordena, dirige e executa atividades altamente especializadas para proteger os sistemas de informação do governo dos EUA. Ao mesmo tempo, executa ações de Inteligência de Sinais no campo externo, dispondo de capacidade para monitorar, interceptar e analisar as comunicações ao redor do Planeta.

[8] *CRYPTOGRAPHY*. In: CNSS Instruction No. 4009. ***National Information Assurance (IA) Glossary***. Ft. Meade, MD, USA: CNSS, 2006. 86 p.

A Câmara Brasileira de Comércio Eletrônico, por meio do Grupo de Trabalho de Criptografia Comercial, entende (BARRETO *et al.*, 2003) criptografia como a "aplicação de um padrão secreto de substituição dos caracteres, de maneira que a mensagem se torna ininteligível para quem não conhece o padrão criptográfico utilizado"[9];

Por sua vez, o Instituto Nacional de Tecnologia da Informação (ITI), da Presidência da República, ensina, didaticamente, que criptografia[10] significa "a arte de escrever em códigos de forma a esconder a informação na forma de um texto incompreensível" (BRASIL, 2005); e que "a informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de **cifragem**, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se **decifragem**" (destaque nosso). Acrescenta, ainda, uma peça fundamental — a chave criptográfica —, por meio da qual são realizadas as operações de **cifração** e **decifração** [que preferimos, alternativamente a cifragem e decifragem, embora Houaiss (2007) as reconheça como sinônimas]. "Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado." E arremata que, assim, "para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave";

Já o Portal ICP Brasil estabelece criptografia[11] como:

> "Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo. [...] Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem". (BRASIL, s.d.)

Além disso, em 2006 o Comitê Gestor da Internet no Brasil (CGIBR), coordenado pelo

---

[9] BARRETO, Ricardo (barretto@cff.com.br_br); LEÇA, José (jalp@cff.com.brjalp@br); MONTAGNA, Camila (cdr@cff.com.br); ARATA, Seiiti (saj@cff.com.br). **Criptografia no Brasil**. São Paulo: Câmara Brasileira de Comércio Eletrônico – Grupo de Trabalho de Criptografia Comercial, 2003. Disponível em: <http://www.camara-e.net/_upload/SLIDESCFF.PDF>. Acesso em: 3 nov. 2008.

[10] PRESIDÊNCIA DA REPÚBLICA. Instituto Nacional de Tecnologia da Informação – ITI. **CRIPTOGRAFIA.** In: **O que é Certificação Digital?** Brasília: ITI/PR, 2005. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 3 nov. 2008.

[11] CRIPTOGRAFIA. In: **DEFINIÇÕES do glossário**. Brasília: Presidência da República: ICP Brasil — Infra-estrutura de Chaves Públicas Brasileiras. Disponível em: <https://www.icpbrasil.gov.br/duvidas/glossary/criptografia?searchterm=criptografia>. Acesso em: 25 out. 2008.

GSIPR, lançou "Cartilha de Segurança na Internet"[12], produzida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), em que define criptografia como:

> "[...] ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:
>
> • autenticar a identidade de usuários;
>
> • autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
>
> • proteger a integridade de transferências eletrônicas de fundos."

Prossegue a cartilha ensinando que

> "Uma mensagem codificada por um método de criptografia deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser assinada, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada."

E finaliza sua definição afirmando que

> "Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. A chave é uma sequência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens."

Por fim, do ponto de vista da legislação brasileira, tentou-se estabelecer definição de criptografia[13], por meio de decreto, como "Disciplina que trata dos princípios, meios e métodos para a transformação de dados, de forma a proteger a informação contra acesso não autorizado a seu conteúdo". Porém, essa tentativa não vingou e o próprio Poder Executivo decidiu pela sua revogação[14] pouco mais de um ano depois. De qualquer forma, fica a idéia para consideração.

---

[12] Disponível em: <HTTP://dsic.planal.tp.gv.br/documentos/cartukg_segurança_internet.pdf>. Acesso em 30 out. 2008.

[13] CRIPTOGRAFIA. In: Decreto nº. 3.587/2000. Anexo II. Glossário. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/d3587.htm>. Acesso em: 30 out. 2008.

[14] Por meio do Decreto nº. 3.996/2001, cujo artigo 6º revoga o Decreto nº. 3.587/2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm>. Acesso em: 30 out. 2008.

Feitas essas observações, verifica-se que a criptografia, seja arte ou ciência, é um processo que se executa por meio de duas operações semelhantes e diretamente inversas: cifração e decifração. Estas significam, simplesmente, conversão e reversão. A primeira converte a informação para uma forma ininteligível; a segunda reverte-a para a sua forma original. Isso é possível com a aplicação de uma chave criptográfica ao texto.

Extraindo-se a essência dessas assertivas, pode-se esquematizar criptografia da seguinte forma (Figura 2):

Figura 2 – Esquema sintético da criptografia.
Inspirado em SCHNEIER (1996, p. 3)

Assim, para os efeitos deste trabalho, considera-se criptografia como **técnica ou conjunto de técnicas que possibilita, com o emprego de chave cifradora/decifradora, tornar ininteligíveis textos em claro e, inversamente, tornar inteligíveis textos cifrados, de forma a proteger a informação contra acesso não autorizado ao seu conteúdo.**

Para complementar, cabe breve menção à **criptoanálise**. É o conjunto de técnicas e métodos por meio dos quais se estudam ou se analisam informações cifradas, com o objetivo de, sem conhecer previamente os sistemas ou as chaves cifradoras, decifrá-las. Ou, simplesmente, como se diz na linguagem coloquial, “quebrar a cifra”. A criptoanálise, juntamente com a criptografia, constitui a **criptologia**. “Enquanto o

criptógrafo desenvolve novos métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, a fim de quebrar mensagens secretas"[15] (SINGH, 1999, p. 15).

Definida a criptografia, será feita, a seguir, uma retrospectiva mostrando aspectos históricos dessa técnica, ou arte, ou ciência, como preferem alguns estudiosos e autores.

[15] "*While cryptographer develops new methods of secret writing, it is the cryptanalyst who struggles to find weaknesses in these methods in order to break into secret messages*."

4. RETROSPECTIVA DA CRIPTOGRAFIA

"No começo, as pessoas sussurravam. Outras escutavam clandestinamente. E, dessas primitivas e rudimentares origens, evoluiu uma das mais poderosas ferramentas da inteligência e uma das mais importantes técnicas de segurança do mundo atual." [16]

Adaptado de David Kahn
(*The Codebreakers*, 1996)

Ao longo da História, a espécie humana tem evoluído acompanhada da preocupação em fazer fluir e fruir a informação, de forma eficaz e, ao mesmo tempo, segura. Essa trajetória, desde os nossos mais remotos ancestrais, tem sido marcada por importantes revoluções da informação. A primeira delas, quando ascendentes do *Homo sapiens* passaram a emitir sons e a articular a linguagem, possibilitando a transmissão de conhecimentos de geração a geração por meio da tradição oral, preferencialmente aos simples atos de "espiar" e copiar comportamentos nos quais se baseava a inteligência[17] primitiva.

Na seqüência dos acontecimentos, idéias e objetos passaram a ser representados por meio de desenhos e pinturas em rochas e paredes de cavernas, num sistema pictórico que se constituiria na primeira expressão simbólica registrada pelo homem. Esse sistema de anotação simplificada dos objetos da realidade, que marcou o início da comunicação impressa, evoluiu para signos gráficos, constituindo o primeiro meio organizado de comunicação, que possibilitou registrar o conhecimento, transmiti-lo e perpetuá-lo de forma mais efetiva.

---

[16] "*In the beginning, people whispered. Others eavesdropped. And from these humble caveman origins have evolved one of the most powerful forms of intelligence and one of the most important forms of security in the world today*."

[17] Inteligência, aqui, pode-se entender tanto do ponto de vista cognitivo — como atividade ou processo mental ou intelectual —, quanto de atividade sigilosa inerente à tomada de decisão. A inteligência relacionava-se (e ainda se relaciona) intimamente à observação e memorização. Por meio do ato de "espiar", se absorviam informações, se apreendiam e aprendiam novas práticas e técnicas e se agregavam novos conhecimentos. E de espiar derivou espionar, em que se assentam os fundamentos da inteligência como atividade de Estado. Considere-se, também, que daí resultaria a contra-inteligência, em que se insere a segurança da informação, objetivo primordial da criptografia.

Estava, assim, inventada a **escrita** — talvez a principal revolução da informação —, logo acompanhada do advento da **escrita secreta**. A ameaça de interceptação indevida motivou a necessidade de ocultar a mensagem e o desenvolvimento de códigos e cifras para disfarçar a informação, dissimular o seu significado, de maneira a torná-la perceptível e inteligível apenas aos reais interessados.

4.1 ESCRITA (OU COMUNICAÇÃO) SECRETA[18]

Escrita secreta é todo tipo de comunicação expressa por meio de signos gráficos que procura manter o texto da mensagem — ou a própria mensagem — em segredo, seja de forma dissimulada ou disfarçada, ou oculta, encoberta ou similar. Historicamente atribuída a espiões, desenvolve-se por meio de três técnicas: **esteganografia**, **codificação** e **criptografia**. A primeira preocupa-se em esconder a própria mensagem; as outras duas, o seu conteúdo e/ou significado.

4.1.1 ESTEGANOGRAFIA

Composta do antepositivo *estegan(o)-*[19] (do grego *steganós,ḗ,ón* "que cobre, que recobre hermeticamente") mais *–grafia,* **esteganografia** pode ser definida como "**escrita encoberta, escondida**". Há mais de 2.500 anos, objetiva fazer com que mensagens trafeguem despercebidas, sem ser notadas ou descobertas.

Desde o século V a.C., várias formas de esteganografia têm sido usadas ao redor do mundo. Como exemplo, Singh (1999, p. 4) relata que o "Pai da História", Heródoto (c. 484 a.C. – c. 425 a.C.), de Halicarnasso, narra, em **As Histórias**, que foi essa técnica que salvou a Grécia de ser conquistada pelos persas, durante as Guerras Médicas[20]. Demarato, o mais antigo espião registrado na História ocidental a empregar escrita

---

[18] Embora "secreto" seja um grau de classificação sigilosa, de acordo com a legislação pertinente em vigor (Decreto n°. 4.553, de 27 de dezembro de 2002), por motivos de tradição e de compreensão será respeitada a expressão "escrita secreta". Mas, em termos atuais, o ideal seria "escrita sigilosa".

[19] ESTEGAN(O)-. In: HOUAISS, Antonio. **Dicionário Eletrônico da Língua Portuguesa**. 2. ed. São Paulo: Ed. Objetiva, 2007. Elemento de composição utilizado na terminologia científica do sXIX em diante.

[20] Também conhecidas como "Guerras Persas" ou "Guerras Greco-Persas", designa os conflitos bélicos entre gregos e persas durante o século V a.C.

secreta, teria avisado os gregos dos planos de invasão do rei Xerxes[21], enviando-lhe uma mensagem escrita em um par dobrável de placas de madeira (Figura 3), que eram, depois, cobertas com cera. No destino, raspada a cera, o texto seria exposto.

Figura 3.
Roman wax tablet with three styli (modern reproduction).
Disponível em: <http://en.wikipedia.org/wiki/Wax_tablet>.
Acesso em: 27 ago. 2008.

Essa técnica de comunicação secreta de Demarato consistia, pura e simplesmente, de ocultar a mensagem. Esse foi o primeiro caso de uso da esteganografia de que há registro no mundo ocidental.

Heródoto reconta, também, outro episódio em que a técnica de ocultação foi suficiente para garantir a comunicação segura da mensagem (SINGH, 1999, p. 5), ainda no transcorrer das Guerras Médicas. Histeu (também Histieu, Histieo ou Histaiaeus), tirano de Mileto, querendo instigar seu enteado Aristágoras a se rebelar contra o rei persa, decidiu enviar-lhe mensagem secreta. Para tal, convocou seu mais fiel escravo, raspou-lhe a cabeça, escreveu as instruções no seu couro cabeludo e esperou o cabelo voltar a crescer. Feito isso, o mensageiro deslocou-se, sem despertar qualquer suspeita, até o destino, onde simplesmente pediu ao destinatário que lhe raspasse a cabeça, expondo-lhe, assim, a informação de que necessitava.

Na Antigüidade, certamente, urgência não chegava a constituir problema crucial e técnicas como essas — simples, mas de inegável imaginação — não comprometiam o princípio da oportunidade. Porém, nestes mais de dois mil anos depois de Heródoto, a complexidade tecnológica tem aumentado tremendamente, propiciando, na medida da criatividade humana, a invenção de diferentes formas de esteganografia pelo mundo afora. Assim, há, ainda, inúmeros outros exemplos históricos, valendo destacar, dentre

[21] Xerxes (520/465 a.C.), "Rei dos Reis", líder despótico dos persas.

os mais conhecidos:

a) Na China antiga, usava-se escrever em um pedaço de seda finíssima, o qual era comprimido até atingir a forma de uma bolinha. Esta, por sua vez, era envolta em cera e, a seguir, engolida pelo mensageiro, que a transportava no estômago. Assim, a informação era esteganografada por ocultação. Essa técnica milenar, originalmente empregada para fins de espionagem, serviu até de inspiração para ilícitos transnacionais de alta periculosidade que adentram o século XXI. Nos dias de hoje, como exemplifica a Figura 4, o crime organizado tem utilizado sistema semelhante para tráfico ilícito de cocaína. Pessoas são empregadas como "mulas" para transportar a droga em seus estômagos, sem despertar suspeitas.

Figura 4 – Cápsulas de cocaína no estômago. Disponível em: <http://g1.globo.com/Noticias/Rio/0,,MUL338045-5606,00.html>. Acesso em: 14 nov. 2008.

b) No primeiro século d.C., inventou-se a escrita com **tinta invisível**, que nada mais era do que simples líquidos à base de ácido cítrico, como sumo de frutas, vinagre, vinho branco e até urina. Com essas "tintas", utilizando-se até palitos como "penas" para aplicá-las, escreviam-se mensagens sigilosas entre as linhas normais de documentos ou cartas aparentemente inofensivas. Depois de seco, o líquido não deixa vestígio visível, mas o ácido permanece no papel e o texto é facilmente recuperado quando submetido a calor. Apenas aproximando-se uma vela ou, em tempos modernos, uma lâmpada incandescente, o que foi escrito adquire uma coloração amarronzada e a mensagem se revela.

Hoje, o Serviço de Segurança e Contra-Inteligência do Reino Unido (*Military Intelligence 5* – MI-5) — que se pode considerar o "Pai da Criptoanálise" — ensina essa técnica a crianças pela internet, como se pode constatar pela Figura 5.

Figura 5.
Tinta invisível — Como preparar, escrever e revelar.
Disponível em: <http://www.mi5.gov.uk/output/Page295.html>. Acesso em: 28 ago. 2008.

Apesar de parecer pueril, a esteganografia com tinta invisível tem sido amplamente usada para fins legítimos importantes, obviamente empregando técnicas modernas. Órgãos e agências de segurança, por exemplo, têm empregado essa técnica para marcar e identificar produtos e objetos particulares, documentos, materiais sensíveis, partes de veículos, dinheiro e até drogas, inclusive para fins jurídicos e legais. Alguns produtos químicos especiais tornam-se legíveis por simples fotoluminescência, quando expostos à luz negra ou ultravioleta, a raios-X, etc., como mostra a Figura 6.

Figura 6.
Marcação com tinta invisível, para leitura com luz negra.
Disponível em: <http://www.riskreactor.com/Invisible_Inks/Invisible_Inks_Main.htm>. Acesso em: 29 ago.2008.

c) Por fim, mas não em definitivo, lugar destacado na história da esteganografia — como, de resto, da própria segurança da informação — desempenhou a Alemanha nazista. Na Segunda Guerra Mundial, as forças de segurança e espionagem de Hitler reintroduziram os **micropontos**[22]. Microfilmes, miniaturizados até atingir menos de um

[22] A origem dos micropontos remonta à Guerra Franco-Prussiana (1870-1871), quando documentos começaram a ser microfotografados e enviados por pombos-correios. No destino, eram lidos com auxílio de microscópios.

milímetro de diâmetro, eram disfarçados como pontos (sinais de pontuação) em locais estratégicos previamente convencionados, normalmente no encerramento de cartas ou documentos comuns, como ponto final. Informações sigilosas diversas eram assim ocultadas e transmitidas (Figura 7).

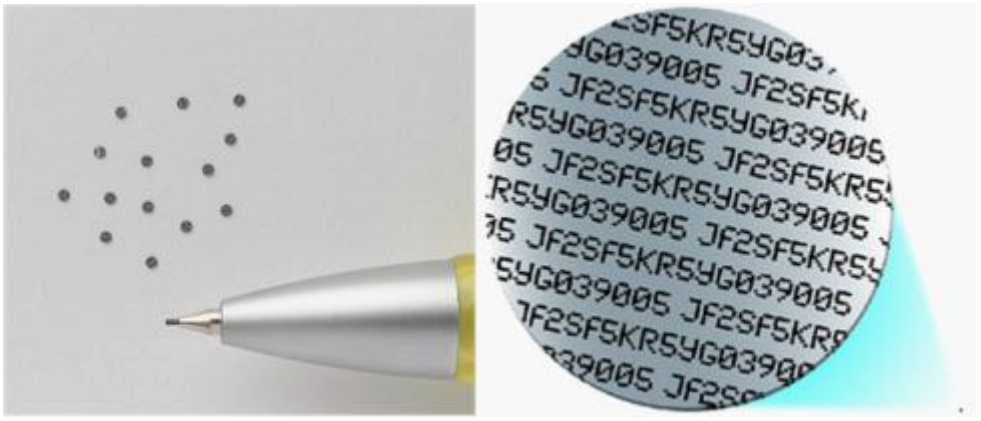


Figura 7 – Micropontos.
Vista em resolução normal e ampliada, revelando a informação inscrita.
Disponível em: <http://www.scienceinafrica.co.za/2005/november/microdot.htm>.
Acesso em: 28 ago. 2008.

De incomum longevidade, a esteganografia perdura até os dias atuais, como já se demonstrou, o que reflete sua aplicabilidade, comodidade e segurança. Contudo, essa técnica padece de uma vulnerabilidade fatal. Como ela se preocupa apenas em ocultar a mensagem, se esta for descoberta o conteúdo da comunicação secreta será revelado no ato e o esforço terá sido em vão. **Na esteganografia, a interceptação da mensagem quebra a segurança.**

Não obstante, a esteganografia possui algumas aplicações práticas interessantes, basicamente as mesmas da “tinta invisível”. Ademais, é uma das técnicas utilizadas, por exemplo, para implementar mecanismos de verificação de direitos autorais em imagens, textos e mídias em geral.

Por outro lado, a preocupar cada vez mais os organismos de segurança e inteligência do mundo atual, a esteganografia também tem servido para divulgação de mensagens malignas de forma sub-reptícia. Essa característica tem sido amplamente explorada,

por organizações criminosas e terroristas, para comunicar-se e coordenar operações ilícitas, atentados, propaganda radical e proselitismo de cunho ideológico e religioso, dentre outros aspectos.

4.1.2 CODIFICAÇÃO

A codificação refere-se a um tipo de comunicação secreta muito particular, mas que tem caído em desuso ao longo do tempo. Consiste no emprego de códigos, em que se substitui uma palavra ou frase por outra palavra, ou um número ou símbolo. Assim, “agentes secretos”, por exemplo, utilizam “codinomes”, para mascarar suas verdadeiras identidades. Porém, as palavras ou locuções a servir de código têm que ser previamente convencionadas e relacionadas num **livro-código** (Figura 8), a ser distribuído entre os correspondentes. Essa é a principal vulnerabilidade da codificação. Se o livro cair em mãos inimigas, a segurança da comunicação estará comprometida. O único remédio será estabelecer novo sistema.

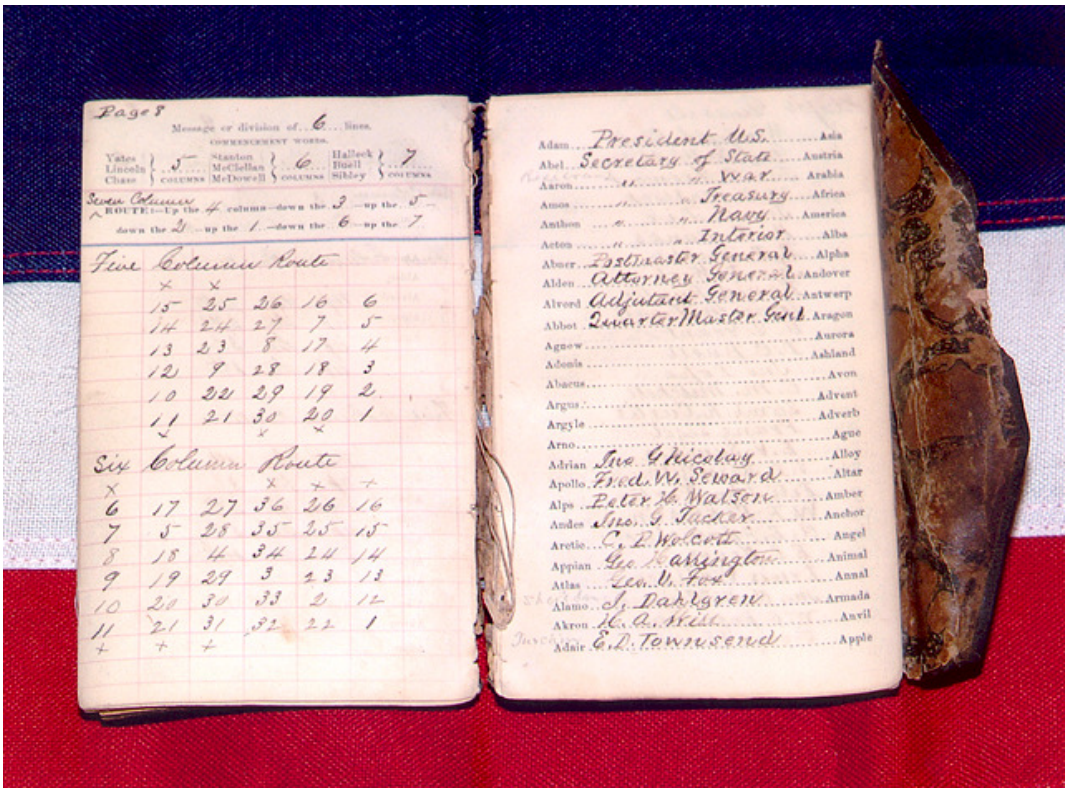


Figura 8
Cipher for Telegraphic Correspondence.
A code book used by Union General Joseph Hooker's code clerk.
Disponível em: <http://en.wikipedia.org/wiki/Code_book>. Acesso em: 29 ago. 2008.

4.1.3 CRIPTOGRAFIA

Como já se antecipou, a criptografia tem por objetivo não esconder a existência da mensagem, como na esteganografia, mas ocultar o seu significado. Para isso, submete-a a um processo de **cifração**[23], o mesmo que **cifragem**, que significa passar o texto por um processo de **cifras**. Estas são definidas como qualquer forma de substituição criptográfica, em que cada letra é substituída por outra letra ou por um símbolo, de acordo com um protocolo particular previamente acordado entre emissor e receptor. Assim, a mensagem é misturada/embaralhada para tornar-se ininteligível a quem não dispuser do protocolo, ou da chave, para decifrá-la. Essa característica constitui, portanto, vantagem no caso de interceptação indevida.

Tecnicamente, a criptografia divide-se em dois ramos: **transposição** e **substituição** (atualmente mais referidos como cifra **simétrica** e cifra **assimétrica)**. Nesta, cada letra mantém sua identidade, mas muda de posição; ao passo em que, naquela, o processo é inverso, isto é, cada letra muda de identidade, mas mantém sua posição. Historicamente conhecidos como **Cifras Clássicas**, esses sistemas de criptografar eram implementados manualmente ou com o emprego de dispositivos mecânicos simples. Na maioria, caíram em desuso, mas é importante fazer-lhes referência, pelo menos aos principais, no sentido de apresentar os rudimentos que desembocaram na criptografia moderna.

a) CIFRA DE TRANSPOSIÇÃO (OU SIMÉTRICA)

Consiste no simples rearranjo das letras no texto da mensagem, gerando um **anagrama**[24], ou seja, uma mensagem diferente. O número de rearranjos possíveis é exponencialmente proporcional ao número de letras contidas na mensagem. Assim, por exemplo, com um texto de 35 letras podem-se obter mais de 5×10^{30} combinações

[23] Que alguns setores especializados teimam em adaptar, do inglês ***encryption***, como "encriptação", termo aberrante, não reconhecido pelo Vocabulário Ortográfico da Língua Portuguesa Brasileira (VOLP). Encriptação, contudo, seria derivado do verbo "encriptar", definido como "colocar em cripta ou em túmulo; sepultar" (HOUAISS, 2007), que não é objeto do presente trabalho. Esta mesma observação se aplica a "decriptação", que derivaria de ***decryption***.

[24] Anagrama define-se como "transposição de letras de palavra ou frase para formar outra palavra ou frase diferente" (HOUAISS, 2007).

diferentes entre os caracteres componentes (SINGH, 1999, p. 7). Dessa forma, é humanamente impraticável quebrar esses anagramas sem conhecer o sistema, ou chave de transposição.

O primeiro instrumento criptográfico, de emprego militar, que incorporava o sistema de transposição, foi o *scytale* (ou *skytale*) espartano (Figura 9), desenvolvido no século V a.C. Consistia de um bastão com uma tira de couro enrolada, na qual se escrevia o texto a ser transmitido. Desenrolada, essa tira constituía uma **cifra transposta** que, para ser decifrada e lida, necessitava que o receptor da mensagem dispusesse de bastão semelhante, com as mesmas características. Conjugando-se com a técnica de esteganografia, a tira de couro poderia ser, ainda, disfarçada sob a forma de um cinto, por exemplo, ou qualquer outra, dependendo da criatividade do mensageiro.

Figura 9 – *Scytale*.
Disponível em: <http://en.wikipedia.org/wiki/Skytale>. Acesso em: 19 jun. 2008.

b) CIFRA DE SUBSTITUIÇÃO (OU ASSIMÉTRICA)

Substituição é a técnica criptográfica alternativa à transposição. Nesta, cada letra mantém sua identidade, mas muda de posição; naquela, a letra muda de identidade, mas mantém sua posição. Nesse método, as unidades do **texto em claro** (original) são substituídas, de acordo com um sistema regular, conformando um **texto cifrado**. As "unidades" podem ser letras simples (o mais comum), pares ou trios de letras, uma mistura disso tudo e assim por diante. Para decifrar, o receptor da mensagem procede à substituição inversa.

I. CIFRA MONOALFABÉTICA — A "CIFRA DE CÉSAR"

Uma das fórmulas mais usadas na criptografia por substituição consiste em apenas emparelhar as letras do alfabeto de forma aleatória e, após, substituir cada letra da mensagem original pela sua correspondente, como na Figura 10. Contudo, apesar de tradicional, a cifra de César pode ser facilmente quebrada, por meio de **análise de freqüência**[25] e **ataque de força bruta**[26].

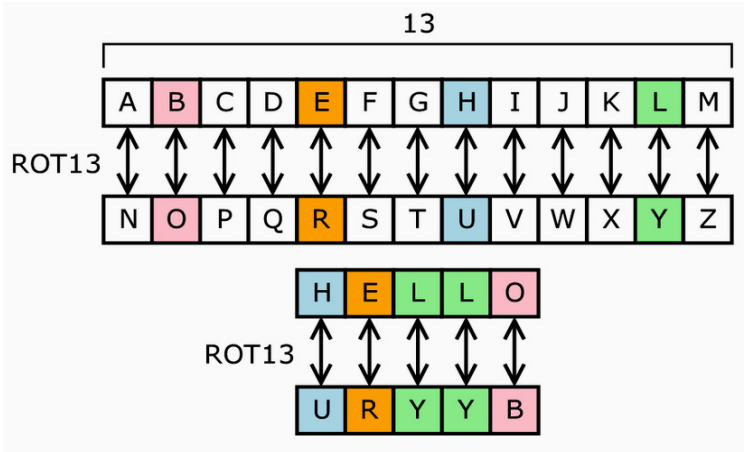


Figura 10– Cifra de César.
ROT13 is a Caesar cipher, a type of substitution cipher. In ROT13, the alphabet is rotated 13 steps.
Disponível em: <http://www.answers.com/topic/substitution-cipher>.
Acesso em: 29 jun. 2008.

[25] Parte da criptoanálise, a análise de freqüência é o estudo da freqüência com que letra(s) ou grupo(s) de letras ocorre(m) em textos cifrados. A variação dessas freqüências pode ser explorada para quebrar cifras.

[26] Que consiste de tentar todos os códigos, combinações ou senhas (*passwords*) possíveis, até que se encontre a fórmula certa, isto é, a chave criptográfica.

As formas tradicionais de criptografia que usam esse sistema são conhecidas como **cifras monoalfabéticas**. Ou seja, mantêm esquema fixo ao longo de toda a mensagem, utilizando alfabeto único.

II. CIFRA POLIALFABÉTICA — A "CIFRA DE VIGENÈRE"

Alternativamente à cifra monoalfabética, há o sistema **polialfabético,** que utiliza determinado número de substituições em tempos diferentes na mensagem. Assim, para cada unidade (letra) do texto em claro, há diferentes possibilidades de ocorrência no texto cifrado e vice-versa. São utilizados, portanto, vários alfabetos.

As cifras monoalfabéticas persistiram até o século XVI, quando o diplomata e criptógrafo francês Blaise de Vigenère criou a cifra que foi batizada com seu sobrenome. A chamada **Cifra de Vigenère** empregava diversos alfabetos para cifrar uma mesma mensagem, de acordo com a grade contida na Figura 11.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 11 – Grade de Vigenère.
Conhecida também como *tabula recta*, para cifrar e decifrar.
Disponível em:
<http://pt.wikipedia.org/wiki/Imagem:Vigenere-square.png>. Acesso em: 29 jun. 2008.

A intenção do sistema de Vigenère — como em toda cifra do gênero — era mascarar a freqüência das letras no texto original. Essa era a sua grande vantagem, pois a tornava resistente à análise de freqüência anteriormente mencionada, obstando a criptoanálise inimiga e, conseqüentemente, a quebra da chave criptográfica.

A cifra de Vigenère permaneceu inquebrantável por cerca de três séculos. Porém, em 1854 cedeu aos esforços criptoanalíticos de um matemático, engenheiro mecânico e inventor inglês, Charles Babbage (SINGH, 1999, p. 78), embora esse fato só tenha vindo a público no século seguinte. Babbage, considerado um dos pioneiros da computação, desenvolveu método de quebrar a cifra de Vigenère baseado no fato de que os sistemas polialfabéticos — embora difíceis de descobrir por análise de freqüência — apresentam uma fraqueza, se a chave for curta e repetida constantemente. Como resultado, letras de uso mais freqüente (Figuras 12 e 13) aparecem cifradas segundo as mesmas letras da chave, o que leva à descoberta de padrões repetidos no texto (Figura 14) e possibilita a quebra da cifra.

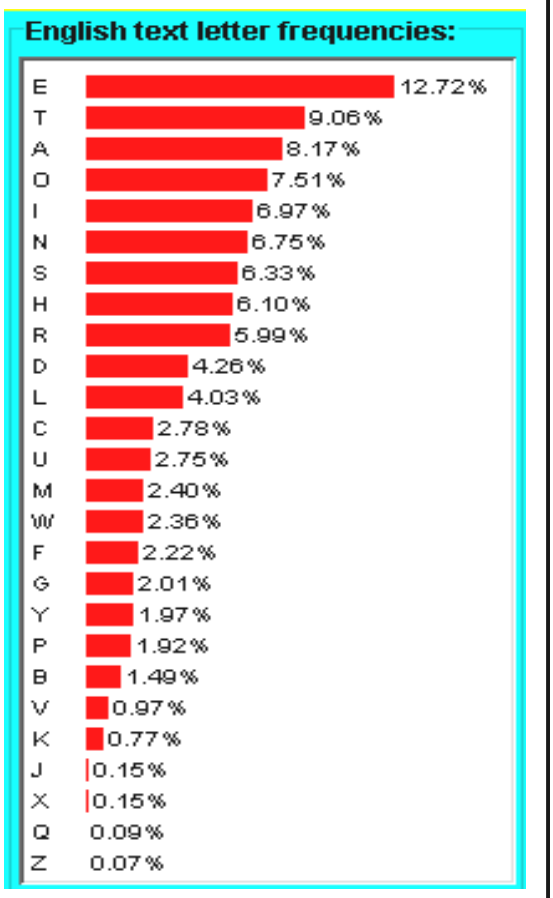


Figura 12.
Disponível em: <http://faculty.rivier.edu/bhiggs/web/cs572aweb/Assignments/CrackingClassicCiphers.htm>. Acesso em: 29 jun 2008.

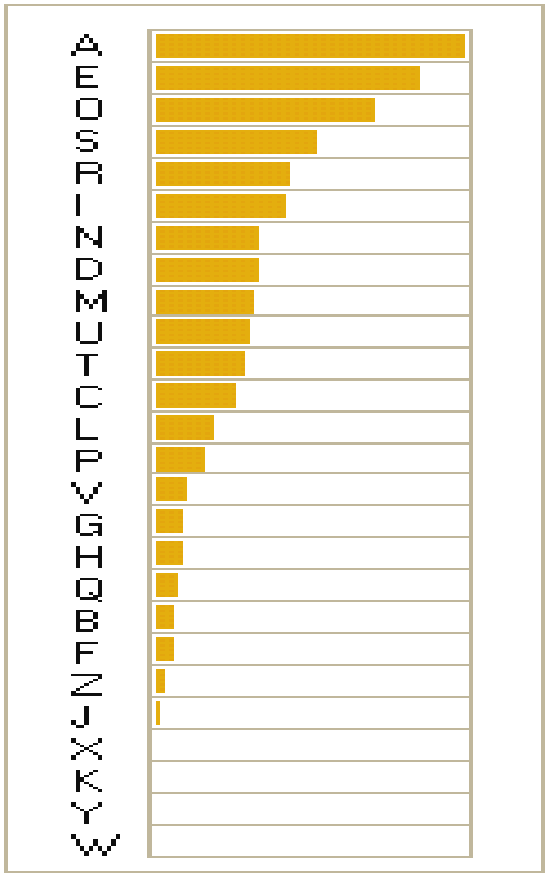


Figura 13
Histograma por ordem de freqüência em português.
Disponível em: <http://www.numaboa.com.br/criptologia/matematica/estatistica/freqPortBrasil.php>. Acesso em: 29 jun. 2008.

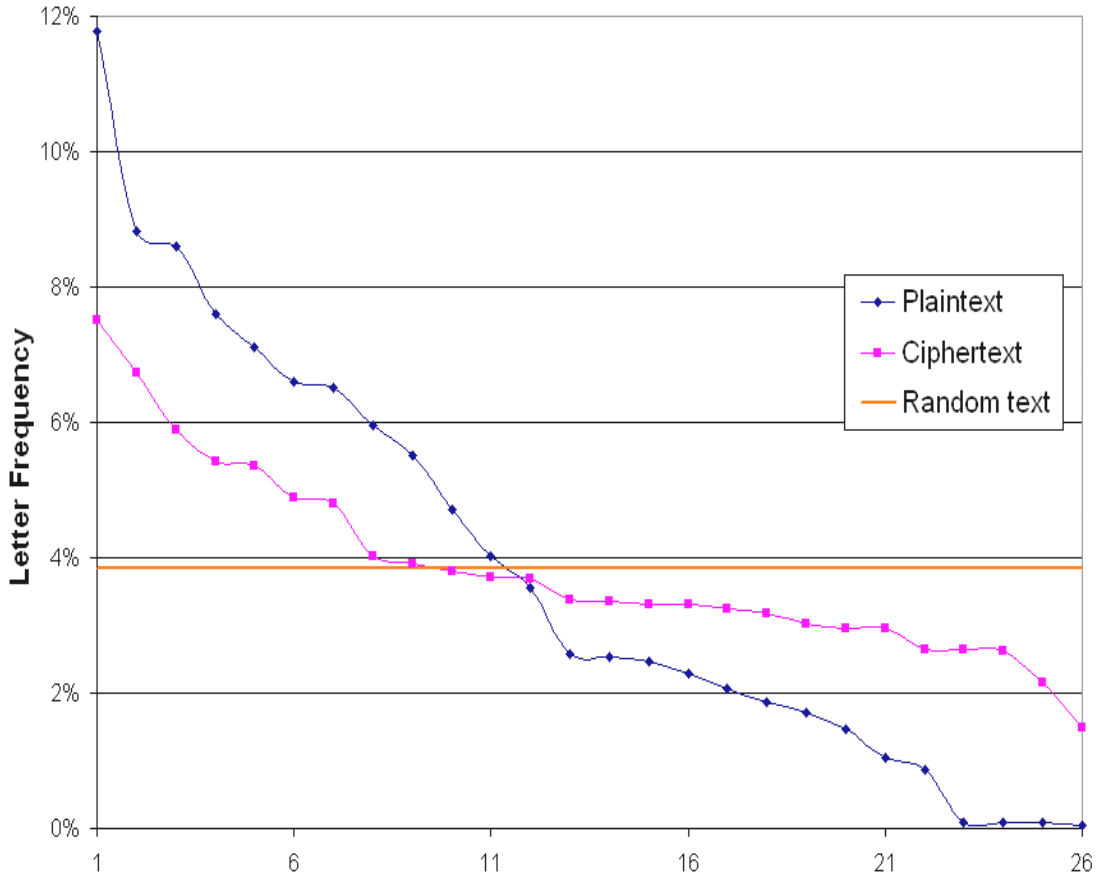


Figura 14.

The Vigenère cipher masks the characteristic letter frequency of English plaintexts, but some patterns remain. Disponível em: <http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>. Acesso em: 29 ago. 2008.

c) O SISTEMA DE ROTORES — A MÁQUINA "ENIGMA"

O mais famoso sistema de criptografia registrado na História (POLMAR, 1998, p. 192), a **Enigma** (Figura 15) era uma máquina criptográfica eletromecânica, que utilizava um conjunto de três, quatro ou cinco (depois sete e oito) rodas intercambiáveis, ou "rotores", e diversos conectores. Assim concebido, esse sistema era imune à criptoanálise da época.

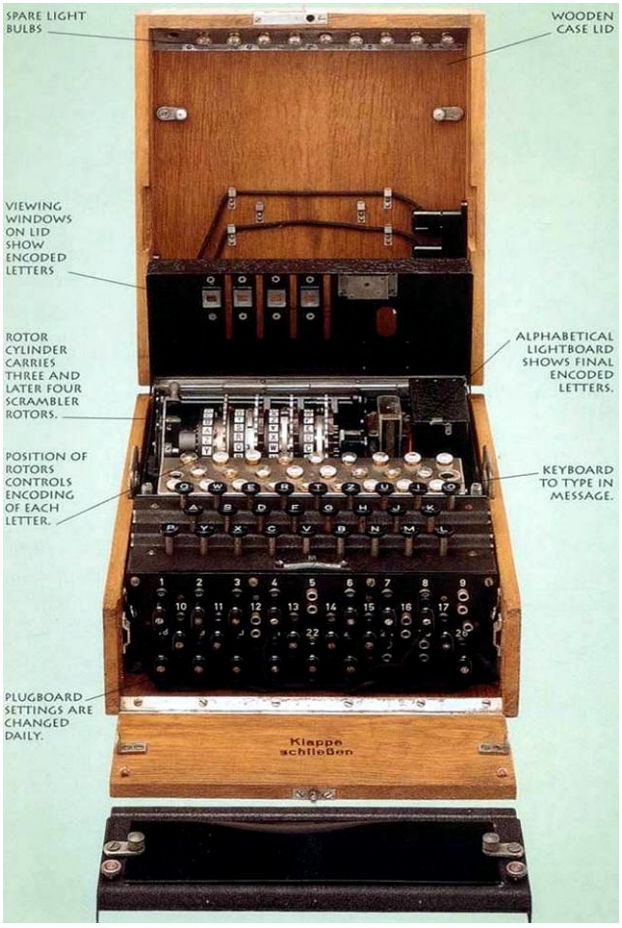


Figura 15 – Máquina Enigma com quatro rotores.
Disponível em:
<http://www.uncp.edu/home/rwb/EnigmaMachine.jpg>.
Acesso em: 30 jun. 2008.

Originalmente criada com fins comerciais, a Enigma veio a se constituir na espinha dorsal das comunicações militares e de inteligência da Alemanha nazista na Segunda Guerra Mundial. Com três rotores, era capaz de fazer até 17.000 permutações para cifrar cada letra do alfabeto. Com cinco rotores, então, esse número se elevava a seis sextiliões (6×10^{21}). Além disso, a ordem desses rotores podia ser alterada várias vezes ao dia, ou segundo qualquer outra periodicidade desejada. A força da cifra dependia, assim, da seqüência de rotores, que era a essência, a alma, da chave criptográfica.

A Enigma de três rotores foi decifrada em 1932, pelo *Biuro Szyfrów* (Escritório de Cifras), da Polônia. Em resposta, em 1938, os alemães acrescentaram um quarto rotor, o que multiplicou por 26 a capacidade de processamento da máquina. Adicionamente, também aumentaram a freqüência com que mudavam a disposição do conjunto de rotores. Em conseqüência, com a Enigma praticamente inquebrantável, os trabalhos de

criptoanálise foram transferidos para o Reino Unido, onde o *Secret Intelligence Service* (SIS), ou *Military Intelligence 6* (MI-6), organizou a Escola Governamental de Códigos e Cifras (*Government Codes and Cypher School* – GC&CS), em Bletchley Park[27], com o objetivo de quebrar as cifras nazistas.

Em Bletchley Park, os principais esforços de criptoanálise dos Aliados concentraram-se em torno da operação "Ultra" (de "ultra-secreta"), desenvolvida por britânicos e norte-americanos e centrada na interceptação de radiocomunicações. As informações assim coletadas eram processadas nas máquinas *Colossus* (Figura 16), destinadas especificamente a quebrar os sistemas criptográficos alemães. Essas máquinas, que foram os primeiros aparelhos de computação eletrônica programáveis e digitais do mundo, viriam a se constituir na principal arma na guerra contra a Alemanha nazista.

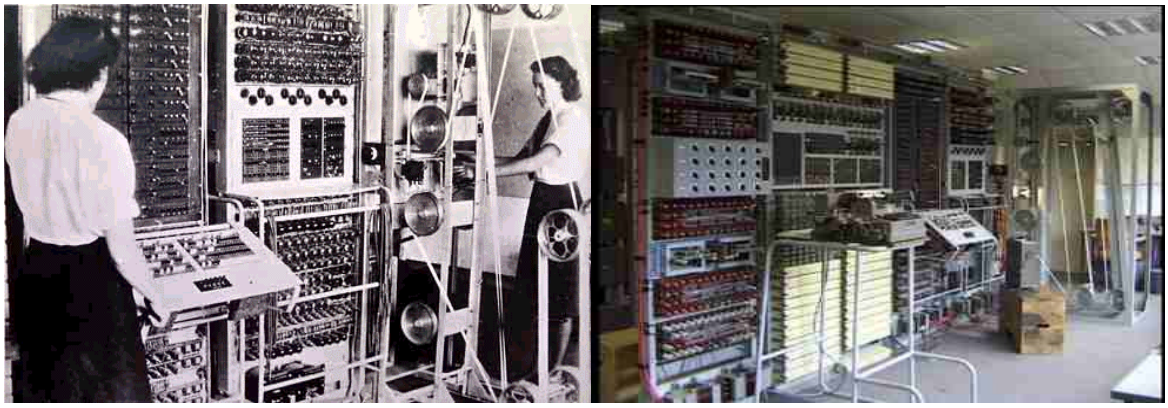


Figura 16 – *Two views of the code-breaking Colossus of Great Britain*.
Disponível em: <http://www.computersciencelab.com/ComputerHistory/HistoryPt3.htm>.
Acesso em: 30 jun. 2008.

Em 1942, graças à capacidade da *Colossus* e às ações de inteligência — que a alimentavam com informações —, o que era considerado inconcebível e impossível (SINGH, 1999, p. 185) aconteceu: o segredo da Enigma foi quebrado. Para isso, foi fundamental a captura, em operação secreta, de material criptográfico e códigos da Marinha nazista, o que forneceu a peça vital de informação que faltava para se decifrar

[27] Voltada exclusivamente para a criptoanálise, a GC&CS de Bletchley Park era um verdadeiro *think tank* multifuncional. Tendo Alan Turing como principal personagem, reunia matemáticos, cientistas, lingüistas e outros tipos de especialistas, numa mistura que o próprio Primeiro-Ministro, Winston Churchill, considerava "bizarra" (SINGH, 1999, p. 178). No seu auge, a escola chegou a abrigar cerca de sete mil pessoas, trabalhando primordialmente em criptoanálise.

o funcionamento do sistema. A partir de então, como expressou o General Alexander, “o conhecimento preciso não apenas do poder e da disposição do inimigo, mas também de como, quando e onde ele pretende executar suas operações, trouxe nova dimensão à continuidade da guerra” (LYCETT, 2001, p. 5).

A longevidade da Enigma, por quase duas décadas, baseou-se nas suas características de simplicidade, portabilidade, diversidade de uso e presumível segurança.

Porém, esse excesso de confiança foi exatamente o que veio a se constituir em uma das suas principais fraquezas. Isso, conjugado com erros de operadores, falhas de procedimentos, capturas ocasionais de máquinas cifradoras ou livros-código e — de fundamental importância — informações de inteligência, contribuiu sobremaneira para a sua derrota, sem contar com a escala industrial que a criptoanálise adquiriu, o que, exatamente, acelerou o seu uso para fins de inteligência. Essa combinação de fatores foi fundamental para os esforços concertados dos criptoanalistas, que conduziram ao final da Guerra ou, pelo menos, anteciparam a vitória dos Aliados.

4.2 A CRIPTOGRAFIA COMO SEGREDO DE ESTADO E A PRODUÇÃO LITERÁRIA

O segredo sempre desempenhou papel de destaque na história da criptografia. A produção literária a respeito era praticamente nula até inícios dos anos 1900. Contudo, até a Primeira Guerra Mundial, começaram a surgir algumas tímidas iniciativas com alguma freqüência. Em 1918, um dos mais influentes trabalhos criptográficos do século XX, a monografia “O Índice de Coincidência e suas Aplicações na Criptografia” (*The Index of Coincidence and its Applications in Cryptography*), de William F. Freidman, apareceu como um relatório de pesquisa dos Laboratórios Riverbank, da iniciativa privada, apesar de o trabalho ter sido feito como parte dos esforços de guerra.

Após o fim da Guerra, contudo, as coisas começaram a mudar. O Exército e a Marinha dos Estados Unidos, trabalhando em segredo absoluto, começaram a conseguir avanços fundamentais na área de criptografia. A publicação ostensiva de trabalhos

sobre o assunto desapareceu. Contudo, houve uma notável exceção: o trabalho “A Teoria da Comunição de Sistemas Secretos” (*Communication Theory of Secrecy Systems*), de Claude Shannon, que apareceu no Boletim Técnico da Bell System em 1949, apesar de também ter sido desenvolvido durante esforços de guerra. Depois da Segunda Guerra Mundial, o documento foi desclassificado, possivelmente por algum erro de controle das autoridades militares.

De 1949 até 1967, a literatura criptográfica foi praticamente proibida. Entretanto, naquele ano, uma contribuição especial apareceu: *The Codebrakers*, de David Kahn. Contudo, não apresentava qualquer nova idéia técnica, mas fazia um relato marcante e completo do que havia acontecido nos tempos anteriores, incluindo menções a alguns itens que o governo ainda considerava sigilosos. Esse fato deu impulso à produção intelectual sobre a matéria. Hoje, há uma vasta produção literária e acadêmica.

Exemplo que não poderia deixar de ser citado é Bruce Schneier, com seu “Criptografia Aplicada” (*Applied Cryptography*). Começando com os objetivos de segurança das comunicações e exemplos elementares de programas usados para atingir esses objetivos, Schneier fornece um panorama do que foi feito nos 20 anos de pesquisa pública anteriores. Chegou a incluir episódios do mundo em que a criptografia é desenvolvida e aplicada, discutindo entidades que variam desde a Associação Internacional para Pesquisa Criptológica até a poderosa Agência de Segurança Nacional (*National Security Agency* – NSA).

Vendo o interesse público na criptografia tomar vulto no final dos anos 1970 e princípios dos anos 1980, a NSA, órgão oficial de criptologia dos Estados Unidos, fez diversas tentativas para interrompê-lo, iniciando com a alegação de que a publicação de material criptográfico constituía violação aos Regulamentos sobre Tráfico Internacional de Armas.

Prosseguindo na sua pressão, a NSA adquiriu substancial influência não apenas no controle de equipamentos e publicações que são exportados, mas também para o que é vendido no interior dos Estados Unidos.

Não obstante, Bruce Schneier contribuiu para abrir os caminhos rumo a um melhor conhecimento das técnicas e práticas criptográficas. Seu livro *Applied Cryptography – Protocols, Algorithms, and Source* (SCHNEIER, 1996) apresenta conceitos, definições, métodos e práticas, constituindo-se em uma das principais fontes de consulta para quem pretende estudar ou trabalhar nessa área. Como se especificou, serviu até de fonte de inspiração para a Figura 2, na página 30 da presente monografia.

Dessa forma, encerra-se este capítulo, passando-se a discorrer, a seguir, sobre a SIC e a criptografia.

5. A SIC E A CRIPTOGRAFIA

Com a evolução da(s) TIC, particularmente no final do século XX e princípio do século XXI, assistiu-se a uma mudança global do mundo físico para o virtual. Quando a informação, e com ela a cultura humana, começa a viajar cada vez mais num ambiente digital, mediado por computadores, as infra-estruturas computacional e de comunicações devem ser expandidas para prover os mecanismos fundamentais necessários para apoiar na totalidade a cultura humana. Um desses mecanismos, amplamente reconhecido, mas pouco entendido, é a segurança, particularmente no que se refere à Segurança da Informação e das Comunicações (SIC).

5.1 A SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES (SIC)

Da mesma forma como ocorre com a criptografia, há inúmeras definições de **Segurança da Informação (SI)** e também não há condições de relacioná-las todas. A título de ilustração, pesquisa na internet, simplesmente para verificar o número de citações feitas a "segurança da informação" e sua correspondente em inglês "*information security*", revelou o seguinte quadro:

Buscador / Entrada	*AOL*	globo.com	*Google*	MSN	*Yahoo*
Segurança da Informação	848.000	726.000	1.410.000	137.000	41.900.000
Information Security	143.000.000	92.100.000	127.000.000	369.000.000	2.060.000.000

Figura 17.
Número de citações de "segurança da informação" e "*information security*" na internet, por ferramenta de busca. (Pesquisa em: 5 dez. 2008.)

Não obstante, na seqüência do encadeamento lógico a fundamentar o presente trabalho, há que se considerar o que dizem algumas das mais importantes autoridades

nacionais e estrangeiras sobre a questão.

O Departamento de Segurança da Informação e Comunicações (DSIC), órgão da estrutura regimental do GSIPR, entende e divulga na internet[28] que a Segurança da Informação e Comunicações (SIC) é uma ação que objetiva viabilizar e assegurar a Disponibilidade, a Integridade, a Confidencialidade[29], e a Autenticidade (DICA) da Informação e das Comunicações, e define cada um desses termos:

> **"Disponibilidade**: propriedade de que a INFORMAÇÃO esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
>
> **Integridade**: propriedade de que a INFORMAÇÃO não foi modificada, inclusive quanto à origem e ao destino, ou destruída.
>
> **Confidencialidade**: propriedade de que a INFORMAÇÃO não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
>
> **Autenticidade**: propriedade de que a INFORMAÇÃO foi produzida, expedida, modificada ou destruída por determinada pessoa física, ou por determinado sistema, órgão ou entidade."

Já a Associação Brasileira de Normas Técnicas (ABNT) estipula, por meio da norma ABNT NBR ISO/IEC 17799, que "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT, 2005, p. ix). E acrescenta a ABNT (2005, p. 1) que a Segurança da Informação consiste da "preservação da confidencialidade da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas".

---

[28] Disponível em <http://portal2.tcu.gov.br/portal/pls/portal/docs/783755.PDF>. Acesso em 31 jul. 2009.

[29] Nesse contexto, "confidencialidade" constituir-se-ia em um neologismo para a Língua Portuguesa, por mera adaptação do original em inglês *confidentiality*, que a comunidade de TIC (academia e iniciativa privada) vem convencionando adotar para significar **sigilo**. Apesar de não reconhecida pelo VOLP, Houaiss (2007) incorpora essa palavra com o significado de "qualidade do que é confidencial". Confidencial, por sua vez, à luz da legislação pertinente em vigor (Decreto nº. 4.553/2002), é um dos graus de sigilo, não o sigilo em si. Este se refere à manutenção de segredo e é graduado de acordo com o valor estratégico ou o potencial de risco do item ou bem classificado. Portanto, respeitado o necessário rigor científico, não cabe neste trabalho o emprego de "confidencialidade" com o pretenso significado ou como sinônimo de sigilo, só se admitindo o seu uso quando imprescindível para evitar problemas de intelecção.

Do ponto de vista legal, no âmbito da Administração Pública Federal (APF), o Decreto nº. 3.505/2000[30] estabelece, no seu artigo 2º (II), que Segurança da Informação é a

> "proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.".

Essa definição, também adotada pelo DSIC/GSIPR, guarda alguma semelhança com o que preconiza a NSA para **Segurança de Sistemas de Informação** (*Information Systems Security* – INFOSEC)[31], que, no *National Information Assurance (IA) Glossary* (CNSS, 2006, p. 33), está definida como:

> "Proteção de sistemas de informação contra acesso não-autorizado ou modificação de informações, armazenadas, em processamento ou em trânsito, e contra negação de serviço a usuários autorizados, incluindo as medidas necessárias para detectar, documentar e conter tais ameaças.".

Contudo, uma definição mais abrangente encontra-se na legislação dos EUA, baixada por meio do *E-Government Act of 2002*[32], que especifica que

> "O termo 'segurança da informação' significa proteção da informação e dos sistemas de informação contra acesso, uso, revelação, interrupção, modificação ou destruição não-autorizados, a fim de prover —
>
> (A) integridade, que significa proteção contra modificação ou destruição indevidas da informação e inclui garantia de não-repúdio e autenticidade da informação;
>
> (B) sigilo[33], que significa preservação das restrições legais relativas a acesso e revelação, incluindo meios para proteção da privacidade das pessoas e da propriedade intelectual; e
>
> (C) disponibilidade, que significa garantia de acesso e uso da informação, de forma confiável e oportuna."

---

[30] BRASIL. Decreto nº. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm>. Acesso em: 8 jun. 2008.

[31] *INFORMATION SYSTEMS SECURITY* (INFOSEC). In: *CNSS Instruction No. 4009. National Information Assurance (IA) Glossary*. Ft. Meade, MD, USA: CNSS, 2006. 86 p.

[32] *UNITED STATES OF AMERICA. Public Law 107–347. 107th Congress. Dec. 17, 2002. An Act To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes. Title III—Information Security. Sec. 301. Information Security. Subchapter III—Information Security. § 3542. Definitions*. Disponível em: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf>. Acesso em: 20 out. 2008.

[33] *Confidentiality*, no original em inglês.

Na essência disso tudo, SIC obtém-se por meio de medidas de proteção de dados e/ou informações contra: perda, furto, corrupção e sabotagem; e acesso, uso, revelação, interrupção, modificação e destruição indevidos ou não-autorizados. Essas medidas implementam-se não obstante o estado ou a condição dos dados e/ou informações, ou seja, não importa se estejam em arquivo, em processamento ou em trânsito. Também independem do suporte desses dados e/ou informações, ou a mídia ou forma como estejam expressos, isto é, impressa, eletrônica, óptica ou outras quaisquer.

As medidas de SIC estendem-se, portanto, a:

Sistemas de informação, que abrangem redes de computadores e de comunicações eletrônicas, bem como dados armazenados, processados, recuperados ou transmitidos por meio dessas redes, ou que sejam essenciais a sua operação, uso, proteção e manutenção;

Redes, que se referem a sistemas de transmissão e podem incluir sistemas computacionais, servidores, *switches* e roteadores, além de outros recursos que permitam tráfego de sinais por fio, rádio e meios ópticos ou outros eletromagnéticos, incluindo redes de satélites, redes terrestres fixas e móveis, redes usadas para radiodifusão e televisão tradicional ou a cabo; e

Gestão de documentos, que a Política Nacional de Arquivos[34] define como "o conjunto de procedimentos e operações técnicas para produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente".

No seu conjunto, esses sistemas conformam a(s) **tecnologia(s) de informação e comunicações** (TIC), objeto da **Segurança da Informação e das Comunicações (SIC)**, entendida esta como a capacidade de um sistema de informação, uma rede ou

[34] Lei nº. 8.159/1991, art. 3º.

um sistema de gestão documental resistir a eventos acidentais e ações ilícitas e/ou maliciosas que possam comprometer as características de dados/informações armazenados, processados ou em trânsito, assim como de serviços relacionados que possam ser oferecidos por esses sistemas.

Para efeitos deste trabalho, essas características consagram-se na sigla DISA[35], que se refere a Disponibilidade, Integridade, Sigilo e Autenticidade:

Disponibilidade é a garantia de que dados e/ou informações possam ser acessados e usados de forma ágil, confiável e oportuna. Inclui proteção contra negação de serviço;

Integridade tem por fundamento evitar corrupção ou modificação não-autorizada de dados e/ou informações, em todas as suas fases de existência, isto é, geração ou produção, difusão e tramitação, uso, avaliação e destinação final (arquivamento ou eliminação);

Sigilo[36], a que se pode agregar "**privacidade**", destina-se a prevenir/evitar revelação não-autorizada ou acidental de dados e/ou informações, garantindo que apenas os usuários reais tenham acesso ao seu conteúdo ou significado; e

Autenticidade visa a assegurar a veracidade e consistência de dados e/ou informações, assim como a identidade e fidedignidade da fonte e do usuário, ou do emissor e do receptor.

---

[35] Em vez de DICA (Disponibilidade, Integridade, **Confidencialidade** e Autenticidade), pelos motivos já explicados com relação a "confidencialidade" para significar "sigilo". Não obstante, DICA é genericamene usada nos círculos governamentais — inclusive o próprio DSIC e o GSIPR como um todo —, acadêmicos e comerciais. DISA, portanto, é uma novidade introduzida por este autor.

[36] Que alguns preferem designar "confidencialidade". Contudo, o conceito "sigilo", está assim expresso em diplomas legais pelo menos desde a edição do Código Penal Brasileiro (CPB), de 1940, referindo-se à manutenção do segredo — que desde o Império já vinha sendo legalmente regulamentado. A propósito de regulamento, convém mencionar, ainda: o "Regulamento para a Salvaguarda das Informações que Interessam à Segurança Nacional" (RSISN), baixado pelo Conselho de Segurança Nacional em 1949 e que define sigilo; e o "Regulamento para Salvaguarda de Assuntos Sigilosos" (RSAS), de 1977, que se inspirou no RSISN e deu origem à legislação sobre o assunto atualmente em vigor.

Amiudando-se detalhes, no processo de comunicação poder-se-ia acrescentar a esse ciclo (DISA) uma quinta característica, a de **não-repúdio**. Embora esta possa estar embutida na “autenticidade”, serve para garantir a responsabilidade final do receptor da mensagem e, ao mesmo tempo, atestar que o emissor especificado foi quem de fato a enviou.

Nos moldes atuais, SIC refere-se, essencialmente, à proteção da informação em mídia eletrônica e meios eletromagnéticos, que existem há cerca de um século. O campo tem uma longa pré-história. Como já se salientou, a informação tem sido protegida em papel e canais rudimentares de telecomunicação, como sinais de fumaça, por milênios, particularmente no tocante à característica de sigilo. Contudo, a SIC como se conhece hoje data do desenvolvimento do rádio e do seu uso na Primeira Guerra Mundial.

5.2 A IMPORTÂNCIA DA CRIPTOGRAFIA PARA A SIC

O primeiro grande problema na área de SIC consistiu na criptografia. Na era anterior ao rádio, essa técnica não passava de uma medida secundária de segurança. Um despacho em papel numa embaixada, por exemplo, normalmente era cifrado, mas a principal medida de proteção consistia não na criptografia em si, visando à preservação do sigilo, da integridade e da autenticidade da informação, mas no cuidado na manipulação da mala diplomática. Embora as mensagens telegráficas fossem freqüentemente codificadas, os usuários confiavam mais na integridade das companhias telegráficas do que nos códigos para segurança.

O advento do rádio introduziu significativas modificações nesse estado de coisas. O seu uso, particularmente para fins militares em tempos de guerra, foi diferente e extremamente valorizado. Antes do rádio, por exemplo, a Real Armada Britânica, que dominou os mares do mundo por muito tempo, tinha apenas noção da localização de seus navios. Era necessário despachar uma flotilha e aguardar notícias de seu regresso, que poderia ser demorado. Poucos anos após a introdução do rádio, porém,

já era possível localizar os navios da frota com maior rapidez. Hoje, naturalmente, com exceção dos submarinos, esse processo é virtualmente instantâneo.

O problema com o rádio, do ponto de vista da segurança, é que suas emissões estão disponíveis no "éter", qualquer um pode captá-las. É possível, até, que mesmo pessoas indesejáveis consigam melhor recepção do que os verdadeiros correspondentes ou interessados. Esse fator promoveu a criptografia a um patamar superior entre as medidas de segurança, no sentido de proteger a integridade, o sigilo e a autenticidade das informações. Passou, então, a ser a única medida de utilização geral na proteção das transmissões radiofônicas.

O resultado foi uma corrida para a automação da criptografia — ao lado da corrida para automação da criptoanálise —, que dominou a criptologia nos anos 1900. Como se viu, por meio século, a criptografia militar foi dominada por máquinas de rotores. A mecanização reduziu a margem de erros, aumentou a velocidade e permitiu muito mais proteção do que se podia conseguir por meios manuais.

No período da Segunda Guerra Mundial, os Estados Unidos da América (EUA), particularmente, já dispunham de sistemas criptográficos seguros, capazes de proteger transmissões telegráficas de até dez caracteres por segundo. Porém, tinham pouca ou nenhuma capacidade para proteger sinais de voz e outros de banda mais larga. O primeiro telefone seguro foi desenvolvido durante a guerra. O sistema, chamado *Sigsaly*[37], provia segurança confiável e comunicação áudio compreensível. Contudo, tinha uma grande desvantagem: o equipamento era por demais espaçoso, pesado e caro (Figura 18).

[37] O *Sigsaly* foi o primeiro sistema seguro de criptografia de voz para telefones. Foi inventado e desenvolvido pela *Bell Telephone Laboratories*, em 1943. As diversas inovações tecnológicas que introduziu revolucionaram a criptografia. O sistema inteiro pesava 55 toneladas e necessitava de 13 pessoas para operá-lo. Durante e após a guerra, foram instaladas unidades em doze diferentes locais do mundo, para garantir comunicação telefônica segura. (SIGSALY Exhibit, 2008)

Figura 18 – *SIGSALY.*
Disponível em: <http://www.nsa.gov/MUSEUM/museu00022.cfm>. Acesso em: 30 jul. 2008.

Não obstante, alguns desses sistemas foram utilizados pelos principais comandos militares. Apesar de limitado no emprego, o *Sigsaly* era a prova de conceito de comunicação-voz segura. Assim, a necessidade de desenvolver criptosistemas mais velozes dominou os desenvolvimentos na área de criptografia por décadas.

Embora a criptografia ainda seja afetada por problemas difíceis de resolver, não é mais o recurso limite para garantir a segurança das comunicações, pelo menos da forma como foi ao longo da maior parte do século XX. Bons sistemas criptográficos atualmente estão disponíveis, assim como os fundamentos matemáticos em que se baseiam agora são amplamente entendidos.

O novo *status* da criptografia é exemplificado pelo **Padrão Avançado de Criptografia** (*Advanced Encryption Standard* – AES), do Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* – NIST) dos EUA, o qual substituiu o **Padrão de Criptografia de Dados** (*Data Encryption Standard* – DES), que havia sido adotado em 1977. Naquela época, a NSA reconheceu a necessidade de usar sistema

criptográfico para proteger informações governamentais também fora da esfera da segurança nacional. Entretanto, considerando que tal sistema não podia atingir seus objetivos sem se tornar público, a NSA julgou que, se isso ocorresse, poderia cair em mãos inimigas. O resultado foi um meio-termo: um sistema considerado forte o suficiente para as pretendidas aplicações da NSA, porém fraco o bastante para não representar obstáculo intransponível, caso se interceptasse algum criptograma DES considerado digno de ser lido. O processo de desenvolvimento, embora formalmente aberto, de fato era mantido fechado.

Na Segunda metade do século XX, a criptografia foi acrescida de um outro problema relacionado à SIC: a segurança da computação. Com o desenvolvimento de computadores capazes de rodar mais de um programa ao mesmo tempo, veio o problema de rodar dois diferentes programas com diferentes padrões de segurança ou diferentes proprietários e evitar que um interferisse no outro. Nas décadas de 1970 e 1980, houve grande otimismo sobre as perspectivas de desenvolver um sistema operacional com diferentes níveis de segurança.

Em grande parte, apresenta-se um novo problema. A questão da segurança da computação vista nos anos 1970 evoluiu para um problema de segurança de redes do século XXI. Alguns problemas foram resolvidos com relação ao passado, outros persistem, e muitos novos têm surgido. Igualmente importante é o fato de que novas ferramentas agora estão disponíveis. Nos anos 1970, a criptografia era primitiva, em comparação com os desenvolvimentos atuais. Dois aspectos da criptografia especialmente cruciais para a segurança computacional — a criptografia de chave pública e a função de *hash* criptográfico, que serão vistas adiante — estavam no seu nascedouro. Igualmente importante, a NSA, cujo monopólio de erudição criptográfica era maior do que agora, era a principal apoiadora das pesquisas de segurança computacional, mas desencorajou a aplicação de muitas técnicas criptográficas ao problema da pesquisa ostensiva. A peça final dos quebra-cabeças é o custo sempre decrescente de computadores. Agora é aceitável dedicar a capacidade computacional à segurança, numa escala inimaginável até pelo menos dez anos atrás.

Na sua essência, a segurança é uma prática orientada para a eliminação de vulnerabilidades e redução de ameaças, efetivas ou potenciais, no ambiente que se deseja proteger. No que se refere à SIC, o emprego de técnicas criptográficas é fundamental, de forma a manter as informações íntegras, garantir-lhes sigilo e autenticidade. Com a aplicação de medidas efetivas e eficazes de segurança, será mais fácil assegurar a continuidade do negócio, seja estatal ou privado, e mitigarem-se os riscos.

Contextualizada a criptografia no âmbito da SIC, serão abordados, no capítulo seguinte, os tipos de aplicação criptográfica.

6. TIPOS DE APLICAÇÕES CRIPTOGRÁFICAS

Há quatro tipos básicos de aplicações criptográficas, tipicamente usadas para conseguir os objetivos de segurança da informação: criptografia simétrica, ou de chave secreta; criptografia assimétrica, ou de chave pública; função *hash* criptográfico; e assinatura digital.

Criptografia simétrica, ou de chave privada: sistema que usa uma mesma chave para cifrar e decifrar a mensagem. Essa chave, portanto, deve ser de conhecimento tanto do emissor quanto do receptor.

Criptografia assimétrica, ou de chave pública: sistema baseado em algoritmos que habilitam o uso de duas chaves: uma pública, para cifrar a mensagem; e outra, diferente, mas matematicamente relacionada, a chave privada, para decifrá-la. Assim, cada usuário possui um par de chaves: uma é abertamente divulgada, a chave pública; a outra é mantida em segredo, a chave privada. Esse sistema também pode ser usado para executar assinaturas digitais e troca de chaves entre correspondentes. Há duas características especiais que devem ser destacadas:

a) uma mensagem cifrada com uma das chaves somente pode ser decifrada com a outra chave correspondente do par; e

b) o conhecimento da chave pública não implica, nem permite, a descoberta da chave privada correspondente;

c) **Função *hash* criptográfico,** ou **função resumo**: é uma função que recebe como entrada (*input*) uma cadeia de caracteres de tamano variável e produz uma saída (*output*) de tamanho fixo, cuja inversão é técnica e matematicamente inviável. Dessa forma, não permite que, a partir de determinados valores, se retorne à informação original. Em outras palavras, a mensagem é resumida. Destacam-se, então, as

seguintes propriedades básicas:

- não é possível fazer a operação reversa, ou seja, feito um resumo é impossível reverter para obter a mensagem original;

- duas mensagens diferentes, quaisquer que sejam, não devem produzir um mesmo resumo. Embora exista a possibilidade, pois não há segurança absoluta, a probabilidade técnica e matemática de produzir resumos idênticos é a mínima possivel. Ademais, a função *hash* criptográfico deve ser de fácil e rápida aplicação; e

- em suma, a função *hash* criptográfico é um resumo criptográfico que pode ser comparado a uma impressão digital, pois cada mensagem possui um valor único de resumo. Assim, até mesmo uma pequena alteração num documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente; e

d) **Assinatura digital**: consiste num método de autenticação, baseado no uso combinado dos algoritmos de criptografia de chave pública operando em conjunto com uma função *hash* criptográfico. Com base na assinatura digital, é possível a certificação digital, que será abordada mais adiante, na parte relativa à ICP-Brasil.

Com relação ainda à criptografia simétrica e à assimétrica, vale destacar que a principal diferença entre elas é que esta última permite que quem conheça a chave pública de determinada pessoa possa enviar-lhe mensagens de forma íntegra, sigilosa e autêntica. Já na simétrica, apenas correspondentes específicos, que disponham da chave privada, podem se comunicar. No geral, a criptografia simétrica é utilizada quando se precisam criptografar grandes quantidades de dados, ou quando o processo tem que ser feito em período determinado de tempo. Já a criptografia assimétrica é mais usada para mensagens curtas, por exemplo, para proteger distribuição de chaves que, por sua vez, serão utilizadas no sistema simétrico. Assim, se conseguirá maior garantia de segurança.

Na prática, o ideal é que cada correspondente disponha de duas chaves: uma pública, disponível a qualquer um e utilizada para cifrar; e outra privada, mantida em segredo pelo usuário, para decifrar.

No sistema assimétrico, as chaves privadas normalmente são geradas de forma independente, mas também podem ser por uma fonte central, como, por exemplo, uma central de segurança corporativa. Contudo, em qualquer caso, ambos os sistemas devem ser mantidos sob o mais estrito sigilo.

Além desses sistemas, também é possível utilizar-se redundância, ou seja, técnicas capazes de criptografar dados já criptografados, o que se poderia designar “supercriptografia”. Significa que a mesma mensagem seria cifrada mais de uma vez, aumentando, assim, a garantia de segurança.

Vistos os tipos de aplicações criptográficas, será mostrada, agora, a evolução da criptografia no Brasil.

7. EVOLUÇÃO DA CRIPTOGRAFIA NO BRASIL

O desenvolvimento autônomo da criptografia no Brasil remonta há 35 anos, quando o Governo Federal identificou a necessidade de adquirir autosuficiência no setor. Este capítulo mostra a trajetória seguida desde então e os progressos obtidos até os dias atuais.

7.1 O "PROJETO PRÓLOGO"

No Brasil, à semelhança dos outros países já citados, as primeiras preocupações efetivas com a criptografia ocorreram no âmbito governamental, ao tempo do Serviço Nacional de Informações (SNI), em 1974, quando seu chefe determinou estudo e criação de um sistema confiável de comunicações para o serviço. Naquele ano, com apoio da Escola Nacional de Informações (ESNI), começou-se a desenvolver sistema de cifração de telex, que, posteriormente, seria estendido a canais de voz e dados.

Contudo, o SNI não era o único orgão de governo a se preocupar com a integridade e segurança dos sistemas de informação. O Ministério das Relações Exteriores (MRE) vivia situação alarmante: a falta de segurança nas ligações com as missões no exterior era tal que não era incomum potências estrangeiras e parceiros comerciais do Brasil terem acesso ao conteúdo de algumas mensagens trocadas entre autoridades brasileiras.

Na época, as soluções de segurança das comunicações no Brasil eram importadas do exterior. Lá fora eram compradas, como "caixas pretas", os meios criptográficos — baseados em códigos e cifras — que se utilizavam para proteger as comunicações mais sensíveis, nos campos diplomático, comercial e militar. Os órgãos governamentais não possuíam capacitação sequer para avaliar a qualidade dos meios que compravam. A vulnerabilidade era grande, pois a tecnologia era dominada por outros países. A solução seria desenvolver um sistema próprio de cifração de

mensagens.

Iniciou-se, então, um projeto, que foi encomendado a um grupo de pesquisadores da Universidade de Brasília (UNB), concluído no final de 1976 e a seguir apresentado à Presidência da República. Em decorrência do sucesso, esse grupo viria, posteriormente, se juntar à equipe da ESNI, com o objetivo de desevolver, de forma autônoma, protótipo de máquina criptográfica genuinamente brasileira. Trabalho altamente sigiloso, foi batizado de “Projeto Prólogo” e iniciado em 1977. Com isso, também se impulsionou, por iniciativa do governo militar, a produção de *chips* no País.

7.2 O CEPESC

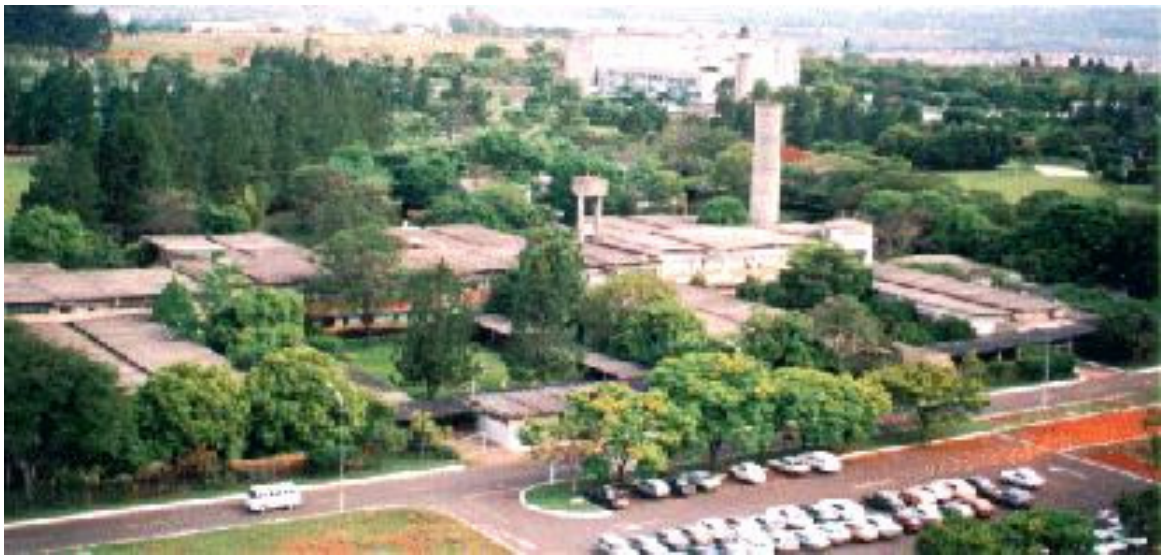


Figura 19 - CEPESC
Disponível em: <http://www.abin.gov.br/modules/mastop_publish/?tac=CEPESC#topo>.
Acesso em: 15 nov. 2008.

Do Projeto Prólogo, originou-se o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC), criado em 19 de maio de 1982, na estrutura do SNI, para responder à necessidade de meios criptográficos de proteção do sigilo das comunicações do governo brasileiro (Figura 19).

Atualmente vinculado à Agência Brasileira de Inteligência, o CEPESC tem como competências regimentais a promoção de pesquisa científica e tecnológica aplicada a

projetos relacionados à segurança das comunicações e a transferência de tecnologia dos seus resultados, considerando os interesses estratégicos envolvidos. Cabe-lhe, também, o papel de órgão de assessoramento e coordenação das propostas de políticas e ações de governo para a utilização da criptografia no País.

Na sua missão básica, o CEPESC já desenvolveu e produziu soluções criptográficas proprietárias para aplicações de Estado, com uma linha de meios de segurança de dados e comunicações, em apoio aos órgãos do governo considerados usuários prioritários. A lista inclui equipamentos criptográficos para telex, autenticadores de assinaturas, criptógrafos para dados e misturadores de voz para rádio e para telefonia. A utilização de vários desses foi interrompida em virtude do processo natural de obsolescência das tecnologias de comunicações.

Para fazer face à velocidade de evolução da microeletrônica e da informática e evitar a obsolescência, o centro tem buscado novos desenvolvimentos com vistas a se manter atualizado, inovando em meios de segurança da informação e das comunicações, conforme as necessidades e as disponibilidades dos seus usuários prioritários.

A força de trabalho do CEPESC é constituída de pesquisadores, tecnólogos e técnicos qualificados, recrutados em universidades e no mercado de trabalho, treinados e aperfeiçoados em suas atividades. Atualmente estão sendo realizados estudos para a elaboração de convênios com universidades e instituições de pesquisa, públicas e privadas, nacionais e internacionais, com o objetivo de acompanhar o estado da arte em tecnologias de ponta de interesse do Estado brasileiro.

Atualmente o CEPESC disponibiliza bens e serviços, valendo destacar: telefone seguro, que proporciona criptografia de voz e dados em linhas comuns de telefonia, em nível estratégico; módulo criptográfico portátil, que viabiliza a criptografia em nível estratégico em microcomputadores comuns sem a necessidade de acesso ao interior da máquina; equipamento para cifração de dados, que permite a proteção de links de comunicação com velocidade de até 10 Mbps; sistema de seqüências aleatórias com alto grau de segurança criptográfica e interface gráfica para emprego em

microcomputadores.

Na categoria de produtos e serviços, o CEPESC fornece suporte técnico em segurança da informação a órgãos estatais, com destaque para a Presidência da República, o Ministério da Defesa e seus Comandos, o Ministério das Relações Exteriores, o Ministério da Justiça e o Departamento de Polícia Federal. Também atua junto ao Judiciário, apoiando as eleições desde 1996, participando do projeto "Voto Informatizado", sob a coordenação e responsabilidade do Tribunal Superior Eleitoral (TSE). Em relação a esse projeto, o CEPESC foi solicitado a desenvolver um sistema de segurança criptográfica para garantir a inviolabilidade dos resultados ao término da votação, durante a fase de transmissão dos votos das urnas eletrônicas para os computadores utilizados na totalização dos votos. Ademais, colabora com a implementação do Programa Nacional de Proteção ao Conhecimento (PNPC), de responsabilidade da ABIN.

O Centro também desenvolveu, a pedido da Imprensa Nacional, uma solução em *software* para a certificação de origem e a manutenção do sigilo dos documentos eletrônicos enviados pelos órgãos do governo e por outras entidades para a publicação no Diário Oficial da União. O sistema permite identificar a autoria e preservar o sigilo de um dado documento.

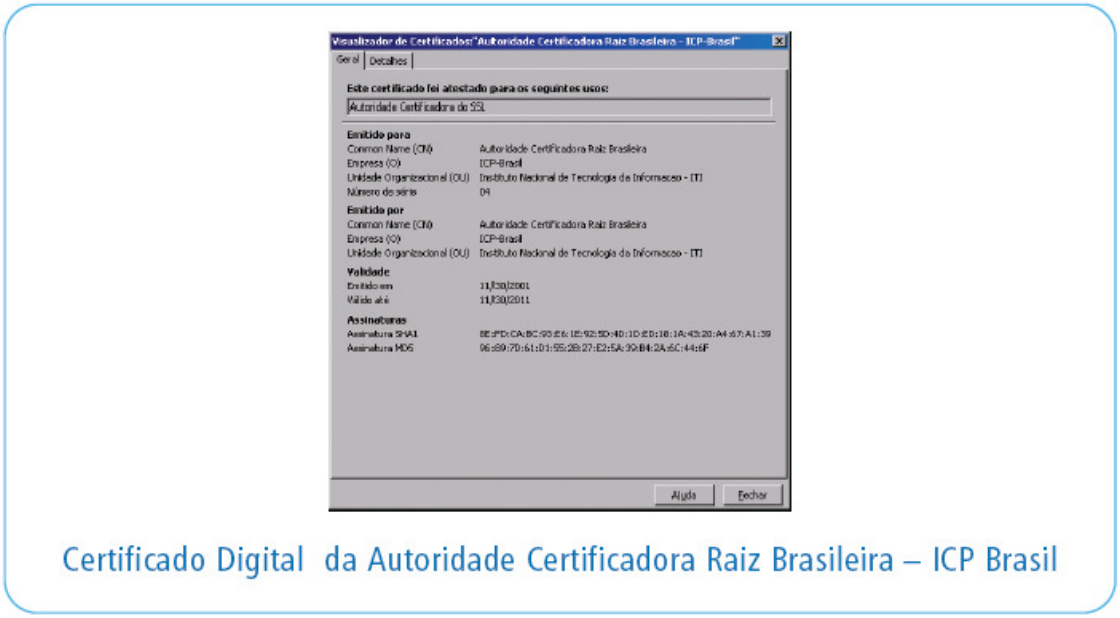
7.3 O ITI E A ICP-BRASIL

Outro órgão que se destaca na área de segurança da informação e criptografia é o Instituto Nacional de Tecnologia da Informação (ITI). Autarquia federal ligada à Casa Civil da Presidência da República, o ITI foi criado em 2001 como Autoridade Certificadora Raiz (AC Raiz), com o objetivo de manter a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

A ICP-Brasil, por sua vez, originou-se da percepção do Governo Federal acerca da importância de regulamentar as atividades de certificação digital no País. Compõe-se

de: entidades, padrões técnicos e regulamentos, para suportar um sistema criptográfico com base em certificados digitais.

Certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos. Normalmente apresenta as seguintes informações: nome da pessoa ou entidade a ser associada à chave pública; endereço eletrônico (*e-mail*); período de validade do certificado; chave pública; nome e assinatura da entidade que assinou o certificado; e número de série (Figura 20).



Certificado Digital da Autoridade Certificadora Raiz Brasileira – ICP Brasil

Figura 20
Disponível em: <https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf>.
Acesso em 3 nov. 2008

Na prática, o certificado digital funciona como uma carteira de identidade virtual, que permite a identificação segura de uma mensagem ou transação em rede de computadores. O processo de certificação digital utiliza procedimentos lógicos e matemáticos para assegurar as características dos dados e informações referidas como DISA (disponibilidade, integridade, sigilo e autenticidade).

Os certificados da ICP-Brasil asseguram: eficácia probatória dos documentos assinados; padrões internacionais de segurança nas instalações e procedimentos;

declaração pública de práticas; identificação presencial do titular do certificado; seguro de responsabilidade civil; guarda de dados por tempo ilimitado; auditoria prévia e anual nas entidades; e interoperabilidade.

Como exemplos de uso de certificados ICP-Brasil, podem-se citar, dentre outros: o Sistema Brasileiro de Pagamentos; escrituração fiscal; nota fiscal eletrônica; operações de câmbio; apólices de seguros; pregões eletrônicos; *internet banking*; e *mobile banking*.

Para adotar as medidas necessárias ao funcionamento da ICP-Brasil, a Presidência da República designou um "Comitê Gestor da ICP-Brasil" (CG-ICP), por meio do decreto nº. 6.605, de 14 de outubro de 2008.

7.4 A RENASIC

Também no âmbito do Governo Federal, mais recentemente foi instituída a Rede Nacional de Segurança da Informação e Criptografia (RENASIC), visando ao cumprimento dos objetivos e diretrizes da Política de Segurança da Informação, prevista no decreto 3.505/2000. Sua meta é elevar a competência brasileira em segurança da informação e criptografia, por meio do estabelecimento e fomento da integração das pesquisas brasileiras em universidades, institutos de pesquisa, órgãos governamentais e empresas.

Criada pela Portaria Nº 31/GSIPR, de 6 de outubro de 2008, e vinculada ao GSIPR, a RENASIC busca o estabelecimento de um nível de excelência das pesquisas nacionais nas áreas de segurança da Informação e criptografia, por intermédio dos seguintes instrumentos:

- fortalecimento e integração das pesquisas em Segurança da Informação e Criptografia no Brasil, diminuindo a atual fragmentação das competências através da

criação de uma infraestrutura de pesquisa e de sua organização em laboratórios virtuais e, assim, estabelecer uma agenda de pesquisa e de projetos conjuntos nessas áreas;

- estabelecimento de laboratórios virtuais que visem a fomentar a pesquisa entre os membros da RENASIC;

- melhoria do estado da arte na teoria e prática da Segurança da Informação e Criptografia no Brasil, igualando-a aos grandes centros internacionais, por meio de: aumento da compreensão dos algoritmos e protocolos existentes; expansão das bases teóricas da Segurança da Informação e Criptografia; e desenvolvimento de melhores algoritmos criptográficos, protocolos e implementações, obedecendo às seguintes diretrizes: alta performance, baixo custo, alta segurança; e

- desenvolvimento de infraestrutura comum, incluindo: ferramentas para a avaliação dos algoritmos de criptografia; ambientes de avaliação para *hardware* e *software* criptográficos; instrumentação física e lógica para análise de ataques secundários (*side-channel atacks*), suas respectivas contramedidas, além de ferramentas para avaliação dos esquemas de defesa cibernética e forense computacional.

7.5 O CPQD

O Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) é uma instituição independente, focada na inovação com base na(s) tecnologia(s) da informação e das comunicações (TIC), tendo como objetivo contribuir para a competitividade do País e para a inclusão digital da sociedade.

Embora o CPQD não atue com foco direto na área de SIC, suas pesquisas e produtos agregam cada vez mais novas tecnologias e são de inegável aplicação para fins de

segurança da informação e das comunicações. O Centro desenvolve amplo programa de pesquisa e desenvolvimento, o maior da América Latina em sua área de atuação, gerando soluções em TIC que são utilizadas em diversos setores: telecomunicações, financeiro, energia elétrica, industrial, corporativo e administração pública.

Criado em 1976, como Centro de Pesquisa e Desenvolvimento da Telebrás, o CPqD era uma empresa estatal que detinha o monopólio dos serviços públicos de telecomunicações no Brasil. Desde aquela época, ocupa posto de vanguarda tecnológica, sintonizado com o futuro e antecipando-se às necessidades de uma sociedade que se modifica e evolui em alta velocidade. Em 1998, com a privatização do sistema Telebrás, o CPqD tornou-se uma fundação de direito privado, ampliando a sua atuação, tanto no escopo como na abrangência do mercado.

Centrais digitais, antenas, sistemas de transmissão digital, equipamentos de transmissão óptica, fibra óptica, laser semicondutor, centrais de comutação por pacote, telefone público a cartão indutivo, centrais de telex, complexos sistemas de suporte a operações e negócios e tantas outras tecnologias desenvolvidas no CPqD, que somadas ao conhecimento sobre o mercado e a sociedade brasileira, em seus aspectos culturais, socioeconômicos e históricos envolvidos com TIC, consolidaram no CPqD potencial inovador único na área.

Em termos de segurança da informação e criptografia, o CPqD trabalha com Segurança em Voz sobre IP (*Internet Protocol),* ou VoIP, no sentido de garantir as características de DISA; gestão integrada de fraude e eventos, monitorando e correlacionando, em tempo real, as regras de negócios e os incidentes de segurança; e, mais importante, na proteção de infraestruturas críticas, em que monitora instalações, serviços e bens considerados críticos.

7.6 O DSIC/GSIPR

Apesar de o DSIC não atuar diretamente com pesquisa e desenvolvimento em criptografia, suas competências estão diretamente relacionadas e o Departamento tem

desenvolvido importante papel no que se refere a sensibilização, conscientização e treinamento sobre segurança da informação e comunicações, alertando para a necessidade de emprego da criptografia para assegurar integridade, confidencialidade e autenticidade das informações.

De acordo com com o decreto de criação do DSIC[38], na estrutura regimental do GSIPR, compete-lhe, dentre outras atribuições: “adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento – SISC, de pessoas e empresas, no trato de assuntos, documentos e tecnologias sigilosos”; “planejar e coordenar a execução das atividades de seguranca da informação e comunicações na administração pública federal”; e “definir requisitos metodológicos para implementação da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal”.

No exercício dessas competências, dentre seus programas mais importantes, o DSIC trabalha no desenvolvimento de propostas de projeto de lei sobre o uso e a comercialização da criptografia no Brasil e, junto com o CEPESC, de padrões criptográficos para as funções administrativas e de Estado.

Dessa forma, é importante fazer-lhe menção, até considerando que este Curso de Especialização de Gestão em Segurança da Informação e Comunicações é exemplo de parte dos seus bem sucedidos esforços.

Feitas todas essas considerações até aqui, chegou-se ao momento das discussões, que serão feitas no capítulo que se segue.

[38] Decreto n°. 5.772, de 8 de maio de 2006.

8. DISCUSSÕES

Depois das pesquisas realizadas, verificou-se que ainda não há no Brasil uma política especificamente voltada para criptografia e a legislação sobre o assunto é praticamente nula. Apenas os decretos 3.505/2000 e 4.553/2002 fazem-lhe alguma referência, porém de forma superficial que não atende aos objetivos que se buscam para uma efetiva segurança da informação e das comunicações no País.

Para piorar essa situação, constata-se encolhimento e envelhecimento da massa crítica envolvida com criptografia, o que não é prerrogativa apenas dessa área. Na administração do presidente Collor, iniciada em 1980, a APF foi praticamente desmantelada. Servidores sem estabilidade foram sumariamente demitidos; muitos se aposentaram; requisitados foram devolvidos aos seus órgãos de origem; recursos foram cortados. O SNI, ao qual se vinculava o CEPESC, foi praticamente extinto. O que se verificou com a Atividade de Inteligência foi a permanência de um reduzido efetivo, grande número de instalações modernas para a época caindo na ociosidade e sucateamento de equipamentos.

A reversão desse quadro tem sido lenta, mas não na medida do desejável. A reposição dos quadros é difícil, pois submete-se às regras do Serviço Público, que exigem concurso e autorização de outros órgãos do governo. Ademais, técnicos e especialistas em matérias como criptografia não se encontram facilmente disponíveis no mercado de trabalho.

Esforços no sentido de melhorar esse estado de coisas demandam parcerias estratégicas, com envolvimento conjunto dos poderes Executivo, Legislativo e Judiciário e da iniciativa privada, com base em amplo debate público e sob o amparo da lei. Um consenso derivado de entendimento entre legisladores, executores, juristas e o setor privado certamente conduzirá a maior aceitação geral e confiança na criptografia, inclusive por parte da opinião pública, permitindo a retomada de um setor, em moldes desejáveis, de extrema importância para a segurança do Estado e da

sociedade brasileiros.

Não obstante, o setor tem sobrevivido e contribuído de forma competente para a segurança da informação e das comunicações no País. O mais amplo emprego estratégico da criptografia vem ao encontro dos interesses nacionais e uma política nesse sentido deve alinhar-se com as necessidades das forças de mercado o máximo possível. Da mesma forma, deve-se enfatizar a utilização por usuários domésticos, que devem estar em condições de determinar o que precisam em termos de funcionalidade, proteção e implementação, de acordo com suas necessidades de segurança, de forma que melhor se adequem.

Além disso, é conveniente que se prevejam controles de importação e exportação de tecnologias, produtos e informações técnicas relacionados à critografia, com o cuidado de que esses controles não constituam impedimento para os esforços voltados para a segurança da informação.

Ademais, há que se ter em mente que criptografia é uma tecnologia de uso dual, com importantes aplicações nos âmbitos civil e militar. Devido às suas implicações críticas no campo da defesa, há poucas alternativas disponíveis que a possam substituir.

Como já se salientou, convém enfatizar, a criptografia é útil às autoridades legais e à segurança nacional como um todo. Ao mesmo tempo, também pode ser prejudicial, tendo em vista que é possível sua utilização por criminosos, para acobertar suas atividades ilícitas. Se as autoridades responsáveis pela aplicação da lei não tiverem acesso às informações criptografadas dos agentes do ilícito, as investigações e julgamentos por certo ficarão prejudicados. Por esse motivo, passos específicos devem ser tomados a fim de mitigar esse tipo de dificuldades.

Na realidade, as necessidades de segurança nacional demandam novas capacidades e habilidades para melhor fazer face aos desafios representados pela criptografia no momento presente.

O problema da segurança da informação, atualmente, requer que as instituições governamentais e privadas compitam em base mundial, trocando e partilhando informações sensíveis com parceiros apropriados, ao mesmo tempo protegendo-as contra competidores, vândalos e governos estrangeiros. O Governo Federal tem papel fundamental nesse esforço, de forma a assegurar que informações sensíveis, de caráter político, econômico e militar, sejam protegidas de ações hostis ou de interesses escusos.

Esforços devem ser feitos no sentido de ampliar e aperfeiçoar os sistemas já existentes, particularmente em termos governamentais. E esses esforços necessitam ser direcionados por uma estratégia ampla e geral, em que papéis e responsabilidades sejam claramente delineados, com liderança e apoio técnico e adequados.

Embora haja alguns progressos na proteção das infraestruturas informacionais, esforços contínuos necessitam estar sempre em progresso, no sentido de acompanhar o ritmo em que essas evoluções ocorrem.

Criptografia é uma técnica de uso dual, surgida dos campos de batalha, na guerra da espionagem. Serve tanto para fins pacíficos quanto agressivos, criminosos, ilícitos. Depende de quem usa. Dessa forma, Estado e governos precisam se precaver. E têm que dominar todas as formas de criptografia, para que estejam em condições de fazer face ao inimigo. Por isso, é importante o controle governamental.

Embora nossa monografia seja voltada para sensibilização/conscientização acerca do emprego da criptografia para a segurança da informação — e segurança genericamente falando —, é importante mostrar e alertar para os usos que podem ser feitos dessa técnica. Até do ponto de vista da espionagem, levando-se em consideração estratégia de guerra: há que se conhecer o inimigo para melhor combatê-lo. Por isso, chamamos a atenção para o uso destinado a fins criminosos que pode ser feito da criptografia.

Imagine-se o que se pode fazer hoje com as modernas tecnologias. Nanotecnologia para micropontos, por exemplo, mescla de criptografia com estagnografia, em que é possível criptografar, minimizar, esteganografar.

Numa época de acelerados avanços tecnológicos, particularmente na área de eletrônica e telecomunicações, muitos interesses nacionais vitais requerem proteção efetiva de informações. Quando usada em conjunto com outras formas de segurança da informação, a criptografia constitui-se em arma poderosa.

Compete ao governo, portanto, adotar medidas e políticas para promover e encorajar o uso cada vez maior dessa ferrramenta, no sentido de garantir proteção dos dados e informações relativos a pessoas, negócios, do próprio governo e da Nação como um todo, tudo isso em estrito atendimento aos preceitos legais em vigor e aos direitos dos cidadãos de acesso à informação.

Tecnicamente a criptografia preocupa-se com as comunicações deliberadamente designadas para guardar segredos contra inimigos. As formas clássicas de escrita secreta, historicamente usadas, foram eficientes a seu tempo, até quando o princípio da oportunidade não era característica essencial. Contudo, na maior parte, caíram em desuso, por obsolescência.

As cifras clássicas normalmente são suscetíveis a ataques diretos ao texto cifrado, às vezes mesmo sem o conhecimento do próprio sistema, com o emprego de ferramentas tais como análise de freqüência.

Na medida em que o tempo passa e a ciência evolui, novas técnicas são descobertas para garantir a segurança da informação, logo seguidas das ferramentas para neutralizá-las, o que pode demorar mais ou menos tempo, dependendo dos interesses das partes, das condições tecnológicas e econômicas para investir em pesquisa e compra de material.

Embora se possa imaginar que existam cifras aparentemente imunes à criptoanálise, não existe sistema perfeito, como comprovou a Enigma. Sob esse aspecto, excesso de confiança pode ser fatal em determinadas situações, já que diminui a sensação de insegurança, o que pode fragilizar o estado de vigília e alerta.

Como se demonstrou, o fator fundamental nesse jogo de inteligência é o elemento humano, passível de cometer erros e/ou falhas ou mesmo servir de fonte de dados para a espionagem adversa. Na guerra da informação, os inescrupulosos partem do princípio de que tudo é permitido.

Originalmente operadas a mão ou com aparelhos mecânicos simples, os sistemas clássicos de escrita secreta atualmente são substituídos por outros mais modernos, que utilizam computadores e outras tecnologias digitais, o que os torna praticamente invulneráveis, mas não, de maneira alguma, infalíveis.

As cifras clássicas foram a origem de todos os sistemas criptográficos e são sua fonte de inspiração. Hoje, apenas se mudam os cenários e as armas. De um mundo compartimentado, que empregava estiletes e tabletes de madeira encerados ou lápis e papel, na Sociedade do Conhecimento globalizado se usam teclados, ou mesmo voz, e *bits/bytes*. Mas o objetivo é o mesmo: garantir a segurança da informação e das comunicações.

Aqui se encerra toda a argumentação que se julgou necessária apresentar, restando, por fim, apresentar as considerações finais, por meio da conclusão, e traçar algumas perspectivas com relação a trabalhos futuros, o que será feito a seguir, antes de se proceder às Referências Bibliográficas.

9. CONCLUSÃO E TRABALHOS FUTUROS

Esta pesquisa teve como objetivos explicar a importância da criptografia para a segurança da informação e das comunicações, sejam governamentais ou particulares, e a necessidade de se adotarem estratégias e táticas criptográficas para assegurar, de forma eficiente e eficaz, integridade, sigilo e autenticidade de dados e informações, particularmente na Administração Pública Federal.

Ademais, buscou-se apresentar subsídios que possam servir de instrumento de sensibilização e conscientização quanto à necessidade de adoção de sistema de gestão de segurança da informação e das comunicações, com foco no uso da criptografia, para a proteção das informações e comunicações governamentais, particularmente as consideradas sensíveis e aquelas cujo sigilo seja de interesse da segurança da sociedade e do Estado.

Tendo em vista que, no âmbito da Administração Pública Federal (APF) — à qual se dirige o curso que ora concluímos —, o encarregado de coordenar as atividades de segurança da informação é o Gabinete de Segurança Institucional da Presidência da República (GSIPR), pretende-se, também, que este trabalho constitua instrumento útil ao exercício de suas atribuições, pelo menos do ponto de vista cultural e educativo quanto à importância da criptografia.

Como desdobramento, esta pesquisa visou a constituir instrumento de sensibilização e conscientização até mesmo do cidadão comum, quanto à importância da criptografia para o resguardo da inviolabilidade de informações relativas à intimidade, à vida privada, à honra e à imagem das pessoas.

Dentre os desafios identificados para a consecução desses objetivos, podem-se destacar: desenvolvimento de um plano nacional de segurança da informação e criptografia que incorpore aperfeiçoamento do sistema de troca de informações e

levantamento de vulnerabilidades entre o governo federal e o setor privado, assim como no seio do próprio governo; aperfeiçoamento das capacidades de análise e alerta com relação a ameaças físicas e cibernéticas; e encorajamento das entidades fora do governo federal para ampliar seus esforços e capacidades relacionados à SIC e à criptografia. Sob esse aspecto, atenção especial também deve ser dada à academia e aos setores privados que se dedicam a pesquisa e desenvolvimento na área de criptografia, com incentivo, na medida do possível, das próprias instituições governamentais. Por fim, deve-se mencionar a parte educativa, com sensibilização, conscientização e treinamento dos usuários, independentemente do grau ou nível hierárquico. Vale lembrar que o elo mais fraco da corrente que representa a segurança da informação reside exatamente no fator humano.

Embora este trabalho esteja focado primeiramente na criptografia, esta seria apenas parte de uma política de segurança da informação abrangente. Sem tal política, de longo alcance, qualquer alteração no estado de coisas da criptografia seria inócua ou teria pouco impacto operacional.

Cabe ao governo desenvolver mecanismos no sentido de promover a segurança da informação também no setor privado. O próprio governo não está bem organizado para enfrentar os desafios representados pela sociedade da informação. Ademais, nenhuma agência governamental tem responsabilidade para promover segurança da informação no setor privado.

Aqueles que pretendem maior segurança da informação e também aqueles que necessitam acesso legal à informação, armazenada ou em trânsito, devem participar de um amplo e robusto processo, a incluir as altamente competitivas questões e interesses de criptografia, que, invevitavelmente, surgirão ao longo do tempo.

É importante que se estruturem ações integradas entre governos federal, estaduais e municipais, sem esquecer da iniciativa privada e da academia, de modo a estabelecer metas comuns para equacionar os principais problemas nas áreas de criptografia e segurança da informação. Atenção especial merecem itens e instalações que tenham

dano potencial associado, em face da sua sensibilidade. Esses envolvem infraestruturas críticas, de segurança pública, energia, água, economia e finanças e malhas de comunicação por terra, mar e ar.

O Governo Federal tem papel fundamental no sentido de promover ativamente a segurança dos sistemas de informação e redes críticas necessárias ao bem estar da Nação. Em outros setores, caberia ao governo prover experiência, apoio e informações.

Em suma, pretende-se com esse debate propiciar subsídios que conduzam a maior sigilo e proteção da informação e das comunicações, sejam individuais, corporativas ou governamentais. Assim, objetiva-se contribuir para a redução de crimes financeiros e econômicos e da espionagem internacional, além do crime organizado, de ações terroristas e mesmo crimes comuns.

Por fim, espera-se que este trabalho seja importante para ampliar a segurança como um todo e a garantia dos sistemas de informação, particularmente, que estão a serviço da Administração Pública Federal e da Nação como um todo.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 17799** – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. 2 ed. Rio de Janeiro: ABNT, 2005. 120 p.

ALBA, Ernest. ***Evolution: The "Debate"***. In: Ernest Alba's Blog. Disponível em: <http://blogs.mit.edu/CS/blogs/eialba/archive/2006/05.aspx>. Acesso em: 12 out. 2008.

ANSWERS.COM. SCI-TECH DICTIONARY. ***Substitution cipher***. Disponível em: <http://www.answers.com/topic/substitution-cipher>. Acesso em: 29 jun. 2008.

ATIS Committee PRQC. ***ATIS Telecom Glossary 2007***. Estados Unidos: disponível em: <http://www.atis.org/glossary/definition.aspx?id=6815>. Acesso: em 15 ago. 2008.

BARKER, Elaine B.; Barker, William C.; Lee, Annabelle.U.S. ***Information Security – Guideline for Implementing Cryptography In the Federal Government***. NIST Special Publication 800-21. 2. ed. Gaithersburg, MD, USA: Department of Commerce. Technology Administration. National Institute of Standards and Technology – NIST, 2005. 97 p. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf>. Acesso em 1° nov. 2008.

BARRETO, Ricardo (barretto@cff.com.br_br); Leça, José (jalp@cff.com.brjalp@br); Montagna, Camila (cdr@cff.com.br); Arata, Seiiti (saj@cff.com.br). **Criptografia no Brasil**. São Paulo: Câmara Brasileira de Comércio Eletrônico – Grupo de Trabalho de Criptografia Comercial, 2003. Disponível em: <http://www.camara-e.net/_upload/SLIDESCFF.PDF>. Acesso em: 3 nov. 2008.

BERKOWITZ, Bruce D. *and* GOODMAN, Allan E. ***Best Truth. Intelligence in the Information Age***. New Haven: Yale University Press, 2000. 203 p.

BERTOL, Viviane Regina Lemos. **O ITI e a Infra-estrutura de Chaves Públicas Brasileira**. instituto nacional de tecnologia da informação – ITI. Disponível em <http://www.tecsi.fea.usp.br/eventos/contecsi2006/port/palestrantes/ITI-Contecsi_2006.pdf>. Acesso em 15 jan. 2009.

BLETCHLEY PARK NATIONAL CODES CENTER. ***Bletchley Park History –*** *World War II History*. Bletchley Park, Reino Unido: 2008. Disponível em: <http://www.bletchleypark.org.uk/content/hist/wartime.rhtm>. Acesso em: 30 jun. 2008.

_____. ***Machines behind the codes — Enigma***. Bletchley Park, Reino Unido: 2008. Disponível em: <http://www.bletchleypark.org.uk/content/machines.rhtm>. Acesso em: 30 jun. 2008.

BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm>. Acesso em: 8 jun. 2008.

BRASIL. **Decreto nº. 27583**, de 14 de dezembro de 1949. Aprova o Regulamento para a Salvaguarda das Informações que interessam à Segurança Nacional. Disponível em: <http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=159804>. Acesso em 10 nov. 2008.

BRASIL. **Decreto nº 79.099**, de 6 de janeiro de 1977. Aprova o Regulamento para Salvaguarda de Assuntos Sigilosos. Disponível em: <http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=102380>. Acesso em 10 nov. 2008

BRASIL. **Decreto nº. 3.505**, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm>. Acesso em: 8 jun. 2008.

BRASIL. **Decreto nº. 3.587**, de 5 de setembro de 2000. Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov, e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/d3587.htm>. Acesso em: 30 out. 2008.

BRASIL. **Decreto nº. 3.996**, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm>. Acesso em 30 out. 2008.

BRASIL. **Decreto nº. 4.376**, de 13 de setembro de 2002. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei n°. 9.883, de 7 de dezembro de 1999, e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/2002/Quadro_2002.htm>. Acesso em: 15 jun. 2008.

BRASIL. **Decreto nº. 4.553**, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/Quadro_2002.htm>. Acesso em: 15 jun. 2008.

BRASIL. **Decreto n°. 5.772**, de 8 de maio de 2006. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil/_Ato2004-2006/2006/Decreto/D5772.htm>. Acesso em: 30 jul. 2009.

BRASIL. **Decreto nº. 6.605**, de 14 de outubro de 2002. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileiras – CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6605.htm>. Acesso em: 3 mar. 2009.

BRASIL. **Decreto-Lei nº. 2.848**, de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso em: 10 nov. 2008.

BRASIL. **Lei n°. 8.159**, de 8 de janeiro de 1991. Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/QUADRO/1991.htm>. Acesso em: 15 jun. 2008.

BRASIL. **Lei n°. 9.883**, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/QUADRO/1999.htm>. Acesso em: 15 jun. 2008.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **PORTARIA Nº 31 – GSIPR/CH**, de 6 de outubro de 2008: Institui a Rede Nacional de Segurança da Informação e Criptografia – RENASIC. Disponível em <http://www.abdir.com.br/legislacao/legislacao_abdir_7_10_08_1.pdf>. Acesso em 10 mar. 2009.

BUDIANSKY, Stephen. ***Her Majesty's Spymaster***. New York: Viking Penguin, 2005. 235 p.

CHEMIN, Beatriz Francisca. **Guia Prático da UNIVATES para trabalhos acadêmicos**. Lajeado: UNIVATES, 2005.

CHIAVENATO, Idalberto. **Introdução à Teoria Geral da Administração**. São Paulo: Editora McGraw-Hill do Brasil, Ltda, 1977. 562 p.

COLLIN, S.M.H. ***Dictionary of ICT***. 4 ed. London: Bloomsbury, 2004. 280 p.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGIBR). **Cartilha de Segurança na Internet**. São Paulo: CGIBR, 2006. 117p. Disponível em: <HTTP://dsic.planalto.gv.br/documentos/cartilha_segurança_internet.pdf>. Acesso em 30 out. 2008.

COMMITTEE ON NATIONAL SECURITY SYSTEMS – CNSS. *Instruction No. 4009.* ***National Information Assurance (IA) Glossary****.* EUA: CNSS, 2006. 86 p. *Home page*: <cnss@radium.ncsc.mil>.

DULLES, Allen W. ***The Craft of Intelligence***. Guilford, Connecticut: The Lyon Press, 2006. 279 p.

ESCRITA DA DISSERTAÇÃO. Disponível em: <http://www.inf.ufsc.br/~raul/disciplinas/metodologia/4-EscritadaDissertacao.ppt>. Acesso em: 30 jun. 2008.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA). ***Regulation (EC) Nº. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security.*** <http://europa.eu/scadplus/leg/en/lvb/l24153.htm>. Acesso em: 5 dez. 2008.

FARINA, Sérgio. **Referências bibliográficas e eletrônicas**. São Leopoldo: UNISINOS, 1997.

GEHLEN, Reinhard. **O Serviço Secreto**. Rio de Janeiro: Editora Artenova S.A., 1972. 382 p.

G1. **Angolanos são presos com cocaína escondida no estômago**. In: Rio de Janeiro/Tráfico de drogas. Rio de Janeiro: globo.com, 2008. Disponível em: <http://g1.globo.com/Noticias/Rio/0,,MUL338045-5606,00.html>. Acesso em: 14 nov. 2008.

HOUAISS, Antonio. **Dicionário Eletrônico Houaiss da Língua Portuguesa**. 2. ed. São Paulo: Ed. Objetiva, 2007. CD-ROM.

ICP Brasil – Infra-Estrutura de Chaves Públicas Brasileiras. **Definições do glossário**. Brasília: Presidência da República. Disponível em: <https://www.icpbrasil.gov.br/duvidas/glossary/criptografia?searchterm=criptografia>. Acesso em: 25 out. 2008.

INSTITUTE FOR TELECOMMUNICATIONS SCIENCES – ITS. *Federal Standard 1037C – **Telecommunications: Glossary of Telecommunication Terms***. Boulder, Colorado, EUA: 1996. Disponível em: <http://www.its.bldrdoc.gov/fs-1037/>. Acesso em: 15 ago. 2008.

KAHN, David. ***The Codebreakers**: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner, 1996. 1200 p.

KAUFMAN, Charlie; PERLMAN, Radia; SPECINER, Mike. ***CRAKING CLASSIC CIPHERS***. In: CS572: Computer Security. EUA: Prentice Hall PTR, 2002. Disponível em: <http://faculty.rivier.edu/bhiggs/web/cs572aweb/Assignments/CrackingClassicCiphers.htm>. Acesso em: 29 jun. 2008.

KOPPLIN, John. ***An Illustrated History of Computers.** Part 3*. Estados Unidos: Computer Science Lab., 2002. Disponível em: <http://www.computersciencelab.com/ComputerHistory/HistoryPt3.htm>. Acesso em: 30 jun. 2008.

LYCETT, Andrew. ***Breaking Germany's Enigma Code***. In: World Wars — World War Two. Londres, Reino Unido: BBC Home, 2001. 6p. Disponível em: <http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_05.shtml>. Acesso em: 17 nov. 2008.

NATIONAL SECURITY AGENGY – CENTRAL SECURITY SERVICE. National Cryptologic Museum. **SIGSALY Exhibit**. USA: NSA/CSS, 2008. Disponível em: <http://www.nsa.gov/MUSEUM/museu00022.cfm>. Acesso em 30 jul. 2008.

NATIONAL SECURITY AGENCY – NSA. Systems and Network Attack Center. ***The 60 Minute Network Security Guide** (First Steps Towards a Secure Network Environment)*. Ft. Meade, MD, USA: 2006. 48 p. Disponível em: <http://www.nsa.gov/snac/downloads_all.cfm>. Acesso em: 25 set. 2008.

O QUE É CERTIFICAÇÃO DIGITAL? Disponível em: <https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf>. Acesso em: 3 nov. 2008.

PC Magazine – PCMAG.COM. ***PCMAG.COM Encyclopedia***. EUA. Disponível em: <http://www.pcmag.com/encyclopedia_term/0,2542,t=cryptography&i=40522,00.asp>. Acesso em: 1° nov 2008.

POLMAR, Norma *and* ALLEN, Thomas B. ***Spy Book*** – *The Encyclopedia of Espionage*. New York: Random House, 1998, 645 p.

POSTMAN, Neil. ***Language Education in a Knowledge Context (1980)***. In: A Review of General Semantics, v37 n°. 1. EUA: Spr 1980. p. 25-37. Disponível em: <http://www.neilpostman.org/articles/etc_37-1-postman.pdf>. Acesso em: 8 nov. 2008.

PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. ABIN. **CEPESC**. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/?tac=CEPESC#topo>. Acesso em: 15 nov. 2008.

_____. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações – DSIC. **A importância da Segurança da Informação e Comunicações para a Administração Pública Federal.** In: 30 anos de TI no TCU – Fórum de Tecnologia da Informação. Disponível em: <HTTP://portal2.tcu.gov.br/portal/pls/portal/docs/783755.PDF>. Acesso em: 31 jul. 2009.

_____. Instituto Nacional de Tecnologia da Informação – ITI. **CRIPTOGRAFIA**. In: O que é Certificação Digital? Brasília: ITI/PR, 2005. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 3 nov. 2008.

RAMOS, Anderson et al. ***Security Officer – 1***. Guia oficial para formação de gestores em Segurança da Informação. Porto Alegre: Ed. Zouk, 2006.

_____. ***Security Officer – 2***. Guia oficial para formação de gestores em Segurança da Informação. Porto Alegre: Ed. Zouk, 2007.

RISK REACTOR. ***Invisible UV Inks!*** Huntington Beach, CA, USA: Risk Reactor, 2008. Disponível em: <http://www.riskreactor.com/Invisible_Inks/Invisible_Inks_Main.htm>. Acesso em: 29 ago.2008.

SAWYER, Ralph D. ***The Tao of Spycraft***. *Intelligence and Practice in Traditional China.* Colorado: Westview Press, 2004. 621 p.

SCHNEIER, Bruce. ***Applied Cryptography*** – *Protocols, Algorithms, and Source Code in C.* 2 ed. New York: John Wiley & Sons, Inc., 1996. 758 p.

SCIENCE IN AFRICA. Africa's First On-Line Science Magazine. *Police and business support Microdot technology*. South Africa: 2005. Disponível em: <http://www.scienceinafrica.co.za/2005/november/microdot.htm>. Acesso em: 28 ago. 2008.

SECURITY SERVICE – MI5. ***How To Make Invisible Ink***. REINO UNIDO: MI-5, 2007. Disponível em: <http://www.mi5.gov.uk/output/Page295.html>. Acesso em: 28 ago.2008.

SHELDON, R.M. ***Espionage in the Ancient World*** – *An Annotated Bibliography*. North Carolina: McFarland & Company, Inc., Publishers: 2003. 232 p.

SIMONS, Gustav J. ***Contemporary Cryptology*** – *The Science of Information Integrity*. Piscataway, NJ, EUA: IEEE Press, 1991.

SINGH, Simon. ***The Code Book*** – *The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor Book, 1999. 412 p.

STALLINGS, William. ***Cryptography and Network Security*** – *Principles and Practices.* 3 ed. New Jersey, EUA: Prentice Hall, 2003.

STEARNS, Peter N., General Editor. ***The Encyclopedia of World History***. 6. ed. New York: Houghton Mifflin Company, 2001. 1243 p.

TKOTZ, Viktoria. **Freqüência das Letras**. In: Freqüência da Ocorrência de Letras no Português. Brasil: Aldeia NumaBoa, 2004. Disponível em: <http://www.numaboa.com.br/criptologia/matematica/estatistica/freqPortBrasil.php>. Acesso em: 29 jun. 2008.

UNITED STATES OF AMERICA. ***Public Law 107–347***. 107th Congress. Dec. 17, 2002. *An Act To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes*. Title III—Information Security. Sec. 301. Information Security. Subchapter III—Information Security. § 3542. Definitions. Disponível em: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf>. Acesso em: 20 out. 2008.

VAN DOREN, Charles. ***A History of Knowledge –*** *Past, Present, and Future*. New York: Ballantine Books, 1991. 422 p.

WEBS DE PERSONAJES. Disponível em: <http://www.webs-de-personajes.com.ar/buscar.php?s=510&id_biograf=RGVtYXJhdG8=>. Acesso em 22 jun. 2008.

WIKIPÉDIA, a Enciclopédia Livre. Disponível em: <http://pt.wikipedia.org/wiki/P%C3%A1gina_principal>.

WIKIPEDIA, the Free Encyclopedia. Disponível em: <http://en.wikipedia.org/wiki/Main_Page>.

WRIXON, Fred B. ***Codes, Ciphers, Secrets and Cryptic Communication****: Making and Breaking Secret Messages from Hieroglyphs to the Internet*. New York: Black Dog & Leventhal Publishers, 2005. 704 p.