Algoritmo Criptográfico Brasileiro – Confidencialidade Nas Informações

Cap Av -Élvio Carlos Dutra e Silva Júnior
Mestre em Telecomunicações – *Technische Universität Darmstadt*
MBA em Gestão Estratégica de Negócios – Escola Superior de Propaganda e Marketing
Bacharel em Engenharia Eletrônica – Instituto Tecnológico de Aeronáutica

1 - Introdução

A humanidade vive hoje a era da informação e da comunicação. Esta fase advém do aumento do poder de proces-samento dos computadores e do crescimento das redes de comunicação em todo o mundo. As corporações possuem, atualmente, maior facilidade para armazenar e trocar informações de seu interesse. Esta vantagem gera uma desvantagem associada na medida que aumenta as atividades de espionagem eletrônica. As corporações civis e militares passam, portanto, a atentar cada vez mais para a necessidade de proteger suas comunicações e seus bancos de dados. Uma das ferramentas disponíveis para esta tarefa chama-se criptografia.

As organizações militares empregam, historicamente, a criptografia. A aplicação de técnicas modernas e criativas de criptografia surge, então, como uma evolução natural e

decorrente do grande volume de dados transmitidos nos modernos sistemas de comunicação militar (Sistema de Comunicações Aeronáuticas do DECEA; Sistema de Telemetria do VLS; SISCENDA; Sistema de Enlace de Dados do SIVAM, entre outros).

O SIVAM coleta e distribui informações de importância estratégica para o Brasil (localização de trafego aéreo hostil, ocorrência de crimes ecológicos, identificação de pistas clandestinas, localização de reservas minerais e outras). O Sistema de Enlaces de Dados do SIVAM, parte do Subsistema de Telecomunicações, transmite estas informações protegidas por um algoritmo criptográfico. Infelizmente, este algoritmo não pode ser considerado totalmente confiável, pois foi importado de uma empresa privada que possui conhecimento de seu funcionamento e suas vulnerabilidades.

Conseqüentemente, pela análise dos argumentos acima expostos, conclui-se que a proposta de nacionalizar o algoritmo criptográfico constitui uma importante solução para a manutenção da Soberania Nacional, pois assegura ao governo brasileiro o sigilo sobre informações de natureza estratégica para a proteção e o desenvolvimento sustentável da Amazônia Legal Brasileira – ALB.

Com o objetivo de justificar a proposta deste trabalho, foram mencionados vários detalhes do SIVAM: sua missão, os tipos de informações estratégicas processadas e o processo de proteção das mesmas. Assim, o primeiro passo para compreender nossa proposta é entender, historicamente, o nascimento do SIVAM.

2 - Histórico

2.1 - A Amazônia Antes do SIVAM

A Amazônia, antes do SIVAM, era dominada por um cenário onde as instituições públicas da região conviviam com grandes dificuldades de atuação. A infra-estrutura era incipiente, a captação de dados e a elaboração de conhecimentos confiáveis eram difíceis, havia explorações predatórias de recursos naturais e ocorriam inúmeras agressões ao ecossistema.

No final da década de 80, vários movimentos apresentavam a floresta amazônica como o pulmão do mundo, e os brasileiros eram vistos como os responsáveis por acabar com o oxigênio e a biodiversidade do planeta. Contestava-se, constantemente, a soberania do Brasil sobre esta região. Eis alguns exemplos: *"O Brasil precisa aceitar uma soberania relativa sobre a Amazônia",* dito por François Mitterrand, em 1989, então Presidente da França; *"A Amazônia é um patrimônio da humanidade. A posse desta imensa área pelos países mencionados – Brasil, Venezuela, Colômbia, Peru e Equador – é meramente circunstancial",* mencionado pelo Conselho Mundial de Igrejas Cristãs, em Genebra, 1992; *"Ao contrário do que os brasileiros pensam, a Amazônia não é deles, mas de todos nós",* proferido por Al Gore, 1989, então Vice-presidente dos Estados Unidos da América[1]. Impulsionado pelo clamor ambientalista da década de 90, cujo ápice ocorreu na Conferência Mundial para o Meio Ambiente - ECO 92, o Brasil era compelido a atuar efetivamente no controle da ALB, que despertava crescente cobiça internacional decorrente de seu grande potencial econômico e ecológico. O país precisava, urgentemente, pôr em prática um programa estruturado de governo que promovesse o desenvolvimento sustentável e o balanceamento das necessidades humanas e ambientais da ALB.

2.2 - Surgimento do SIVAM

Em 1990, a Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR), o então Ministério da Aeronáutica (MAER) e o Ministério da Justiça (MJ),

1- Brasil. CCSIVAM. *SIPAM – Sistema de Proteção da Amazônia. 2002. p. 19 e 20*

apresentaram ao governo a Exposição de Motivos 194. Ela relatava vários problemas presentes na ALB e propunha a criação de um sistema de monitoração e vigilância da região. Em 21 de setembro de 1990, ela foi aprovada e, por determinação da Presidência da Republica, foi criado o Sistema de Vigilância da Amazônia – SIVAM.

Coube à SAE/PR formular e implantar um Sistema Nacional de Coordenação, hoje conhecido por Sistema de Proteção da Amazônia (SIPAM), visando a atuação dos órgãos governa-mentais na repressão aos ilícitos ambientais da Amazônia. Devido à experiência obtida com a implantação de sistemas como o DACTA (sistema de Defesa Aérea e Controle de Tráfego Aéreo), coube ao MAER a implantação do SIVAM. O Ministério da Justiça foi encarregado de estruturar um conjunto de medidas, o chamado Pró-Amazônia, cuja respon-sabilidade era aprimorar a capacidade da Polícia Federal no desempenho de suas tarefas na região.

O Presidente da República, em 27 de maio de 1995, autorizou a assinatura do contrato comercial para fornecimento de bens e serviços pela empresa Raytheon, (vencedora do Processo de Licitação do SIVAM), que ofereceu uma proposta técnica superior, o menor preço e também garantiu o financiamento integral do projeto. Em 25 de julho de 1997, o contrato entrou efetivamente em vigor, sendo inaugurado pelo Presidente da República em 25 de Julho de 2002.

Durante os cinco anos de implantação do maior projeto ambiental do mundo, muitos esforços foram realizados de forma a se obter a estrutura organizacional e funcional que opera hoje no SIVAM. O entendimento da situação atual do projeto se torna, portanto, imperativo para a compreensão da solução proposta.

3 - Sistema Atual

3.1 - Estrutura do SIVAM

O SIVAM é uma grande rede de coleta e processamento de dados sobre a ALB. Ele é composto de uma variada gama de sensores (alguns deles instalados em aeronaves R99A e R99B), além de radares de vigilância aérea e de meteorologia, de plataformas de coletas de dados e de terminais de usuários. Estes dados são armazenados no Banco de Dados do SIVAM, atendendo diversas instituições de pesquisa.

Aeronaves de Vigilância	5
Aeronaves de Sensoriamento	3
Equipamentos de Rádio-determinação	300
Terminais de Usuários Remotos	703
Radares Fixos	19
Radares Transportáveis	6
Plataformas Fluviais de Coleta de Dados	200
Estações Meteorológicas de Superfície	53
Estações Meteorológicas de Altitude	13
Radares Meteorológicos	10
Detectores de Raios	11
Sensores de Monitoração de Comunicações	3
Estações de Satélites Meteorológicos	4

Fig. 3-1: Equipamentos e Sensores Empregados no Projeto SIVAM

O SIVAM é dividido funcionalmente em 3 subsistemas. O Subsistema de Aquisição de Dados é composto por sensores aéreos, terrestres e fluviais, com a função de obter, em tempo real, os dados brutos necessários à análise situacional da ALB. O Subsistema de Tratamento de Informações coleta os dados brutos e pré-processados enviados pelos sensores do Subsistema de Aquisição de Dados, originando a informação que resulta em produtos fornecidos aos OP. O Subsistema de Telecomunicações utiliza diversos canais e meios de comunicação com

a finalidade de promover a interconectividade do sistema, permitindo que o dado bruto, coletado no mais distante sensor, seja incorporado ao sistema.

Além da divisão funcional em três subsistemas, o SIVAM é, também, composto de três Centros Regionais de Vigilância (sediados em Manaus, Belém e Porto Velho) e de nove Centros Estaduais de Usuários localizados nas capitais da ALB. Estes órgãos são subordinados ao Centro de Coordenação Geral (CCG) em Brasília.

3.2 - Sistema de Enlace de Dados do SIVAM

A idealização do Sistema de Enlace de Dados do SIVAM concretizou um antigo anseio do COMAER. Em 1995, com a definição dos Requisitos Operacionais Preliminares da aeronave A-29, o Alto Comando da Aeronáutica foi sensível no que se refere a necessidade de integrar suas aeronaves de forma a compartilhar, com todos os envolvidos em uma operação, as informações coletadas por seus diversos sensores. Almejava-se dar à FAB uma vantagem competitiva, flexibilizando e acelerando o ciclo decisório dos diversos atuantes de um cenário operacional.

O Sistema de Enlace de Dados do SIVAM, parte do Subsistema de Telecomunicações, permite compartilhar tanto os dados brutos obtidos pelo Subsistema de Aquisição de Dados quanto as informações produzidas pelo Subsistema de Tratamento de Informações.

Trata-se de um sistema de comunicações digitais protegidas por criptografia e por salto de freqüências em V/UHF (padrão SECOS), utilizando rádios produzidos pela empresa alemã Rohde & Schwarz. O sistema SECOS é adotado também como padrão pelo SISCENDA, tendo sido realizado com sucesso, em 25 de agosto de 2004, um teste de interconexão entre os rádios de três aeronaves A-29 e uma aeronave R-99A.

3.3 - Algoritmo de Criptografia HCA-373

O padrão SECOS, na função de COMSEC, emprega o algoritmo HCA-373 de criptografia para a proteção das informações transmitidas pelo Sistema de Enlace de Dados do SIVAM. Este algoritmo trabalha com um esquema de chaves criptográficas, codificando a mensagem e impedindo a obtenção direta de seu conteúdo.

Infelizmente, por meio de técnicas de análise criptográfica, é possível quebrar o código e decifrar as mensagens mesmo sem possuir conhecimento prévio da chave criptográfica utilizada. A complexidade do algoritmo e o tamanho da chave aumentam a segurança do sistema e são responsáveis pelo aumento do esforço de processamento necessário para decifrar uma mensagem[2].

O algoritmo HCA-373 apresenta robustez e segurança, mas possui um ponto fraco. O esforço de quebra de um sistema criptográfico pode ser substancialmente redu-zido caso se saiba qual foi o algoritmo empregado. O ponto fraco reside, portanto, no fato de o algoritmo de criptografia HCA-373 ter sido desenvolvido por uma compa-nhia privada sub-contratada pela empresa alemã Rohde & Schwarz (R&S). Esta companhia, em um cenário de conflito bélico, no qual interesses de grandes blocos econômicos estejam envolvidos, não será capaz de suportar a pressão resultante dos interesses internacionais sobre a ALB.

O tema proposto neste artigo foi trocar o algoritmo de criptografia HCA-373 empregado no SIVAM por um algoritmo brasileiro – torna-se, assim, uma questão de Soberania Nacional. Estudar e propor alternativas criativas para o Algoritmo Criptográfico Brasileiro é, portanto, o primeiro passo a ser tomado.

2 MENEZES, Alfred et al. *Handbook of Applied Cryptography*. 2001. 816 p.

4 - Sistema Proposto

4.1 - Algoritmo Criptográfico Brasileiro

O sistema proposto nesta monografia visa a nacionalizar e substituir o algoritmo de criptografia HCA-373 embarcado nos equipamentos de Enlace de Dados do SIVAM. Com este intuito, o ACB deve se adequar a quatro princípios:

1. desempenhar as mesmas funções do algoritmo original;

2. não alterar os procedimentos operacionais e de manutenção dos rádios R&S;

3. não modificar o Layout dos equipamentos fornecidos; e

4. manter alto grau de semelhança de concepção com algoritmo HCA-373.

O ACB aqui proposto é fundamentado na Teoria do Caos. Esta teoria foi, primeiramente, apresentada pelo meteorologista Lorenz do Instituto de Tecnologia de Massachusetts. Baseado em seus estudos sobre previsão do tempo, em 1963, ele escreveu o artigo "Deterministic Non-Periodic Flows", primeiro trabalho a identificar e explicar a ocorrência de fenômenos caóticos na natureza.

$$\frac{dx}{dt} = 10(y - x)$$
$$\frac{dy}{dt} = 28x - y - xz$$
$$\frac{dz}{dt} = xy - \frac{8}{3}z$$

Fig. 4-2: Equações Caóticas Propostas por Lorenz

Em um sistema caótico, pequenas alterações em seu estado inicial provocam grandes alterações após certo tempo. Por exemplo, o tênue deslocamento de ar provocado pelo bater de asas de uma borboleta na floresta amazônica pode ser o responsável pela ocorrência de um ciclone na América do Norte num prazo de 11 meses. Caso esta borboleta não bata as suas asas, este ciclone pode não ocorrer ou acontecer em outro lugar.

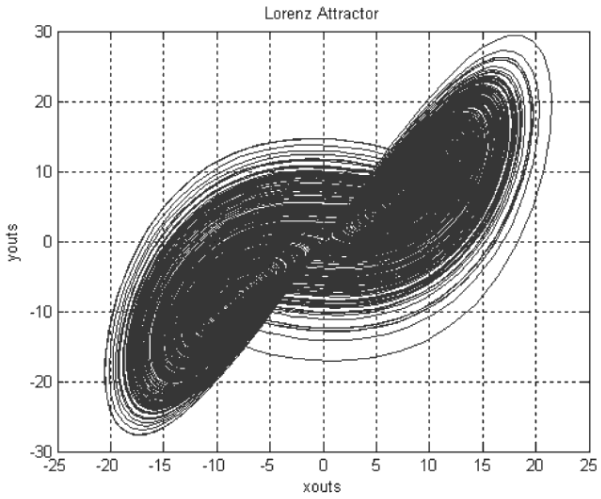

Fig. 4-3: Representação Gráfica das Equações de Lorenz[3].

A grande contribuição da Teoria do Caos é a sua capacidade de encontrar ordem e previsibilidade em fenômenos considerados totalmente caóticos e imprevisíveis. Esta característica é a pedra fundamental para a utilização desta teoria em criptografia.

Para entender isto, utilizar-se-á um exemplo didático que emprega o ruído determinístico produzido pelo circuito caótico desenvolvido na dissertação de mestrado *"Analysis, Design and FPGA-Implementation of Chaotic Systems as Alternative for Gaussian Noise Generation"* (Análise, Projeto e Implementação, usando circuitos integrados tipo FPGA, de sistemas caóticos como alternativa para a geração de ruído gaussiano), de mesma autoria do elaborador deste artigo. Ressalta-se que, nesta tese de dissertação, nenhum trabalho envolvendo criptografia foi desenvolvido, garantindo a originalidade deste trabalho monográfico.

É de senso comum que a recepção de uma comunicação (por rádio ou telefone, por exemplo) é bastante prejudicada na presença de ruído. Caso este ruído seja muito mais forte que o som transmitido, torna-se impossível entender o conteúdo transmitido.

Ao se adicionar a uma mensagem o ruído gerado pela implementação eletrônica das equações caóticas de Lorenz, pode-se impedir

3 - SILVA, Élvio Carlos Dutra Júnior. *Analysis, Design and FPGA-Implementation of Chaotic Systems as Alternative for Gaussian Noise Generation.* p. 34. 2004.

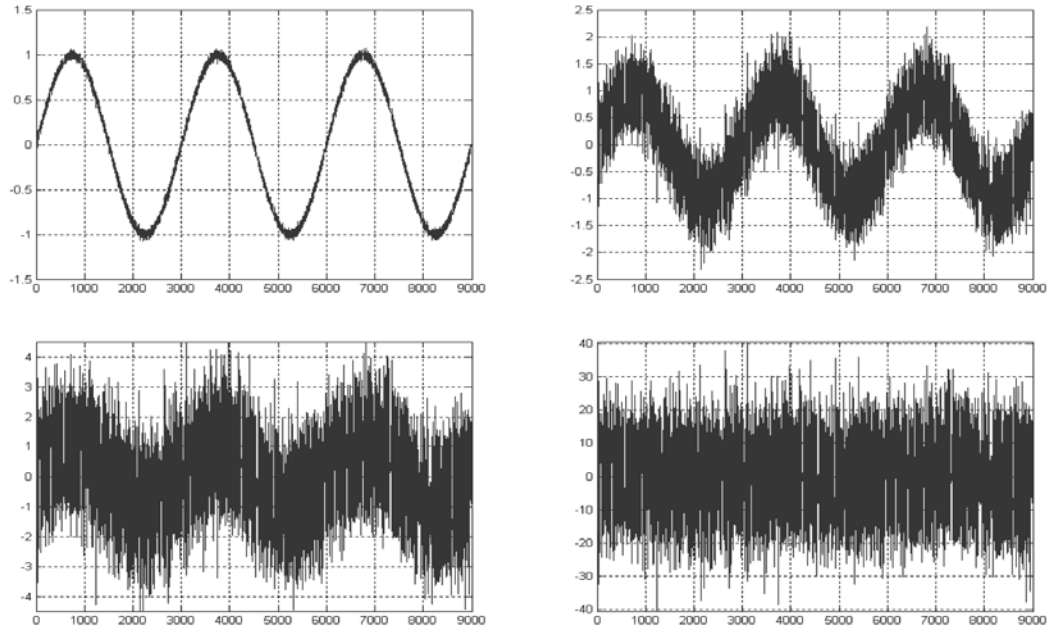

Fig. 4-4: Influência da Adição de Ruído Caótico a uma Mensagem

totalmente a compreensão da mensagem. A figura 4-4 mostra como a mensagem é danificada com a adição de ruído caótico de diferentes intensidades. Para se recuperar a informação, é necessário se ter conhecimento do circuito caótico que gerou o ruído, a respectiva chave criptográfica e realizar a operação contrária à utilizada inicialmente. Neste exemplo, como o ruído foi adicionado à mensagem, a operação contrária é uma subtração.

Este exemplo é didático e serve para visualizar como proteger uma mensagem por meio do emprego de circuitos caóticos. Logicamente, o ACB emprega uma operação muito mais complexa do que a simples adição utilizada neste exemplo (provendo a criatividade deste sistema criptográfico), e o sistema caótico utilizado deve ser mais complexo do que o apresentado na figura 4-2 a fim de aumentar o grau de dificuldade em se decifrar o código criptográfico.

4.2 - Análise da Proposta

Para analisar a proposta do ACB corretamente, far-se-á, a seguir, uma análise das vantagens e desvantagens proporcionadas pela adoção desta solução.

4.2.1 - Vantagens do ACB

A primeira vantagem do ACB é relativa a sua nacionalização, o que implica em dois fatores: total domínio da tecnologia empregada e independência de empresas estrangeiras. O primeiro fator torna o SIVAM capaz de substituir o algoritmo criptográfico sempre que necessário, capacitando-o para o emprego de Medidas de Proteção Eletrônica. O segundo fator garante a Soberania Nacional ao proteger informações estratégicas do SIVAM – principal finalidade a ser atendida por esta proposta.

Ao desenvolver o ACB em âmbito nacional, obtém-se uma vantagem adicional relativa ao controle das equipes de pesquisa, desenvolvimento e instalação. Como as equipes são brasileiras, pode-se escolher criteriosamente seus integrantes. Agrega-se, assim, maior confiabilidade quanto ao sigilo do projeto, garantindo-se, conseqüentemente, a confidencialidade nas informações transmitidas.

Os custos envolvidos no desenvolvimento do ACB são baixos, pois não haverá alterações físicas nos rádios R&S; far-se-á apenas a mudança do algoritmo HCA-373 embarcado. Os custos do projeto estarão relacionados, basicamente, à pesquisa e à logística de sua instalação em campo.

A utilização da Teoria do Caos gera seqüências determinísticas e não periódicas, apresentando melhores resultados do que a técnica de LFSR utilizada no HCA-373. Esta última gera seqüências periódicas, que podem ser previstas a partir da análise histórica dos dados. Criam-se, assim, mensagens criptográficas menos seguras. O emprego de circuitos caóticos em criptografia aumenta em diversas ordens de grandeza a segurança das comunicações, alcançando-se melhores valores de Relação Sinal-Caos.

4.2.2 - Desvantagens do ACB

A principal desvantagem na substituição do HCA-373 pelo ACB deve-se a necessidade de substituir o algoritmo em todos os elos do sistema para garantir que a comunicação não seja interrompida. Os esforços logísticos devem ser bem calculados a fim de minimizar o tempo de vulnerabilidade do sistema, pois, a partir do momento em que se começa a substituição, ocorre uma cisão no sistema, coexistindo duas partes que não trocam informações entre si: uma com o algoritmo HCA-373 e outra com o ACB. Este momento de fraqueza deve ser minimizado pela utilização de várias equipes trabalhando concomitantemente.

Outra desvantagem a ser observada se relaciona aos custos de conservação das equipes de pesquisa e de substituição. Objetiva-se, assim, manter uma estrutura científica e logística capaz de realizar constantemente mudanças por novas versões do ACB, garantindo a confidencialidade das informações nos casos em que se desconfiar do vazamento da chave ou do algoritmo criptográfico.

Vantagens	Desvantagens
Domínio da tecnologia empregada	Substituição em todo o sistema
Código criptográfico próprio	Vulnerabilidade momentânea
Controle da equipe de pesquisa	Estrutura logística de substituição
Baixo custo do projeto	-
Baixa relação sinal-caos	-

Fig. 4-5: Síntese da análise da proposta do ACB

As desvantagens da substituição do HCA-373 pelo ACB são relativas ao esforço necessário para a substituição propriamente dita. Os custos relativos à implantação justificam-se integralmente pelas vantagens proporcionadas pelo ACB, principalmente no tocante à manutenção da Soberania Nacional proporcionada pela proteção de informações estratégicas do SIVAM. Por meio da análise da solução aqui proposta, observa-se que as vantagens superam totalmente as desvantagens, tornando plenamente recomendável o desenvolvimento do ACB, cabendo neste momento, portanto, a realização de uma revisão dos principais tópicos aqui abordados por meio de uma resenha conclusiva que tem o intuito de fixar as principais idéias apresentadas.

Conclusão

A função do SIVAM é coletar e processar informações sobre a Região Amazônica, distribuindo-as aos seus OP.

Inicialmente, apresentou-se uma visão geral da situação da Região Amazônica antes do projeto SIVAM, expondo o crescente interesse internacional sobre a ALB. Mostrou-se, também, como foi apresentada e aceita a Exposição de Motivos 194.

A seguir, foi apresentada a situação atual do SIVAM. Foram identificados seus três subsistemas: Aquisição de Dados, Tratamento de Informações e Telecomunicações. Situou-se o Sistema de Enlace de Dados do SIVAM dentro do subsistema de Telecomunicações, e se explicou o funcionamento do padrão

SECOS. O algoritmo criptográfico HCA-373 foi, então, apresentado, citando sua limitação: falha intrínseca de segurança motivada por sua importação.

Fundamentado na Teoria do Caos, o ACB foi apresentado a seguir, demonstrando-se seu funcionamento por meio de um exemplo ilustrativo. Finalizou-se o capítulo com uma análise das vantagens e desvantagens da implementação do ACB no SIVAM.

Nosso objetivo é aumentar o nível de confidencialidade nas informações transmitidas pelo Sistema de Enlace de Dados do SIVAM. A proposta aqui apresentada contempla inteiramente este objetivo devido a duas razões principais. Primeiramente, ao nacionalizar o algoritmo criptográfico do SIVAM, impede-se que outras nações ou instituições tenham conhecimento do algoritmo utilizado e possam decifrar as mensagens. A segunda razão se deve a melhoria proporcionada pelo ACB, pois ele permite obter menores valores na relação sinal-caos.

O Comando da Aeronáutica recebeu a incumbência de implantar o SIVAM diretamente da Presidência da República. Cumprindo esta atribuição, o COMAER viu a necessidade de proteger a transmissão das informações do SIVAM usando técnicas de criptografia. O ACB surge, portanto, como uma importante solução ao oferecer a possibilidade de desenvolver e manter nosso próprio algoritmo criptográfico, tornando o SIVAM mais protegido contra a espionagem de suas transmissões.

Para finalizar este trabalho, transcreve-se abaixo as palavras de Thomas Lovejoy:

"O maior desafio imposto pela natureza aos brasileiros é explorar a Amazônia com inteligência e perícia. O desafio torna-se maior ainda se houver falhas, pois nesse caso não haverá uma segunda chance"[4].

Referências

BRASIL. Centro de Comunicação Social da Aeronáutica. Notícias: Esquadrão Guardião faz teste de conexão entre rádios de aeronaves. 30 Ago. 2004. Disponível em <http://www.fab.mil.br/Publicacao/Imprensa/Noticias/3008_06.htm>. 15 Mar. 2005.

BRASIL. Comando Geral do Ar. Centro de Guerra Eletrônica. Introdução a Criptografia. Brasília. 1998. 47 p.

BRASIL. Comando Geral do Ar. SISCENDA – A Melhor Maneira de Não Conseguir se Comunicar. Spectrum. Número 07. Ago. 2003. 7 p.

LORENZ, N. Edward. *Deterministic non-periodic flows*. *Journal of Atmospheric Science*, Vol. 20, Nº. 02. 1963.

MENEZES, Alfred et al. *Handbook of Applied Cryptography*. 5ª Edição. [S. l.: s. ed.] 2001. 816 p.

OLIVEIRA, Dailson M. SIPAM–SIVAM, Olhos da Amazônia. *Airpower Journal*. 2º Trimestre 1995. Edição Brasileira. 10 p.

SILVA, Élvio Carlos Dutra Júnior. *Analysis, Design and FPGA-Implementation of Chaotic Systems as Alternative for Gaussian Noise Generation*. Darmstadt, Alemanha, 2004. 140 p.

(Footnotes)

[1] Brasil. CCSIVAM.
SIPAM – Sistema de Proteção da Amazônia.
2002. p. 19 e 20

[2] MENEZES, Alfred et al.
Handbook of Applied Cryptography
2001. 816 p.

[3] SILVA, Élvio Carlos Dutra Júnior.
Analysis, Design and FPGA-Implementation of Chaotic Systems as Alternative for Gaussian Noise Generation.
p. 34.
2004.

[4] OLIVEIRA, Dailson M.
SIPAM –SIVAM, Olhos da Amazônia
. Airpower Journal. 1995.

4 - OLIVEIRA, Dailson M. *SIPAM–SIVAM, Olhos da Amazônia*. Airpower Journal. 1995