Anais XIV Simpósio Brasileiro de Sensoriamento Remoto, Natal, Brasil, 25-30 abril 2009, INPE, p. 1617-1624.

Localizador GPS com criptografia de dados

André Barros Cardoso da Silva[1]
Wilton Ney do Amaral Pereira[1]
Wilson Yamaguti[2]

[1]Universidade de Taubaté - UNITAU
Rua Daniel Danelli - s/n - 12060-440 - Taubaté - SP, Brasil
andrebcs@hotmail.com
wilton.pereira@uol.com.br

[2] Instituto Nacional de Pesquisas Espaciais - INPE
Av. dos Astronautas – 1758 – 12227-010 - São José dos Campos - SP, Brasil
yamaguti@dss.inpe.br

Abstract. The Brazilian Environmental Data Collection System (SBCDA) actually has over 700 data collecting platforms which attend around 100 organization users, mainly hydrological and meteorological applications. The system uses Brazilian satellites developed and managed by the National Institute for Space Research (INPE). However, new data collection applications, such as vessel monitoring, need to transmit geographic positions applying a cipher algorithm over the data. A further point to consider is that these kinds of locators are available mainly in foreign systems. Thus, according to those needs, a locator was developed to be used on single data collecting platforms. First of all the locator has a GPS receiver that will collect the geographic position data. A microcontroller will apply over them a cipher algorithm, providing a reliable and safe communication. After encryption, the data will be transmitted through an UHF transmitter to the SBCDA satellites. Studies about different cipher algorithms focusing their feasibility, efficiency, and easiness implementation pointed to the Advanced Encryption Standard (AES) as the best option to be adopted. The AES was announced by the National Institute of Standards and Technology (NIST) as a standard cipher algorithm, in 2001. It is based on full byte permutations considering the flexibility to choose the input data and cipher key blocks length: 128, 192, 256 bits. Ciphering tests were realized according to existing references in order to validate the algorithm implementation into microcontroller. Future improvements such as ciphering on smaller data block lengths and coding / decoding algorithms are foreseen.

Palavras-chave: satellite, cryptography, Rijndael, GPS, criptografia, AES, PIC, satélite.

1. Introdução

Segundo Sklar (2001), os sistemas de telecomunicações vêm sofrendo profundas alterações com o advento da comunicação digital e de outras tecnologias, como comunicações via satélite, localização GPS, entre outras.

O Instituto Nacional de Pesquisas Espaciais (INPE), através do Sistema Brasileiro de Coleta de Dados Ambientais (SBCDA), oferece a oportunidade de realizar experimentos de comunicação envolvendo diversas tecnologias de comunicação digital com ênfase em aplicações de coleta de dados ambientais. Este sistema utiliza em seu segmento espacial um conjunto de satélites desenvolvidos e operados pelo INPE. Os serviços prestados por este sistema são relacionados à coleta de dados ambientais adquiridas pelas Plataformas de Coleta de Dados (PCD), que utilizam os satélites como meio de comunicação para transmissão dos dados até as estações de recepção. Os dados recebidos são posteriormente enviados ao Centro de Missão Coleta de Dados que faz o processamento, o armazenamento e a difusão desses dados aos seus usuários. Segundo Yamaguti et al. (2006), atualmente mais de setecentas plataformas foram instaladas no sistema atendendo a cerca de cem organizações usuárias, como a Agência Nacional de Águas, SIVAM, e diversos núcleos estaduais de meteorologia. Porém, novas demandas de coleta de dados necessitam adquirir as posições geográficas de uma dada plataforma e ao mesmo tempo garantir a proteção dos dados contra acesso não permitido.

Com ênfase nestas necessidades foi desenvolvido um sistema de localização acoplado a uma PCD já existente, onde um localizador oferece o serviço de localização geográfica através de um receptor do Sistema de Posicionamento Global (GPS), aplicando sobre os dados de posição um algoritmo de criptografia. Recursos similares de localização e segurança de acesso são disponíveis em sistemas estrangeiros, contudo em termos nacionais, o uso de criptografia nos dados transmitidos por uma plataforma tem característica inovadora. O método criptográfico adotado para esta aplicação foi o *Advanced Encryption Standard* (AES), criado por Vincent Rijmen e Joan Daemen. Sucessor do método DES (*Data Encryption Standard*), o AES (Rijndael) é um algoritmo baseado em permutações de bytes completos, permitindo flexibilidade ao usuário na escolha dos tamanhos da chave simétrica e dos blocos de mensagem: 128, 192, 256 bits.

Os resultados obtidos neste trabalho possuem elevado potencial de uso face às demandas existentes no mercado nacional, como: embarcações de pesca, bóias oceânicas, entre outros.

2. Metodologia de Trabalho

Por se tratar de um trabalho essencialmente de pesquisa tecnológica, a metodologia utilizada visa atender necessidades reais que nortearam a definição de objetivos e o estabelecimento de um conjunto de fases de desenvolvimento e testes. A infra-estrutura necessária para o desenvolvimento do protótipo, como: ferramentas de desenvolvimento, módulos receptores GPS e transmissores em UHF, foi disponibilizada pelo INPE. Assim como os testes realizados em campo, em condições reais, com o auxílio do SBCDA.

2.1 Primeira etapa: estudos preliminares:

Esta etapa visou obter conhecimento preliminar das possíveis ferramentas utilizadas na concepção do projeto: receptores GPS, microcontroladores, transmissores UHF, entre outros, de modo a poder estabelecer os primeiros arranjos práticos do sistema. Abrange também estudos sobre o SBCDA e o sistema de navegação GPS.

2.2 Segunda etapa: métodos de criptografia:

Esta etapa abrange os estudos realizados sobre algoritmos de criptografia a serem aplicados às mensagens do receptor GPS. Foram primeiramente abordados conceitos básicos sobre comunicação digital, codificação de fonte, e criptografia, visando compreender a importância da segurança dos dados em uma comunicação digital. Por fim, foram estabelecidas comparações a fim de se determinar o algoritmo mais conveniente a ser implementado na prática, via *software*.

2.3 Terceira etapa: elaboração do mapa de projeto:

Esta etapa reúne os primeiros planos práticos do projeto, onde foi estabelecido o diagrama em blocos de um primeiro protótipo junto às ferramentas escolhidas para integrar o projeto. Todos os conceitos teóricos adquiridos nas etapas anteriores foram utilizados nesta etapa.

2.4 Quarta etapa: desenvolvimento de *software* e *hardware* do projeto:

Todas as técnicas de *software* e os conhecimentos obtidos nas etapas anteriores foram utilizados para a programação do microcontrolador. Paralelamente ao desenvolvimento do *software*, foram adotados modelos que definiram o *hardware* do sistema, de modo a evitar desconformidades entre *software* e *hardware* ao longo do projeto.

2.5 Quinta etapa: integração e testes:

Esta etapa compreende a montagem do protótipo final, integrando as partes do projeto. Foram realizados também os últimos testes dos módulos do sistema, que determinaram a

aptidão do mesmo à realização dos testes em campo aberto. Assim, as mensagens recebidas passaram por um processo de decriptografia, permitindo então avaliar a eficiência do sistema.

3. Resultados e Discussão

3.1 Descrição da plataforma de coleta de dados

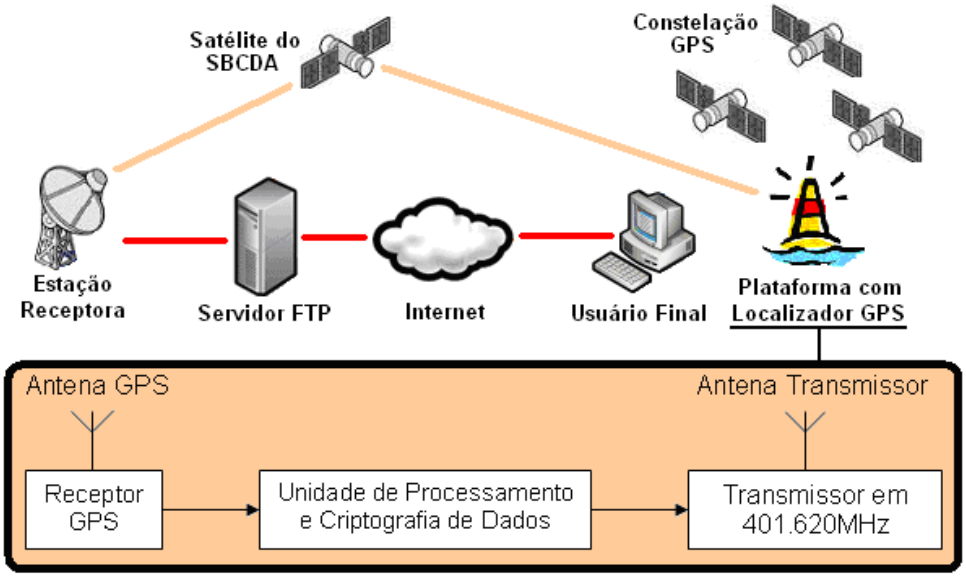

Figura 1. Sistema de rastreamento com a plataforma de coleta de dados.

A descrição completa da PCD é mostrada na Figura 1, e pode ser dividida em três segmentos: recepção, processamento e transmissão. O primeiro é responsável pela aquisição dos dados de posição geográfica provenientes da constelação GPS (*Global Positioning System*). Para a aquisição dos dados de posição geográfica, o receptor GPS Lassen iQ dispõe de uma antena ativa com um amplificador de sinal interno. Os dados recebidos por este receptor são enviados a uma unidade de processamento e criptografia de dados, onde são processados por um microcontrolador. O receptor GPS disponibiliza diferentes protocolos para envio dos dados de posição geográfica, entre os quais foi escolhido o NMEA-0183 devido à sua larga utilização em vários segmentos, como: comunicações industriais, equipamentos de navegação náutica, entre outros.

O microcontrolador PIC18F4550 realiza o processamento e criptografia dos dados de posição geográfica, programado em linguagem "C". Este microcontrolador recebe a mensagem completa (estabelecida pelo protocolo NMEA-0183) armazenando somente os dados imprescindíveis para a criação do campo final da mensagem "*header 0*". Assim, sobre este campo é aplicado o algoritmo de criptografia AES (Rijndael), proporcionando elevada segurança sobre os dados para então serem transmitidos aos satélites do SBCDA.

Esta transmissão é feita através do transmissor ELTA HAL-2 (*High Accuracy Locator 2*), cuja escolha deve-se a completa possibilidade de programação de seus parâmetros de transmissão, tais como: *ID*, freqüência, potência, tamanho do campo de mensagem, etc.

3.1.1 O formato do campo de mensagem "*header 0*"

Cada mensagem transmitida é estruturada de acordo com um formato padrão para transmissão de dados de localização. No caso particular deste projeto fez-se o uso do formato "*header 0*", utilizado em aplicações cuja precisão da posição geográfica é da ordem de 0.001°. Este formato provê a cada pacote uma posição absoluta e três posições relativas, estabelecendo um campo final de 160 bits. A posição absoluta de cada mensagem refere-se à

posição "mais atual", ou seja, a última posição na qual foi realizada a aquisição de dados pelo receptor GPS. As posições relativas são juntamente transmitidas com a absoluta com o intuito de oferecer um "histórico" da posição ao usuário, posto que nem sempre os satélites do SBCDA serão visíveis pela PCD, podendo ocasionar períodos sem recepção de dados. Deste modo, as posições relativas devem sempre ser referidas a posição absoluta, contendo somente a variação entre as coordenadas latitude e longitude (deltas), e o tempo de atraso entre cada transmissão (*delays*).

O formato do campo final da mensagem é mostrado abaixo, através das Tabelas 1 e 2:

Tabela 1. Primeira posição fixa (absoluta).

Header	CRC	Longitude	Latitude	Horas	Minutos	Período
4 bits	8 bits	19 bits	18 bits	5 bits	6 bits	4 bits

Tabela 2. Segunda, terceira e quarta posições fixas (relativas).

Δ Longitude	Δ Latitude	Delay	Time index
13 bits	13 bits	4 bits	2 bits

As convenções a seguir foram adotadas para este projeto:

- Longitude absoluta: 0 (0°) a 360000 (360°);
- Latitude absoluta: 0 (90°S) a 180000 (90°N);
- Horas e minutos: 0 a 23 horas / 0 a 59 minutos;
- Longitude e latitude relativas: Variação de 0 (-4°) a 8000 (+4°);
- *Delay*: 0 a 15 minutos;
- *Time index*: Adota-se como "00" (binário), indicando que o tempo real da aquisição é o contido na mensagem.

O campo "*Header*" identifica o formato da mensagem. Para este caso deve ser igual à zero (formato "*header 0"*).

O campo de "CRC" (*Cyclic Redundancy Check*) é calculado para cada mensagem transmitida de acordo com o polinômio "X^7+X+1". É utilizado como um mecanismo de verificação de erros na mensagem recebida.

O campo "Período" (aquisição de posição geográfica) é um parâmetro configurável pelo usuário. Cada período estabelecido corresponde a conteúdo diferente no campo "Período" da mensagem, conforme demonstrado na Tabela 3:

Tabela 3. Códigos dos períodos de aquisição das mensagens.

Código do Campo "Período"	Período de Aquisição das Mensagens
0000	20 minutos
1001	30 minutos
1010	45 minutos
0011	1 hora
1100	2 horas
0101	3 horas
0110	4 horas
1111	1 minuto (demonstração)

3.2 O método criptográfico AES (Rijndael)

Segundo Katzan Jr. (1977), o termo criptografia (do grego *kryptós*: "escondido/oculto"; e *gráphein*: "escrever") pode ser entendido como o estudo das técnicas e princípios pelos quais uma informação pode ser transformada da sua forma original para outra ilegível, ou aparentemente sem valor. Na prática, é um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática.

Para se iniciar um processo de criptografia, primeiramente deve-se escolher uma chave "forte" para o sistema. Segundo Balparda Carvalho (2001), entende-se como "chave forte" uma chave que é de difícil dedução. Tanto a chave quanto os blocos de mensagem podem assumir três tamanhos: 16 bytes, 24 bytes e 32 bytes. O número de iterações de transformação da mensagem é variável em função dos tamanhos da chave e mensagem, de acordo com a Tabela 4:

Tabela 4. Número de iterações do AES (Rijndael).

Chave	Mensagem		
	16 bytes	24 bytes	32 bytes
16 bytes	10*	12	14
24 bytes	12	12	14
32 bytes	14	14	14

Particularmente no projeto foi utilizada uma chave de 16 bytes junta a blocos de mensagens também de 16 bytes. Logo, serão necessárias 10 iterações de transformação da mensagem*. A chave e cada bloco da mensagem devem ser constituídos matricialmente, como mostra a Figura 2:

Bloco [0]	Bloco [4]	Bloco [8]	Bloco [12]
Bloco [1]	Bloco [5]	Bloco [9]	Bloco [13]
Bloco [2]	Bloco [6]	Bloco [10]	Bloco [14]
Bloco [3]	Bloco [7]	Bloco [11]	Bloco [15]

Chave [0]	Chave [4]	Chave [8]	Chave [12]
Chave [1]	Chave [5]	Chave [9]	Chave [13]
Chave [2]	Chave [6]	Chave [10]	Chave [14]
Chave [3]	Chave [7]	Chave [11]	Chave [15]

Figura 2. Matrizes dos blocos da mensagem (esq.) e chave secreta (dir.).

Cada campo "bloco[n]" representa um byte da mensagem a ser criptografada, e cada campo "chave[n]" representa um byte da chave secreta de criptografia. Com a chave devidamente escolhida, dá-se início ao processo de criptografia.

Os diagramas em blocos de todo o processo criptográfico são mostrados na Figura 3. Descrições mais aprofundadas podem ser encontradas nas referências bibliográficas utilizadas.

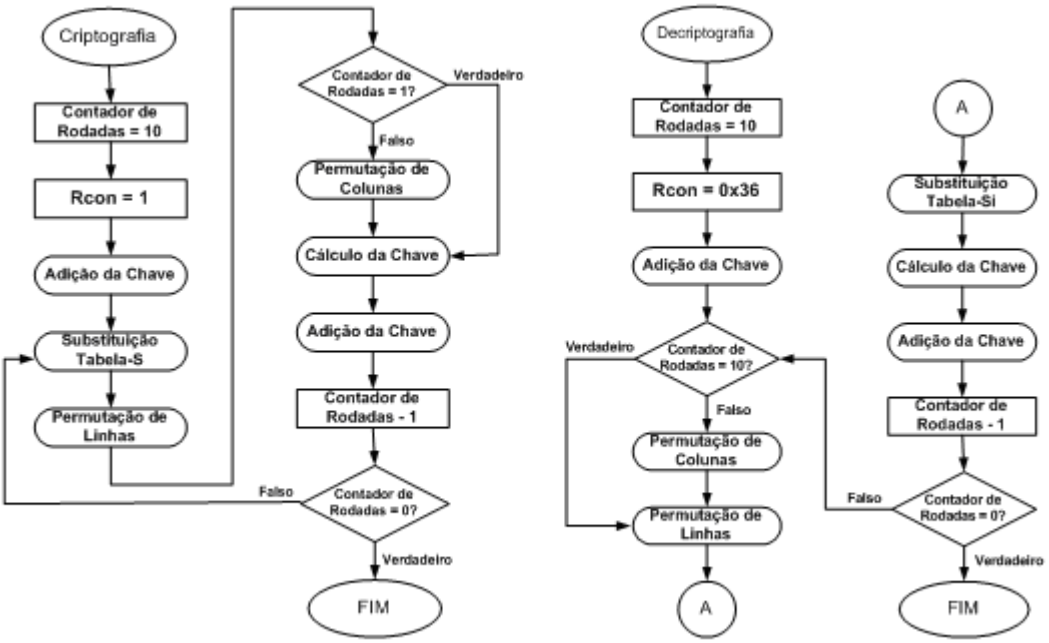

Figura 3. Diagramas em blocos dos processos de cifragem (esq.) e decifragem (dir.).

3.3 Validação do algoritmo AES (Rijndael)

Os valores matriciais contidos nos testes a seguir foram retirados do próprio *software*, e confrontados com duas fontes confiáveis:

- FIPS (*Federal Information Processing Standards*) PUB 197 – "*Announcing the Advanced Encryption Standard* (AES)". Arquivo público nº197 de aprovação do AES pela FIPS, em Novembro/2001, anunciando o método de Rijndael como padrão de segurança computacional.
- *Rijndael Simulator*: simulador virtual do método de criptografia AES (Rijndael). Exibe o processo completo de cifragem para uma mensagem (texto puro) e chave previamente estabelecidas.

A mensagem e a chave de criptografia foram baseadas no "Apêndice B" da primeira fonte, citada acima. Através deste documento, onde são demonstradas as dez iterações necessárias para a cifragem de um texto puro, foi possível validar o desenvolvimento completo do algoritmo.

Seguem a mensagem e a chave secreta utilizadas na validação do algoritmo:

- Texto Puro: 0x3243F6A8885A308D313198A2E0370734h (128 bits).
- Chave Secreta: 0x2B7E151628AED2A6ABF7158809CF4F3Ch (128 bits).

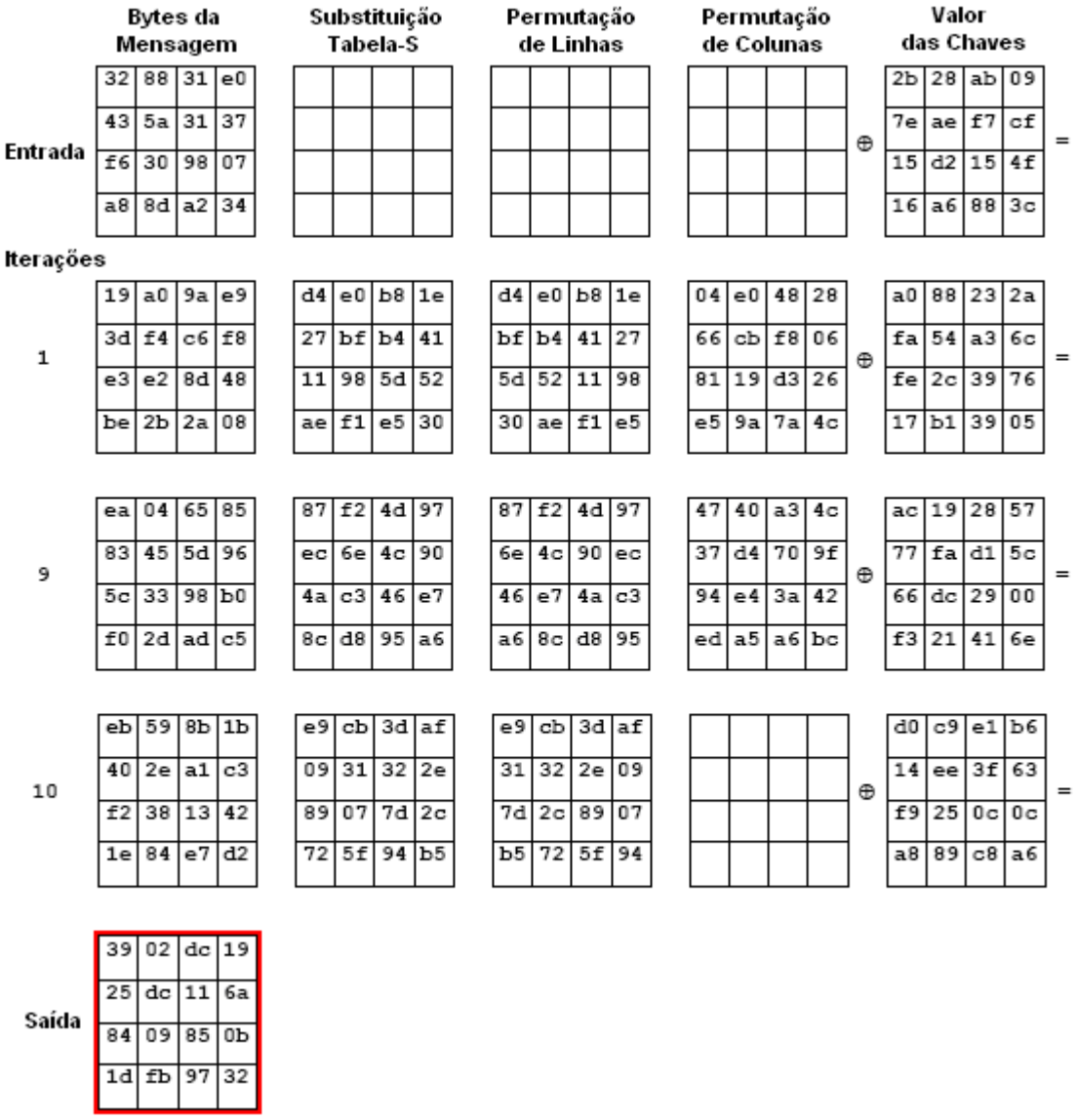

Figura 4. Matrizes com os dados do teste de cifragem.

Segundo Flowers (2005), o método criptográfico AES (Rijndael) calcula a cada iteração uma nova chave, que será utilizada na iteração seguinte. Cada uma das dez iterações utiliza uma chave diferente, cujo cálculo é baseado na chave anterior. Na última iteração não é executada a rotina "Permutação de Colunas", também verificada no diagrama em blocos previamente mostrado. A matriz de saída já contém a mensagem criptografada: "3925841D02DC09FBDC118597196A0B32h" (128 bits).

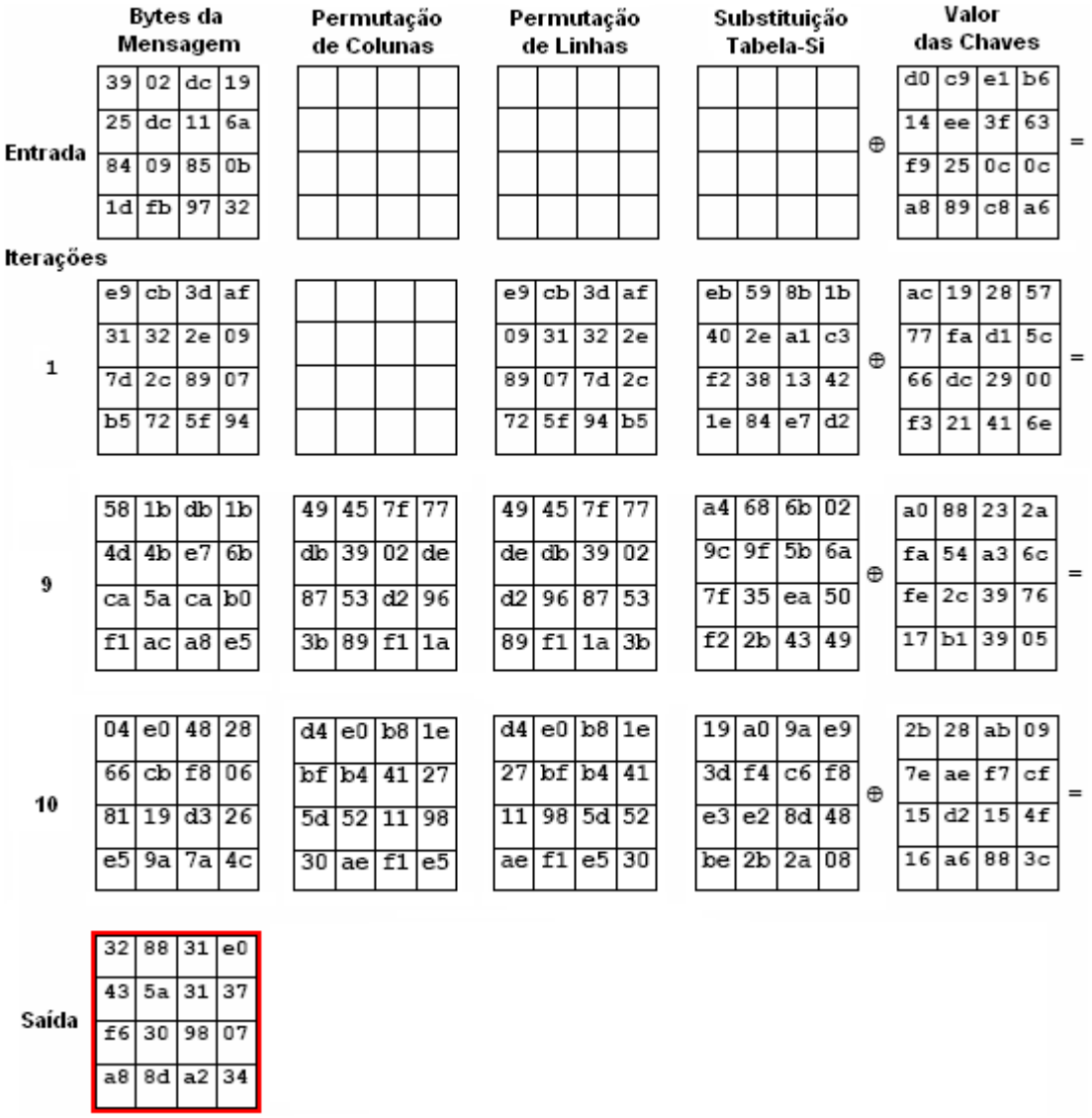

Figura 5. Matrizes com os dados do teste de decifragem.

No processo de decifragem do algoritmo AES (Rijndael) a chave inicial é a última chave calculada no processo de cifragem. Assim, nota-se na última iteração a recuperação do texto puro, e da chave propriamente dita. A rotina "Permutação de Colunas" não é executada na primeira iteração do processo de decifragem, também verificada no diagrama em blocos previamente mostrado. A matriz de saída contém então a mensagem em sua forma original, recuperando o texto puro: "3925841D02DC09FBDC118597196A0B32h" (128 bits).

3.4 Montagem do protótipo

A Figura 4 mostra a interconexão entre as ferramentas utilizadas no projeto. À esquerda é mostrada a bancada de testes do protótipo. Com o sucesso dos testes realizados em laboratório, foi desenvolvida a placa de circuito impresso (PCI) do protótipo (à direita).

Figura 6. Bancada de testes em laboratório (esq.) e PCI do protótipo (dir.).

4. Conclusões

Os estudos realizados e os conceitos adquiridos face às dificuldades encontradas em cada etapa deste projeto contribuíram primeiramente para a ampliação do conhecimento na área de Sistemas de Telecomunicações, em especial a comunicação digital, satélites e sistema GPS. O conhecimento teórico destas ferramentas pôde ser verificado na prática por meio das comunicações realizadas com os satélites do SBCDA.

Excluso o enfoque matemático, o domínio praticável de um método de criptografia é de grande valia, pois possibilita futuramente o desenvolvimento de novas aplicações no segmento de transmissão segura de dados, oferecendo confiança e integridade às mensagens transmitidas. A validação do algoritmo criptográfico AES (Rijndael) implementado no microcontrolador pôde ser realizada através de duas fontes confiáveis, sendo a primeira o próprio artigo de publicação do AES (Rijndael), e a segunda um simulador virtual do mesmo.

Com o apoio do INPE, a recuperação dos dados de posição geográfica foi realizada através das estações terrenas de Cuiabá (MT) e Alcântara (MA), e o processamento dos mesmos foi realizado pelo Centro de Missão de Coleta de Dados, em Cachoeira Paulista (SP). Uma vez processados, os dados são disponibilizados na Internet por meio de um servidor FTP, onde o algoritmo de decriptografia retorna cada mensagem a sua forma original.

No futuro deseja-se realizar novos estudos criptográficos a fim de possibilitar a criptografia em blocos menores de mensagem, e, subsequentemente submetê-los a um algoritmo de codificação / decodificação, visando corrigir erros na recepção dos dados.

Agradecimentos

À Universidade de Taubaté pela oportunidade oferecida através do Programa de Iniciação Científica (PIC/UNITAU). Ao Instituto Nacional de Pesquisas Espaciais (INPE) por toda a infra-estrutura disponibilizada para o desenvolvimento e testes do projeto. Aos orientadores Wilton Ney do Amaral Pereira (UNITAU) e Wilson Yamaguti (INPE) por todo o suporte oferecido ao longo de cada etapa do projeto.

Referências Bibliográficas

SKLAR, Bernard. **Digital Communications: Fundamentals and Applications**. 2. ed. New Jersey: Prentice Hall PTR, 2001. 1078p.

KATZAN JR, Harry. **The Standard Data Encryption Algorithm**. 1. ed. New York: PBI, 1977. 134p.

CARVALHO, D. B. **Segurança de Dados com Criptografia: Métodos e Algoritmos**. 2. ed. Rio de Janeiro: Book Express, 2001. 215p.

PERMADI, Edi. Cryptography Made Easy. Rijndael Simulator. Disponível em: <http://jsnerd.googlepages.com/index01a.htm> Acesso em: 5 maio 2008.

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197,1., 2001. **Announcing the Advanced Encryption Standard (AES)**... NIST, 2001. 52 p.

FLOWERS, David. **Data Encryption Routines for the PIC18**. Disponível em: <http://ww1.microchip.com/downloads/en/AppNotes/00953a.pdf>. Application Note 953: 14 Jan, 2005.

YAMAGUTI, W.et al. **O Sistema Brasileiro de Coleta de Dados Ambientais: Estado Atual, Demandas e Estudos de Propostas de Continuidade da Missão de Coleta de Dados.** INPE, 2006. (SCD-ETD-002).