FACULDADE DE ENGENHARIA
MESTRADO EM ENGENHARIA ELÉTRICA
PROCESSAMENTO DE SINAIS E ENGENHARIA BIOMÉDICA

CARLOS HENRIQUE DA COSTA CANO

# TÉCNICA DE CRIPTOGRAFIA COM DADOS GEODÉSICOS

Porto Alegre
Fevereiro de 2008

**CARLOS HENRIQUE DA COSTA CANO**

# TÉCNICA DE CRIPTOGRAFIA COM DADOS GEODÉSICOS

Dissertação apresentada para obtenção do grau de Mestre, pelo Programa de Pós-Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientador: Prof. Dr. Rubem Dutra Ribeiro Fagundes

**Porto Alegre**

**Fevereiro de 2008**

# Agradecimentos

Ao Orientador Professor Dr. Rubem Dutra Ribeiro Fagundes pela oportunidade de ser seu orientando durante o mestrado e principalmente por sua motivação, dedicação e disponibilidade que possibilitaram a realização deste trabalho.

Ao corpo de professores do Mestrado da Engenharia Elétrica da PUCRS ao qual me deram ferramentas e conhecimentos para o desenvolvimento deste trabalho.

Aos meus colegas Luís Vitório Cargnini e Diogo Scolari por suas sugestões dadas ao aprimoramento deste trabalho.

Aos funcionários do programa de Pós-Graduação da Faculdade de Engenharia Elétrica, em especial para as colegas Inelve Colognese e Maria Helena Maciel de Almeida pela paciência e dedicação.

A minha família e a minha namorada que compreenderam minha ausência e minha dedicação a este trabalho.

A todos meus colegas de trabalho e de aula que direta ou indiretamente me ajudaram a desenvolver este trabalho.

**Resumo**

O objetivo principal desta dissertação é mostrar a criação e a implementação de uma solução composta por componentes de navegação e posicionamento atuando em conjunto com módulos de criptografia e softwares adicionais.

Esta extensão será através da utilização do sistema Global Positioning System (GPS), que é um sistema desenvolvido inicialmente para uso militar ao qual prove informações cartográficas fundamentais como: coordenadas geográficas, velocidade, altura, hora.

Foram estudados algorítimos de criptografia simétricos e assimétricos e além disso foi realizada uma descrição detalhada do sistema GPS que fundamentou o presente trabalho. Neste trabalho foi escolhido o padrão AES, ao qual é de domínio público, sem royalties e foi escolhido num processo publico e rigoroso pelo NIST como padrão para criptografia.

Para validação do presente trabalho utilizou-se um equipamento real de GPS, com o qual foram realizados testes de campo. Nestes testes foi determinada a precisão efetiva destes equipamentos bem como a validação da proposta em funcionamento de campo.

Os resultados obtidos demonstraram que a técnica de utilização de coordenadas geodésicas globais de GPS bem como as coordenadas cartográficas comuns são eficientes no processo de criptografia proposto. Criando desta forma um novo modelo de criptografia.

Deste modo, este trabalho apresenta como grande inovação a possibilidade de estabelecer uma nova forma de criptografia. E ao mesmo tempo simples, dado que utiliza o sistema GPS já popularizado e no entanto extremamente eficiente pois a mensagem somente é acessível quando o destinatário estiver em um determinado local cujo conhecimento pode ser usualmente restrito. Sendo assim, a partir deste trabalho, abre-se uma nova forma de realizar a codificação de mensagens de cunho sigiloso, com um ampla gama de novas possibilidades.

**Palavras Chave**: Criptografia, GPS, Geodésico, Coordenadas, Segurança, Tecnologia, Comunicação, Privacidade, Mobilidade

**Abstract**

The main objective on this thesis is to show the creation and implementation of a solution composed by navigational, positional components acting together with cryptography modules and software.

This implementation will use the Global Positioning System (GPS), that in its beginning was used mainly for military objectives, this system provide geographic, cartographic and geodesic information as: latitude, longitude, velocity, time and height.

Some encryption algorithms mode as asymmetric and symmetric were studied, also the GPS system and its variables to better describe this work. In this proposal was used the AES (Rijndael) encryption for its security and desempenho certified by the NIST department.

To validate this work a GPS receiver was used to make field tests to check the precision and accuracy of the receiver and this proposal.

The obtained results show that this proposal that uses geodesic coordinates and cryptography and cartography coordinates too are efficient in this cryptographic system proposed. As in this proposal the data transmitted has more security because they only can be decoded in the right coordinates or geodesic variables, that the transmitter set up.

Overall this work creates a new way to encrypt and send information, that is simple, effective and can use the GPS system or another, and several kind of cryptographic systems. Indeed the message only can be decoded in the right coordinates or geodesic variables. This open a new way to communicate with new products and solutions. Creating by this new possibilities for business, security and society.
**Keywords**: Cryptography, GPS, Geodesical, Coordinates, Security, Technology, Communication, Privacy, Mobility

# Conteúdo

# Lista de Tabelas

# Lista de Figuras

# Acrônimos

AES Advanced Encription Standard

API Application programming interface

AS Anti-Spoofing

DES Data Encryption Standard

DVD digital versatile disc

ECC Elliptic Curve Cryptography

GF Galois Field

GHZ Giga Hertz

GPS Global Positioning System

HTML HyperText Markup Language

IBGE Instituto Brasileiro de Geografia e Estatística

ND Não Disponível

NIST National Institute of Standards and Technology

NMEA National Marine Electronics Association

PKI Public Key Infrastructure

PPS Precise Positioning Service

RAM Random Access Memory

SPS Standard Positioning System

SSL Secure Sockets Layer

# 1 Introdução

A sociedade humana tem demonstrado nos últimos tempos uma crescente aceleração e avanços nos seus mais diversos campos de ciência. Desde o advento da eletricidade, do telégrafo e dos computadores. Não se passou mais de um século para isso. O progresso se apresenta de forma cada vez mais rápida e complexa em conseqüência destes avanços.

Das necessidades militares para cálculos de artilharia e de outras formas de simulação, os computadores progrediram enormemente, novas necessidades e usos foram criados numa escalada cada vez maior e complexa.

Dentro destes avanços, o campo de comunicação foi um dos que avançaram exponencialmente. Do telégrafo até o telefone e as posteriores formas digitais foi um passo. Os custos desta comunicação e os equipamentos utilizados , são cada vez são mais baixos, onde antes se precisava de uma sala cheia de operadores e telefonistas, hoje faz-se com um equipamento portátil.

Com os sistemas receptores de GPS cada vez mais baratos e ao mesmo tempo mais presentes nas nossas vidas, como veículos, celulares, microcomputadores. Suas possibilidades e novos usos devem ser usados além de simples posicionamento ou referenciamento geodésico.

As possibilidades de se usar as informações do sistema GPS em conjunto com um sistema de criptografia são imensas, podendo criar-se sistemas que poderiam ser habilitados para funcionarem somente quando estivesse na localidade geográfica correta, no horário, ou então até mesmo na velocidade designada.

Poderia-se obrigar um caminhão ou outro tipo de transporte a percorrer um caminho pré-determinado para que ele recebesse as instruções adicionais, ou então, o endereço final. Ao mesmo tempo disso, há possibilidade de restringir o mesmo meio de transporte se ele se desviasse dos limites impostos de velocidade.

No campo de entretenimento é possível restringir que um programa somente rode a partir de certa localidade, criando uma alternativa ao uso de códigos regionais, como por exemplos nos discos de DVD ou de jogos.

É inegável a permeabilidade das tecnologias de informação e comunicações

dentro do nosso cotidiano, com aparelhos telefônicos móveis, telefones por satélites, redes de comunicação multi-nacionais e até mesmo extra-terrestres.

A concepção da alta via de informação agregando informações e serviços de forma instantânea e interativa também está presente.

As pessoas e corporações , hoje cada vez mais, utilizam a Internet, correio eletrônicos e outras aplicações para troca de dados e informações.

Dentro destes avanços tecnológicos as necessidades também foram mudando. A necessidade de uma comunicação confiável e segura, se tornaram questões inclusive de segurança nacional, onde quem tem informação tem poder.

Dentro deste escopo esta comunicação deverá preencher alguns requisitos previamente acertados no sistema, como nível de segurança, forma de comunicação e outras variáveis definidas.A criptografia e outras técnicas de segurança de dados têm uma participação fundamental no campo das comunicações, pois provê uma forma de codificar a mensagem. E tem custo computacional pequeno para seus legítimos participantes. Por outro lado, o custo computacional para um invasor ao dado ou mensagem é altíssimo, criando assim um ambiente seguro.

A comunicação deve se dar entre os participantes de forma transparente, de forma que não interrompa o funcionamento de suas outras atividades e funções. Provendo para aqueles que a utilizam uma forma rápida, barata e transparente de se comunicar.

Algoritmos com uma complexidade computacional maior, mais robustos e com a possibilidade de manter a comunicação secreta por um tempo considerável de tempo, tem se tornado cada vez mais comum e mais disponíveis. Ainda com o avanço de outras tecnologias é possível expandir a utilização e formas como a criptografia é usada.

## 1.1 Objetivos

O objetivo deste estudo visa ampliar a comunicação criptográfica e adicionar variáveis geodésicas, permitindo assim, maior confiabilidade e novas possibilidades de uso para os sistemas envolvidos.

Através de um receptor GPS os dados geodésicos serão recebidos e usados em conjunto com um módulo criptográfico para criação de uma chave e posterior decodificação de mensagens recebidas.

Desta forma só ocorrerá a decodificação correta da mensagem quando o receptor estiver nas coordenadas geodésicas corretas. Criando deste modo uma nova gama de soluções as quais podem ser ativadas ou limitadas conformes as coordenadas definidas.

# 2 Fundamentação Teórica

O objetivo desta fundamentação teórica é o de revisar alguns conceitos matemáticos, criptográficos e geodésicos utilizados, para melhor compreensão do texto.

Inicialmente será feita uma revisão matemática de alguns conceitos como campos finitos. Estes conceitos são principalmente usados no campo de criptografia e de comunicações.

Campos Finitos foram descobertos e desenvolvidos pelo grande matemático Évariste Galois [1].

Após será feita uma revisão dos principais conceitos de criptografia e do algoritmo AES(Rijndael).

E finalmente será feita uma revisão dos principais conceitos de geodesia e receptores GPS.

## 2.1 Campos Finitos

Define-se campos como um grupo de elementos(números) finitos dentro das operações de adição, subtração, multiplicação e divisão por números não nulos. Contudo um campo é um grupo de números com duas operações binárias: adição e multiplicação[2].

Estas duas operações possuem as seguintes características:

- São associativas e comutativas:$(ab) * c = a * (bc)$;
- Possuem identidades: 1
- Possuem as operações inversas: subtração e divisão;
- Possuem as regras distributivas como: $a(b + x) = ab + bx$

Estas principais características são as mais comumente usadas, outras propriedades fazem parte de um grupo menor de campos devido a complexidade de certos campos são menos usadas[1].

Um dos grupos mais conhecidos como o grupo dos inteiros $\mathbb{Z}$, não é um campo, neste caso porque $\mathbb{Z}$ não é finito na divisão. Os campos mais comuns estão dentro dos grupos dos racionais $\mathbb{Q}$, reais $\mathbb{R}$ e os números complexos $\mathbb{C}$

### 2.1.1 Adição de Campos Finitos

A adição de campos finitas é feita através da adição das potências dos dois polinômios. O modo de adição de campos finitos em bytes são diferentes dos métodos usados em números. Na computação por bytes a adição de campos finitos é feita utilizando-se a operação XOR, simbolizada aqui como $\oplus$ , na tabela 1 abaixo é demonstrado os seus resultados.

Tabela 1: Adição de Campos Finitos

| a | operador | b | resultado |
|---|---|---|---|
| 1 | $\oplus$ | 1 | 0 |
| 1 | $\oplus$ | 0 | 1 |
| 0 | $\oplus$ | 1 | 1 |
| 0 | $\oplus$ | 0 | 0 |

Ainda nesta mesma linha de raciocínio é possível descrever a adição de campos finitos como uma adição dos bits dentro dos correspondentes bytes, como por exemplo:

$$(x^6 + x^5 + x^2) + (x^7 + x + 1) = x^7 + x^6 + x^5 + x^2 \tag{1}$$

$$00110010 \oplus 01000011 = 01110011 \tag{2}$$

### 2.1.2 Multiplicação de Campos Finitos

O padrão AES utiliza a multiplicação polinomial de GF($2^8$), simbolizada aqui por " $\bullet$ ". Descreve-se esta operação como uma multiplicação de polinômios com um polinômio irredutível ( somente divisível por 1 e por ele mesmo). No caso do AES o polinômio utilizado é :

$$m(x) = x^8 + x^4 + x^3 + x + 1 \tag{3}$$

usaremos o exemplo abaixo para descrever esta operação:

$$(x^6+x^4+x^2+x+1)(x^7+x+1) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1 \quad (4)$$

reduzindo-se

$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$
$$mod(x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + 1 \quad (5)$$

Através desta redução é possível garantir que o polinômio final será de ordem inferior a 8 permitindo assim ser representado através de 1 byte. Ao contrário da adição não existe uma operação binária simples para este procedimento.

Esta multiplicação é associativa e elemento $\{01\}$ é a identidade na multiplicação. Para qualquer polinômio binário não-nulo $b(x)$ de grau menor que 8, o inverso aqui denominado de $b^{-1}(x)$ pode ser encontrado através do uso do algoritmo estendido de Euclides [3]:

$$b(x)a(x) + m(x)c(x) = 1 \quad (6)$$

Sendo que $a(x) \bullet b(x) \text{mod } m(x) = 1$, a qual se traduz por

$$b^{-1}(x) = a(x) mod\ m(x) \quad (7)$$

Ainda deduz-se que para qualquer valor de $a(x), b(x), c(x)$tem as seguintes propriedades associativas:

$$a(x) \bullet (b(x) + c(x)) = a(x) \bullet b(x) + a(x) \bullet c(x) \quad (8)$$

Por conseqüência para todos os valores possíveis de dentro de um byte (256), com a operação de XOR usada como adição e multiplicação, tem sua

estrutura definida por GF($2^8$).

### 2.1.3 Multiplicação por $x$

Um byte pode ser demonstrado através de um polinômio, com a seqüência de bits:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^{7} b_ix^i \qquad (9)$$

Multiplicando-se o polinômio acima por x ($x \bullet b(x)$) tem-se o seguinte polinômio resultante:

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \qquad (10)$$

Para obter-se o resultado da operação $x \bullet b(x)$ é necessário fazer a redução de módulo como definido na seção 1.3 (multiplicação de polinômios). Caso b7 seja igual a zero, o polinômio já se encontra na forma reduzida. Do contrário será necessária a redução subtraindo o polinômio m(x). Esta operação de multiplicação pode ser implementada binariamente através um deslocamento do byte para a esquerda e uma operação XOR condicional com {1b}. Esta operação é comumente denominada como xtime(). A operação ***xtime()*** permite que resultados intermediários sejam usados até as potências maiores finais. Por exemplo:

$$\begin{aligned} \{57\} \bullet \{13\} &= \{fe\} \\ \{57\} \bullet \{04\} &= xtime(\{ae\}) = \{47\} \\ \{57\} \bullet \{08\} &= xtime(\{47\}) = \{8e\} \\ \{57\} \bullet \{10\} &= xtime(\{8e\}) = \{07\} \end{aligned} \qquad (11)$$

por conseguinte,

$$\begin{aligned} \{57\} \bullet \{13\} &= \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\}) \\ \{57\} \oplus \{ae\} \oplus \{07\} &= fe \end{aligned}$$

### 2.1.4 Polinômios com Coeficientes em $GF(2^8)$

Um polinômio com quatro termos pode ser definido com elementos de campo finito como por exemplo em grupos de bytes[4].

Um conjunto de bytes $[a0, a1, a2, a3]$pode ser definido através do polinômio:

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \tag{12}$$

No uso para criptografia este polinômio é usado um pouco diferente do seu uso normal, utilizando bytes como coeficientes e usando um polinômio de redução diferente também.

Uma operação de adição de dois polinômios de quatro termos é feita adicionando-se os termos de iguais coeficientes. A adição corresponde a uma operação binária XOR entre os bytes correspondentes.

Seja o segundo termo:

$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \tag{13}$$

A adição seria definida por:

$$a(x) + b(x) = (a_3 \oplus b_3)x^3 + (a_2 \oplus b_2)x^2 + (a_1 \oplus b_1)x^1 + (a_0 \oplus b_0) \tag{14}$$

A multiplicação destes polinômios é feita em dois processos, primeiramente é realizada a operação de expansão e adição da equação $c(x) = a(x) \bullet b(x)$e seus coeficientes com potencias iguais somados, resultando em :

$$c(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \tag{15}$$

onde

$$\begin{aligned}
c_0 &= a_0 \bullet b_0 \\
c_1 &= a_1 \bullet b_0 \oplus a_0 \bullet b_0 \\
c_2 &= a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \\
c_3 &= a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3 \\
c_4 &= a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3 \\
c_5 &= a_3 \bullet b_2 \oplus a_2 \bullet b_3 \\
c_6 &= a_3 \bullet b_3
\end{aligned}$$

O polinômio c(x), por sua estrutura, não representa desta forma uma variável de 4 bytes como necessária para algumas operações de criptografia como a AES. Para tanto, é necessário executar uma redução deste polinômio para um grau menor que 4. Esta redução pode ser feita com o polinômio $x^4 + 1$ descrita pela equação:

$$x^i mod(x^4 + 1) = x^{i \, mod \, 4} \tag{16}$$

Sendo assim o produto modular entre a(x) e b(x) sendo simbolizado por $a(x) \otimes b(x)$ tem como resultante o polinômio d(x) definido como:

$$d(x) = d_3x^3 + d_2x^2 + d_1x + d_0 \tag{17}$$

sendo que,

$$d_0 = (a_0 \bullet b_0) \oplus (a_3 \bullet b_1) \oplus (a_2 \bullet b_2) \oplus (a_1 \bullet b_3) \tag{18}$$

$$d_1 = (a_1 \bullet b_0) \oplus (a_0 \bullet b_0) \oplus (a_3 \bullet b_2) \oplus (a_2 \bullet b_3) \tag{19}$$

$$d_2 = (a_2 \bullet b_0) \oplus (a_1 \bullet b_1) \oplus (a_0 \bullet b_2) \oplus (a_3 \bullet b_3) \tag{20}$$

$$d3 = (a_3 \bullet b_0) \oplus (a_2 \bullet b_1) \oplus (a_1 \bullet b_2) \oplus (a_0 \bullet b_3) \tag{21}$$

## 2.2 Criptografia

Criptografia origina-se da palavra grega *cryptos* ao qual significa secreto ou oculto. O objetivo do estudo da criptografia são os métodos e meios de codificação de mensagens ou dados para que somente um receptor legítimo daquela informação possa ter acesso. Ao mesmo que temos a sua ciência "irmã" chamada criptoanálise, que estuda os meios de decifrar uma mensagem criptografada, sem a totalidade das informações necessárias para decodificar a mensagem corretamente[5].

Dentro da criptografia tem-se as seguintes características principais as quais tem sido evoluídas ou modificadas conforme os avanços tecnológicos[6]:

1. Confidencialidade: a mensagem criptografada não pode ser lida por alguém não autorizado;
2. Integridade: quando criptografada qualquer tentativa de mudar a mensagem é detectada;
3. Sem repúdio: o enviante depois de a ter enviado não pode negar o envio desta mesmo;
4. Autenticidade: tanto receptor quanto receptor podem confirmar as suas identidades.

### 2.2.1 Histórico

A criptografia vêm desempenhando um papel importante desde os tempos mais antigos da humanidade, principalmente na transmissão de mensagens

militares ou até mesmo para fórmulas secretas. Abaixo temos os principais usos de criptografia dentro da linha do tempo:

- 1900 A.C: escritos egípcios de forma não padrão são usados por um escriba desconhecido;
- 1500 A.C.: é encontrada uma formula encriptada de um procedimento para pintura de potes de barro;
- 500 a 600 A.C.: escribas hebreus usam uma forma de criptografia no livro de Jeremias;
- 487 A.C.: uso do aparelho skytel pelos gregos, era composta de um cinto de seda em conjunto com um pedaço de madeira. Primeiro uso de esteganografia registrado, os mensageiros tinham suas cabeças raspadas. E era escrita a mensagem em suas cabeças e quando o cabelo cresciam eles eram enviados para transmitir a mensagem;
- 50 a 60 A.C.: Julius Caesar desenvolve o algoritmo de troca e substituição que seria no futuro conhecido pelo seu nome;
- 1 a 400 D.C : Mallanaga Vatsayana da Índia descreve a criptografia como uma forma de yoga, dentro de seu compêndio de conhecimentos conhecido como Kama Sutra;
- 200 D.C : Os papiros de Leiden são encontrados com supostas fórmulas mágicas;
- 725 a 855 D.C: várias escrituras e papiros persas são usados para comunicações militares principalmente entre as "embaixadas" em áreas militarizadas do mundo árabe;
- 1226: Nos arquivos de Veneza é encontrada uma forma simples de criptografia onde pontos e cruzes substituíam vogais;
- 1250: Roger Bacon, escreve que "é louco aquele que escreve um segredo de outra forma que não a de manter segredo do profano";

- 1379: Gabrieli di Lavinde a pedido do Papa Clemente VII desenvolve um método de criptografia usando substituição de alfabeto e códigos;
- 1412: Numa enciclopédia árabe é encontrado um capítulo inteiro sobre criptografia, falando especialmente de substituição e justaposição, com exemplos e demonstrações de uso;
- 1466: Leon Battista Alberti desenvolve o primeiro encriptador polialfabético e constrói um disco de encriptação;
- 1518: Johannes Trithemius escreve e publica o primeiro livro sobre criptografia chamado Poligraphiae Libri Sex;
- 1553: Giovan Batista Belaso adiciona uma chave ao método de Johannes Trithemius;
- 1623: Sir Francis Bacon: descreve um sistema bilateral de criptografia, que considerava uma forma de esteganografia.
- 1790: Thomas Jefferson inventa seu disco de criptografia;
- 1817: Coronel Decius Wadsworth constrói um sistema de disco criptográfico com números diferentes de letras e números, resultando numa forma progressiva de permutação e criptografia;
- 1854: Charles Wheatstone desenvolve o sistema PlayFair de criptografia;
- 1859: Pliny Earle Chase publica a primeira criptografia de fracionamento;
- 1861: Friederich W. Kasiski publica a solução para criptografia polialfabética com chaves idênticas;
- 1895: com o desenvolvimento comercial do rádio por Guglielmo Marconi, causou uma grande evolução no campo da criptografia. Não necessitando mais de fios para a transmissão de mensagens para a transmissão e recepção o campo de criptografia se desenvolveu bastante;

- 1917-1918: é criado o Bureau de Criptografia dos Estados Unidos como parte da inteligência militar;
- 1939: o sistema de Criptografia Enigma é quebrado
- 1976: o sistema desenvolvido pela IBM chamado de DES é selecionado como o padrão para os Estados Unidos;
- 1976: Withfield Diffie e Martin Hellmann publicam "New Directions in Cryptography" abrindo caminho para criptografia de chaves públicas;
- 1977: Ronald Rivest, Adi Shamir e Leonard Adleman criam o método de criptografia chamado de RSA, baseado no trabalho de Withfield Diffie e Martin Hellmann. Sua segurança é baseada principalmente na dificuldade de se fatorar números grandes;
- 1982: Criação da criptografia quântica por Gilles Brassard e Charles Bennett;
- 1991: Phil Zimmermann lança a primeira versão do PGP, criando um meio fácil para que pessoas comuns pudessem ter uma criptografia de bom nível;
- 2001: Publicação da AES como escolha para criptografia dos órgãos governamentais americanos.

### 2.2.2 Sistemas Assimétricos e Simétricos

No caso de sistemas simétricos, as chaves de encriptação são iguais a de decodificação, causando assim, que elas tenham que ser transmitidas antes da comunicação da mensagem enviada. Devido ao fato das chaves serem iguais o sistema é chamado de simétrico.

Nos sistemas assimétricos as chaves denominadas D e F são distintas e de difícil computabilidade. Neste caso, a chave de encriptação pode ser pública, enquanto que a chave de decodificação é guardada. Num exemplo, os usuários X e Y transmitem um ao outro suas chaves de encriptação mas guardam as suas chaves de decriptação em segredo. Assim sendo a outra

parte envolvida sabe como encriptar a mensagem, porém não tem acesso à função de decodificar a mensagem da outra parte.[7]

Este sistema de "trocas" de chaves é comumente chamado de sistemas de chaves públicas ou PKI[6].

### 2.2.3 Sistema de Criptografia de Chaves Públicas e Privadas (RSA)

Um dos sistemas criptográficos de chaves públicas e privadas mais conhecido é o RSA. Seu nome provêm dos autores deste sistema os três colegas R. L. Rivest, A. Shamir e L. Adlemann que em 1978 criaram o sistema dentro do Massachusetts Institute of Technology, principalmente depois da difusão do uso da internet, este se tornou o protocolo mais usado, sendo usado principalmente em navegadores de internet[5].

Pode-se definir um sistema de criptografia de chaves públicas e privadas através dos seguintes componentes (P, C, K, E, D), com as seguintes definições:

1. P é considerado o conjunto plaintext ou o texto não criptografado;

2. C é o conjunto de texto criptografado;

3. K é o conjunto de chaves usadas;

4. E são famílias de funções que neste caso executam ou transformam o texto não criptografado em texto criptografado;

5. D são famílias de funções que permitem a transformação do texto criptografado em texto não criptografado;

Para cada função de criptografia existe uma função correspondente para decodificar a mensagem.

Para exemplificar um destinatário denominado X quer transmitir a mensagem dentro do conjunto (P) para o destinatário Y. Para transmitir ele iria usar a função (E) em conjunto com as chaves (k) para transmitir. Enquanto que no outro lado seria usada as funções (D(eM)) para decodificar[8]

### 2.2.4 Ataques na Criptografia

Da mesma forma que a criptografia tem como interesse manter as informações confidencias, existe toda uma classe e um grupo de ataques destinados a decodificar a mensagem ,com nenhuma ou alguma informação, das chaves e métodos de criptografia[3].

Os principais tipos de ataques são:

- Ataque de texto criptografado: neste caso o atacante tenta descobrir a chave ou texto decodificado somente através do texto criptografado;
- Ataque com texto descriptografado conhecido: neste caso o atacante possui uma parte ou texto decodificado e seu correspondente texto criptografado;
- Ataque com texto decodificado escolhido: neste ataque é escolhido um texto decodificado e através de ataques são fornecidos textos correspondentes codificados. Através deste método é tentado descobrir os dados de outros textos decodificados;
- Ataque com texto decodificado escolhido adaptado: é escolhido um texto específico durante os ataques permitindo uma melhor análise em alguns casos;
- Ataque com texto codificado escolhido: neste ataque é selecionado especificamente um texto a ser codificado e é recebido o texto decodificado. Usado principalmente para compreensão do processo de decodificação aonde não se tem a chave de decodificação. Geralmente usado quando se tem acesso ao equipamento de decodificação;
- Ataque com texto codificado adaptável: nesta caso o ataque são feitos com textos codificados específicos e conforme se progredi nos ataques estes textos são mudados para melhor interpretação dos dados recebidos.

Estes ataques se concentram basicamente no modelo de codificação de textos, caso o ataque seja feita em protocolos, tem-se os seguintes métodos de ataque:

- Chaves já previamente conhecidas: neste ataque já se possui algumas chaves previamente usadas, e elas são usadas para determinar as chaves de decodificação novas;

- Reprodução: neste caso uma sessão de codificação é gravada e usada posteriormente para análise ou ataque;

- Impersonificação: neste ataque o atacante se identifica como uma parte legítima do processo, obtendo vantagens;

- Ataque por dicionário: neste caso um grande dicionário com algumas variantes é usado para atacar o protocolo de segurança;

- Homem no meio: neste ataque o atacante se disfarça de uma parte legítima e age como intermediário;

- Ataque por diferença de tempo: em algumas operação de codificação e decodificação o tempo de uma chave errada é diferente da chave certa, deste modo o atacante faz uma análise dos tempos para obter uma vantagem[9, 3];

Estes são os modos principais de ataque importante de se notar, que conforme as tecnologias avançam, outros ataques serão criados.

### 2.2.5 Avaliação da Segurança de Sistemas Criptográficos

A segurança dos sistemas criptográficos e protocolos podem ser realizadas de várias formas. A comunidade científica, através de pesquisas, tenta avaliar a segurança de um sistema criptográfico de diversas formas. Tem-se como as principais, os seguintes modelos de avaliação[3]:

- Segurança incondicional ou confidencialidade perfeita: neste caso é uma forma de modelagem teórica que tenta avaliar que o atacante possui infinitos recursos computacionais, e se ele consegue ou não decodificar a mensagem através somente do texto codificado. Neste caso, principalmente a observação do texto criptografado não produz nenhum

padrão perceptível para a decodificação do texto. Esta perfeita confidencialidade se torna cada vez mais fraca conforme o número de textos criptografados aumentam;

- Complexidade teórica: neste modelo a codificação se utiliza de métodos matemáticos onde ,no pior dos casos, assume que o atacante tem um alto grau de capacidade computacional ainda é impraticável a decodificação ou ataque do sistema criptográfico;

- Segurança provável: neste caso o sistema criptográfico é considerado seguro pelo fato de ser supostamente tão difícil de ser computado quanto a um outro problema de difícil computabilidade;

- Segurança computacional: é medida a melhor capacidade computacional, dentro dos melhores métodos e então através de uma grande margem de segurança é definida a segurança do sistema frente a um atacante. Esta característica é mais conhecida como segurança prática. Importante notar isso através do avanço da tecnologia e de novas formas de computação;

- Segurança Ad Hoc: neste modelo de segurança, se supõe que o atacante deverá ter algum recurso como tempo ou espaço superior ao tempo necessário para decodificar a mensagem.

### 2.2.6 Processo de escolha Padrão AES

Depois de algumas pesquisas indicando que o DES (Data Encryption Standard), padrão usado pelo governo dos Estados Unidos para criptografia em documentos não classificados como de altíssima segurança, foram publicadas[10] o governo dos Estados Unidos num esforço com a comunidade científica global, lançou o desafio chamado AES (Advanced Encryption Standard) que iria escolher o sucessor do DES[4].

Este processo de escolha iniciou-se em 1997 com iniciativa do NIST, departamento responsável pelas padronizações e processos deste tipo. Dentro desta primeira chamada foram estabelecidos alguns parâmetros mínimos como por exemplo:

1. Bloco mínimo de dados: 128 bits;

2. Tamanho mínimo de chaves: 128, 192 e 256 bits;

3. Sem cobrança de Royalties ou licenças;

4. Para uso público e de graça;

Iniciado o processo, foram submetidos quinze candidados de diversos países conforme tabela 2.

Tabela 2: Candidados Inicias para o AES

| País | Algoritmo | Autor |
|---|---|---|
| Austrália | LOKI97 | Lawrie Brown, Josef Pieprzyk, Jennifer Seberry |
| Bélgica | RIJNDAEL | Joan Daemen, Vincent Rijmen |
| Canada | CAST-256 | Entrust Technologies, Inc. |
| Canada | DEAL | Richard Outerbridge, Lars Knudsen |
| Costa Rica | FROG | TecApro Internacional S.A. |
| França | DFC | Centre National pour la Recherche Scientifique (CNRS) |
| Alemanha | MAGENTA | Deutsche Telekom AG |
| Japão | E2 | Nippon Telegraph and Telephone Corporation (NTT) |
| Coréia | CRYPTON | Future Systems, Inc. |
| EUA | HPC | Rich Schroeppel |
| EUA | MARS | IBM |
| EUA | RC6 | RSA Laboratories |
| EUA | SAFER+ | Cylink Corporation |
| EUA | TWOFISH | Bruce Schneier, John Kelsey, Doug Whiting,. David Wagner, Chris Hall, Niels Ferguson |
| UK, Israel, Noruega | SERPENT | Ross Anderson, Eli Biham, Norway Lars Knudsen |

Cada representante de seu sistema de algoritmo fez uma apresentação indicando as maiores virtudes e características do seu algoritmo[11].

Dentro da chamada para a submissão dos padrões foram incluidos critérios aos quais os algoritmos serão avaliados, como os seguintes:

- Segurança;
- Portabilidade;
- Custo computacional;

A questão da segurança é de extrema importância pois outros padrões como DES já não estavam mais sendo considerados suficientemente seguros. Portabilidade é extremamente importante visto que o algoritmo finalista será usado em diversos ambientes e diferentes tipos de plataformas como circuitos embarcados, smart-cards e outros. O custo computacional também é importante porque o desempenho deverá ser aceitável em plataformas com poucos recursos, para que o padrão seja usado em um maior conjunto de plataformas e funções.

Em Agosto de 1999 houve a escolha de cinco algoritmos candidatos, constituindo-se no chamado "segundo round". Os cinco finalistas foram os algoritmos: MARS, RC6, Rijndael, SERPENT e TWOFISH.

Estes cinco finalistas possuem algumas características em comum como, por exemplo, serem algoritmos de encriptação de bloco iterativo. Neste tipo de processamento a chave principal é expandida em várias sub-chaves, e em cada iteração é usada uma sub-chave diferente. O processo de uma iteração com uma sub-chave é denominado ciclo.

Ainda dentro destes cinco finalistas foi implementado o processo de misturar a chave com dados a serem criptografados. Caso o algoritmo não tenha feito isso, no inicio ou final, ele é feito dentro de cada ciclo, prevenindo assim a capacidade de um atacante de poder encriptar ou decodificar uma mensagem sem possuir a chave certa.

Outra similaridade encontrada nos algoritmos foi o uso de tabelas de permutações, mais conhecidas como S-Box. Nestas tabelas, suas operações se fazem pelas entradas de bits A que geram uma saída B de bits na tabela.

Dentro destes cinco finalistas foi feito um resumo das principais características e vantagens, que resumidamente são apresentadas [11]:

- MARS: Usando uma mistura de ciclos principais utilizando-se de Feistel e de ciclos normais, contendo até 25 variações. Esta mistura foi uma forma inovadora, sendo assim não citaram nenhum algoritmo como antecessor.

- RC6: O algorítimo RC6 é uma evolução do algoritmo RC5 ao qual já é conhecido da comunidade acadêmica. O principal deste algoritmo são os ciclos variáveis que possuem boas propriedades de segurança. A variação nos ciclos tem como origem reguladora uma função quadrática dos dados, onde o sistema de ciclos do RC6 é uma variante da construção Feistel.

- Rijndael: Este algoritmo foi feito baseado num desenho de um quadrado. Além disso este algoritmo funciona orientado a bytes. Grande parte das operações são padrão. A principal diferença é o uso de Campos de Galois (GF) e de transformações na tabela de permutações.

- SERPENT: Algoritmo também orientado a bytes, com operações padrões. A tabela de permutações é gerada da mesma forma que a do padrão DES.

- TWOFISH: O algoritmo TWOFISH utiliza uma forma modificada da estrutura de Feistel, com sua tabela de permutações dependentes da chave.

Importante salientar que todos estes algoritmos candidatos declararam que não possuem nenhum tipo de brecha de segurança intencional (*trapdoor*).

#### 2.2.6.1 Análise de segurança dos Algoritmos Finalistas

No processo de escolha do algoritmo padrão para o AES, os cinco finalistas foram testados em vários quesitos para melhor escolha do finalista.

No caso de avaliação da segurança do algoritmo foi usado o método de busca exaustiva da chave, ou seja , o total de operações necessárias para a

descoberta da chave em todas as possibilidades. No caso a análise foi feita com ciclos reduzidos por questões práticas de avaliação.

Na composição da avaliação foram usados os seguintes itens:

1. Texto: Quantidade de parâmetros de texto e seus correspondentes textos criptografados para a realização do ataque;
2. Uso de memória: tamanho de memória máximo a ser utilizado no ataque;
3. Operações: número de operações necessárias para o ataque.

Tabela 3: Sumário de Analise de segurança dos Algoritmos[11]

| Algoritmo Ciclos | Artigo | Ciclos (chave) | Ataque | Texto | Mem. | Oper. |
|---|---|---|---|---|---|---|
| MARS | [12] | 11C | Amp. Boomerang | $2^{65}$ | $2^{70}$ | $2^{229}$ |
| 16 Cocc(C) 16 Mixing(M) | [13] | 16M, 5c | M.I.M | 8 | $2^{236}$ | $2^{232}$ |
| | | 16M, 5c | Diff. M.I.M | $2^{50}$ | $2^{197}$ | $2^{247}$ |
| | | 16M, 5c | Amp. Boomerang | $2^{69}$ | $2^{73}$ | $2^{197}$ |
| RC6 | [14] | 14 | Stat. Disting. | $2^{118}$ | $2^{112}$ | $2^{122}$ |
| 20 | [15] | 12 | Stat. Disting. | $2^{94}$ | $2^{42}$ | $2^{119}$ |
| | | 14(192,256) | Stat. Disting. | $2^{110}$ | $2^{42}$ | $2^{135}$ |
| | | 14(192,256) | Stat. Disting. | $2^{108}$ | $2^{74}$ | $2^{160}$ |
| | | 15(256) | Stat. Disting. | $2^{119}$ | $2^{138}$ | $2^{215}$ |
| Rijndael | [16] | 4 | Truncated Diff. | $2^{9}$ | pequena | $2^{9}$ |
| 10(128) | | 5 | Truncated Diff. | $2^{11}$ | pequena | $2^{40}$ |
| 12(192) | | 6 | Truncated Diff. | $2^{32}$ | $7 * 2^{32}$ | $2^{72}$ |
| 14(256) | [17] | 6 | Truncated Diff. | $6 * 2^{32}$ | $7 * 2^{32}$ | $2^{44}$ |
| | | 7(192) | Truncated Diff. | $19 * 2^{32}$ | $7 * 2^{32}$ | $2^{155}$ |
| | | 7(256) | Truncated Diff. | $21 * 2^{32}$ | $7 * 2^{32}$ | $2^{172}$ |
| | | 7 | Truncated Diff. | $2^{128} - 2^{119}$ | $2^{61}$ | $2^{120}$ |
| | | 8(256) | Truncated Diff. | $2^{128} - 2^{119}$ | $2^{101}$ | $2^{204}$ |
| | | 9(256) | Chave Relacionada | $2^{77}$ | N.D | $2^{224}$ |
| | [18] | 7(192) | Truncated Diff. | $2^{32}$ | $7 * 2^{32}$ | $2^{184}$ |
| | | 7(256) | Truncated Diff. | $2^{32}$ | $7 * 2^{32}$ | $2^{200}$ |
| | [19] | 7(192, 256) | Truncated Diff. | $2^{32}$ | $7 * 2^{32}$ | $2^{140}$ |
| Serpent | [12] | 8(192,256) | Amp. Boomerang | $2^{113}$ | $2^{119}$ | $2^{179}$ |
| | [20] | 6(256) | M.I.M | 512 | $2^{246}$ | $2^{247}$ |
| | | 6 | Diff. | $2^{83}$ | $2^{40}$ | $2^{90}$ |
| | | 6 | Diff. | $2^{71}$ | $2^{75}$ | $2^{103}$ |
| | | 6(192,256) | Diff. | $2^{41}$ | $2^{45}$ | $2^{163}$ |
| | | 7(256) | Diff. | $2^{122}$ | $2^{126}$ | $2^{248}$ |
| | | 8(192,256) | Boomerang | $2^{128}$ | $2^{133}$ | $2^{163}$ |
| | | 8(192,256) | Amp. Boomerang | $2^{110}$ | $2^{115}$ | $2^{175}$ |
| | | 9(256) | Amp. Boomerang | $2^{110}$ | $2^{212}$ | $2^{252}$ |
| TwoFish | [21] | 6(256) | Impossible Diff. | ND | ND | $2^{256}$ |
| 16 | [22] | 6 | Chave Relacionada | ND | ND | ND |

Importante notar que como a tabela 3 mostra todos os candidados apresentaram uma boa segurança, exigindo-se que o atacante tenha no mínimo $2^{30}$ textos específicos encriptados. Com esta dimensão seria necessário que o atacante tivesse acesso físico ao dispositivo de encriptação com a mesma chave.

Dentro da avaliação feita pelo NIST, foram considerados também a margem de segurança, o desenho do algoritmo e a simplicidade do mesmo.

#### 2.2.6.2 Análise da Margem de Segurança dos algoritmos

Margem de segurança é uma análise que se faz no algoritmo, levando-se em conta o desenvolvimento das tecnologias atuais. É uma suposição de quanto tempo um algoritmo levará para ficar obsoleto considerando-se a velocidade da evolução da tecnologia atualmente.

A métrica usada foi retirada inclusive dos comentários feitos durante o processo[23].

O fator de segurança neste estudo era definido sendo $a$ o número total de ciclos do algoritmo e $b$ o total destes ciclos que já foram quebrados o fator de segurança é equacionado da seguinte forma:

$$\sigma = \frac{a}{b} \tag{22}$$

Por esse modelo, um algoritmo que estivesse já com todos os seus ciclos quebrados teria um valor de 1, enquanto que o mesmo algoritmo caso estivesse somente com a metade dos ciclos quebrados teria um valor de 2.

Apesar de ser uma medida que busca racionalizar esta questão, ela apresenta alguns problemas na avaliação do candidado para o padrão AES. Algoritmos mais antigos e portanto mais explorados, teriam teoricamente mais chances de serem quebrados que os algoritmos mais inovadores ou originais. E nem sempre o algoritmo inovador ou original é o mais seguro, um algoritmo bem conhecido tem a vantagem de ter mais tempo de avaliação.

Portanto na escolha do AES foram usados todos os dados possíveis inclusive não publicados para a avaliação[11].

Desta forma as seguintes conclusões foram feitas dos algoritmos:

- MARS: Os resultados do algoritmo MARS são extremamente dependentes do pré-processamento e pós-processamentos, que contendo 16 ciclos sem relação com a chave e mais 16 ciclos principais com a chave. Com a utilização da chave durante os ciclos, a segurança aumenta dramaticamente, comparada a não utilização da chaves nos ciclos.

- RC6: Ataques foram criados para ciclos de 12, 14 e 15. Ainda assim os próprios criadores do algoritmo supõem que ataques até 16 ciclos são passíveis de serem criados[24]. Com um total de 20 ciclos e ataques até 16 ciclos, o algoritmo RC6 foi considerado com uma margem de segurança adequada.

- Rijndael: A estrutura de ciclos é dependente do tamanho de chave. Com chaves de 128 bits ataques foram executados em até 7 ciclos do total de 10, sendo que o ataque de até 7 ciclos necessitou praticamente quase toda a exaustão de todas as chaves possíveis. Para chaves de 192 7 ataques até o sétimo ciclo de um total de 12 foram possíveis. Com chave de 256 bits ataques até 9 ciclos de um total de 14 foram executados, sendo que o ataque com 8 ciclos exigiu a quase exaustão de todas as chaves possíveis e no ataque de 9 ciclos requeria encriptação de chaves específicas. Considerou-se que o algoritmo possui uma margem de segurança adequada.

- Serpent: Ataques até 9 ciclos do total de 32 ciclos foram possíveis. Este algoritmo apresentou uma alta margem de segurança.

- TWOFISH: Foram criados ataques até 6 ciclos de um total de 16 sendo necessária operações de encriptação em chaves específicas. Usando a chave de 256 bits neste algoritmo o ataque proposto de até 6 ciclos se mostrou tão efetivo quanto a exaustão de todas as chaves possíveis. Este algoritmo apresentou uma alta margem de segurança.

Todos os candidatos apresentaram uma margem de segurança adequada[11].

#### 2.2.6.3 Avaliação de Desempenho e Portabilidade dos Finalistas

Na avaliação, o desenho do algoritmo foi considerado também, para avaliar como a implementação do algoritmo iria ocorrer nas diversas plataformas, considerando-se também, o consumo de recursos e de memória. O desempenho é muito importante visto que o algoritmo vai ser empregado em diversas situações e sendo em muita delas em sistemas embarcados e portáteis.

Para isso, foram testadas as velocidade de codificação e decodificação em varias plataformas, inclusive a desempenho das operações com a chave (Key Scheduling).

Nas tabelas 4 e 5 têm-se demonstrado o resultado.

Tabela 4: Desempenho em codificação e decodificação

| | 32-bit (c) | 32-bit (Java) | 64-bit (C e Assembler) | 8-bit(C e Assembler) | 32-bit Smartcard | DSP |
|---|---|---|---|---|---|---|
| MARS | II | II | II | II | II | II |
| RC6 | I | I | II | II | I | II |
| Rijndael | II | II | I | I | I | I |
| Serpent | III | III | III | III | III | III |
| TWOFISH | II | III | I | II | III | I |

Nas tabelas interpreta-se o I como o mais veloz e III como o mais lento.

Tabela 5: Desempenho com as operações de Chave

| | 32-bit (c) | 32-bit (Java) | 64-bit (C e Assembler) | 8-bit(C e Assembler) | DSP |
|---|---|---|---|---|---|
| MARS | II | II | III | II | II |
| RC6 | II | II | II | III | II |
| Rijndael | I | I | I | I | I |
| Serpent | III | II | II | III | I |
| TWOFISH | III | III | III | II | III |

Importante notar que o algoritmo Rijndael, em termos de desempenho, claramente foi o campeão de todos os algoritmos conforme as tabelas 4 e 5.

Foram feitas várias análises, de segurança, desempenho, portabilidade e outros. Através de um processo rigoroso e em constante acompanhamento da comunidade científica foi escolhido o sistema Rijndael por se apresentar como uma excelente escolha nos quesitos de segurança, portabilidade e velocidade[11].

Após o processo de escolha foi decidido que o padrão Rijndael seria o novo AES [4], sendo denominado publicamente como AES.

Mesmo o processo sendo de 2001, atualmente alguns artigos confirmam as qualidades do AES como desempenho[25, 26, 27]. E ainda alguns artigos confirmam a capacidade de velocidade e portabilidade nas mais diversas plataformas e usos[28, 25].

O AES se constitui de bloco de dados fixos de 128 bits e chaves de: 128, 192 e 256 bits.

O padrão AES determina as seguintes condições mínimas para os tamanhos de chaves:

Tabela 6: Requisitos para tamanho de chave e ciclos

| | Tamanho da chave (NK ) | Tamanho do Bloco(NB) | Numero de Ciclos |
|---|---|---|---|
| AES-128 | 128 | 128 | 10 |
| AES-192 | 192 | 128 | 12 |
| AES-256 | 256 | 128 | 14 |

O uso de 14 voltas e de uma chave de 256 bits no AES é principalmente para aumentar a segurança e evitar t*iming attacks* [29].

### 2.2.7 Algoritmo AES(Rijndael)

Internamente no seu algoritmo o AES, realiza suas operações dentro de uma matriz de duas dimensões denominada "State". Esta matriz é formada por 4 colunas de *bytes*, cada uma contendo N bytes, sendo que NB é o tamanho do bloco dividido por 32. Dentro desta matriz de Estados aqui denominada por "S", dois índices são usados para cada *byte* individualmente ("r" para linha e "c" para coluna). Deste modo, um byte individual pode ser denominado como s[r,c] dentro da matriz de estados.

Tanto no processo de codificação quanto de decodificação, a entrada e saída dos bytes da matriz se da mesma forma, conforme demonstrado na figura abaixo. A entrada denominada de *in*, a matriz de estado de $S$ e saída de *out*.

Esta cópia dos dados de entrada para a matriz de dados segue a seguinte fórmula:

$$s[r,c] = in[r+4c] sendo\, que\, 0 \leq 4,\ 0 \leq c < Nb \tag{23}$$

- **AddRoundKey()**: Transformação tanto na codificação quanto na decodificação, onde a RoundKey é adicionada para a matriz de estados usando operações de XOR;
- **K** : Chave criptográfica;
- **MixColumns():** Transformação no codificador ao qual transforma todas as colunas da matriz de estados e mistura seus dados para formar outras colunas;

- **Nb**: Número de colunas cada qual com tamanho de 32 bits. Seguindo o padrão FIPS deve se usar 4 colunas[4];
- **Nk**: Tamanho da chave
- **Nr**: Número de rounds;
- **RotWord()**: função na expansão de chave que recebe uma sentença de 4 bytes e faz uma permutação cíclica;
- **ShiftRows()**: Processo dentro do codificador ao qual desloca ciclicamente as últimas três linhas da matriz de estados;
- **SubBytes()**: Transformação no codificador ao qual processa a matriz de estados utilizando uma tabela de substituição;
- **SubWord()**: é a função usada na expansão da chave onde se pega uma palavra de quatro bytes e aplica-se a matriz de permutação "S", para cada um dos quatro bytes, produzindo uma palavra na saída do processo.
- **Rcon[]**: Lista de constantes dos ciclos;
- **InvMixColumns()**: operação inversa de MixColumns().
- **InvShiftRows()**: operação inversa de ShiftRows().
- **InvSubBytes()**: Operação inversa de SubBytes().

**2.2.7.1 A codificação do AES** Para uma chave de 256 bits são feitas 14 ciclos no algoritmo, um ciclo é composta pelos seguintes processos: criação da matriz de estados, deslocamento, combinação dos dados com a matriz de estados, adição da chave à matriz de estado. Estes passos são denominados como SubBytes(), ShiftRows(), MixColumns(), e AddRoundKey(), são executados em todas as voltas somente na última volta o MixColumns não é executado.

Na figura 1 o diagrama onde é demonstrada a atuação destas funções.

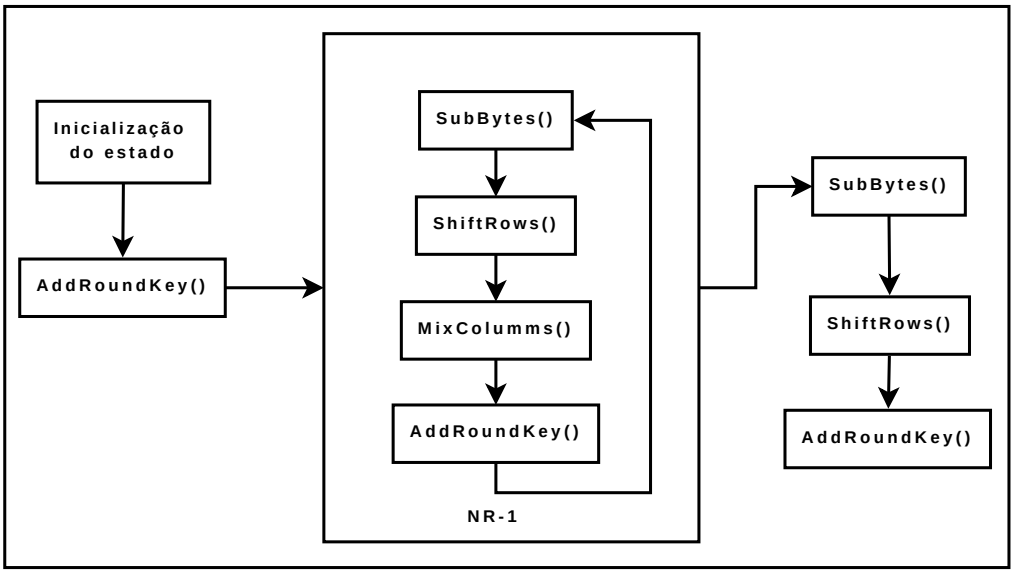


Figura 1: Diagrama de Codificação AES

Primeiramente, é copiado os valores de entrada dentro da matriz de estado e em seguida, é feita a operação de AddRoundKey. Logo após é realizado um conjunto de operações em círculos determinadas pelo parâmetro Nr(número de ciclos).

Na função SubBytes é feita uma substituição não linear independente dos bytes, utilizando uma matriz de substituição inversível chamada de S-box.

A matriz S-box é constituída dos seguintes passos:

1. Utiliza-se o multiplicativo inverso dos campos finitos em GF($2^8$), sendo que o elemento $\{00\}$ é mapeado para ele mesmo;

2. Utiliza-se da transformação:

$$b'_i = b_i \oplus b_{(i+4)mod\,8} \oplus b_{(i+5)mod\,8} \oplus b_{(i+6)mod\,8} \oplus b_{(i+7)mod\,8} \oplus c_i \qquad (24)$$

Sendo que $0 \leq i < 8$, e $b_i$ é o n-enésimo bit do byte, e $c_i$ é o enésimo bit do byte de valor $\{63\}$ ou $\{01100011\}$. Sempre que $b'$for um número primo, a variável deve ser atualizada com o valor da direita.

Matricialmente podemos representar estas operações binárias da seguinte forma:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Após é executada a função de ShiftRows(). Nesta função as últimas três linhas são deslocadas circularmente, de formas diferentes entre elas. A primeira coluna não é modificada.

A definição matemática é :

$$S'_{r,c} = S_{r,(c+deslocamento(r,4))mod4} \tag{25}$$

,sendo que 0<r<4

Na prática isso faz com que os bytes sejam deslocados à esquerda (posições mais baixas), nas matrizes abaixo é demonstrado.

| | | | |
|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ |
| $S_{1,0}$ | $S_{1,1}$ | $S_{1,2}$ | $S_{1,3}$ |
| $S_{2,0}$ | $S_{2,1}$ | $S_{2,2}$ | $S_{2,3}$ |
| $S_{3,0}$ | $S_{3,1}$ | $S_{3,2}$ | $S_{3,3}$ |

$\Rightarrow$

| | | | |
|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ |
| $S_{1,1}$ | $S_{1,2}$ | $S_{1,3}$ | $S_{1,0}$ |
| $S_{2,2}$ | $S_{2,3}$ | $S_{2,0}$ | $S_{2,1}$ |
| $S_{3,3}$ | $S_{3,0}$ | $S_{3,1}$ | $S_{3,2}$ |

Logo em seguida é feito o processo da função MixColums(). Neste processo as colunas são utilizadas como polinômios de GF($2^8$) e multiplicadas pelo modulo $x^4 + 1$ com o polinômio fixo:

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

Simbolicamente representada como:

$$s'(x) = a(x) \otimes s(x) \tag{26}$$

Matricialmente representada como:

$$\begin{bmatrix} S_{\prime 0,c} \\ S_{\prime 1,c} \\ S_{\prime 2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

O resultado desta multiplicação é:

$$S'_{0,c} = (\{02\} \bullet S_{0,c}) \oplus (\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c} \tag{27}$$

$$S'_{1,c} = S_{0,c} \oplus (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{3,c} \tag{28}$$

$$S'_{2,c} = S_{0,c} \oplus S_{1,c} \oplus (\{02\} \bullet S_{2,c}) \oplus (\{03\} \bullet S_{3,c}) \tag{29}$$

$$S'_{3,c} = (\{03\} \bullet S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (\{02\} \bullet S_{3,c}) \tag{30}$$

Após estas funções de substituições e permutações tem-se a função AddRoundKey(), a qual adiciona às colunas da matriz de estados, uma variável de mesmo tamanho da coluna.Variável esta criada dentro do processo de expansão da chave.

Em cada ciclo é adicionada uma palavra diferente, na equação é descrita esta função.

$$[S'_{0,c}, S'_{1,c}, S'_{2,c}, S'_{3,c}] = [S_{0,c}, S_{1,c}, S_{2,c}, S_{3,c}] \oplus [Palavra_{Ciclo*Nb+c}] \quad (31)$$

É feita uma AddRoundKey inicial, e após são realizados sucessivos processos durante os ciclos internos de criptografia.

#### 2.2.7.2 Expansão da Chave (Key Expansion)

Dentro do algoritmo de AES a chave simbolizada por K é expandida para um número total de palavras de $Nb(Nr + 1)$. Dentro do processo de codificação são necessárias inicialmente palavras do tamanho de Nb (4 colunas no caso), ainda em cada ciclo requerem mais 4 palavras. No final, tem-se um grupo de palavras de 4 bytes, denominadas $w_i$ de tamanho definido por $0 \leq iNb(Nr + 1)$.

Neste processo, primeiramente é utilizada a função SubWord(), a qual recebe uma palavra de 4 bytes de entrada e aplica o processo de S-box para cada um dos bytes formando na saída um palavra também de quatro bytes. Após a função RotWord() utiliza-se desta palavra e faz uma permutação simples, conforme abaixo:

$$[a_0, a_1, a_2, a_3] \longrightarrow [a_1, a_2, a_3, a_0] \quad (32)$$

Logo após é feita uma operação de XOR com Rcon[i] que é definido por: $[x^{i-1}, \{00\}, \{00\}, \{00\}]$, sendo que em $x^{i-1}$as potências $x$é $\{02\}$ em $GF(2^8)$.

(incrementar)(melhor relacionar)

#### 2.2.7.3 Decodificação do AES

O mesmo processo descrito anteriormente para codificação pode ser usado para a decodificação usando seus processos inversos denominados respectivamente como Invshiftrows(), Invsubbytes(), invmixcolumns() e o AddRoundkey().

A operação denominada Invshiftrows() é a inversa de Shiftwrows. Nesta operação os bytes das últimas três linhas da matriz de estados são deslocadas. A primeira linha não é deslocada mas somente as outras linhas. A equação de transformação é definida como:

$$S'_{r,(c+deslocamento(r,NB))mod(Nb)} = S_{r,c} \text{sendo que } 0<\text{r}<4 \text{ e } 0 \leq c \leq Nb$$

Este processo é melhor demonstrado nos diagramas a seguir.

S

| | | | |
|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ |
| $S_{1,0}$ | $S_{1,1}$ | $S_{1,2}$ | $S_{1,3}$ |
| $S_{2,0}$ | $S_{2,1}$ | $S_{2,2}$ | $S_{2,3}$ |
| $S_{3,0}$ | $S_{3,1}$ | $S_{3,2}$ | $S_{3,3}$ |

$\Rightarrow$

$S'$

| | | | |
|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ |
| $S_{1,3}$ | $S_{1,0}$ | $S_{1,1}$ | $S_{1,2}$ |
| $S_{2,2}$ | $S_{2,3}$ | $S_{2,0}$ | $S_{2,1}$ |
| $S_{3,1}$ | $S_{3,2}$ | $S_{3,3}$ | $S_{3,0}$ |

Após esta transformação, é feita a operação Invsubbytes() a qual é a inversão da operação SubBytes, usando-se a multiplicativa inversa de GF($2^8$).

A operação de Invmixcolumns() é uma operação que executa transformações na matriz de estados de colunas a colunas, considerando que cada coluna é definida por um polinômio de quatro termos. As colunas são tratadas como polinômios definidos por $GF(2^8)$multiplicadas pelo módulo $x^4 + 1$ através de um polinômio $a^{-1}(x)$definido por:

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\} \tag{33}$$

Na definição da forma matricial de : $S'(x) = a^{-1}(x) \otimes s(x)$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \text{sendo que } 0 \leq \text{c} \leq \text{Nb}$$

Depois desta multiplicação os bytes das quatro colunas são substituídos pelas seguintes equações:

$$S'_{0,c} = (\{0e\} \bullet S_{0,c}) \oplus (\{0b\} \bullet S_{1,c}) \oplus (\{0d\} \bullet S_{2,c}) \oplus (\{09\} \bullet S_{3,c}) \quad (34)$$

$$S'_{1,c} = (\{09\} \bullet S_{0,c}) \oplus (\{0e\} \bullet S_{1,c}) \oplus (\{0b\} \bullet S_{2,c}) \oplus (\{0d\} \bullet S_{3,c}) \quad (35)$$

$$S'_{2,c} = (\{0d\} \bullet S_{0,c}) \oplus (\{09\} \bullet S_{1,c}) \oplus (\{0e\} \bullet S_{2,c}) \oplus (\{0b\} \bullet S_{3,c}) \quad (36)$$

$$S'_{3,c} = (\{0b\} \bullet S_{0,c}) \oplus (\{0d\} \bullet S_{1,c}) \oplus (\{09\} \bullet S_{2,c}) \oplus (\{0e\} \bullet S_{3,c}) \quad (37)$$

Na inversão da operação AddRoundKey() é necessário somente invertê-la visto que esta operação só envolve basicamente XOR.

## 2.3 Dados Geodésicos

A topografia tem como objetivo a obtenção da planta topográfica.

O objeto de estudo, a Terra, é na realidade um geóide. Um modelo físico que representa o globo com suas deformidades.

Sendo um modelo curvo, com superfícies em elipse, existe uma dificuldade em transformar esse corpo geóide numa representação plana, com seus desníveis e diferenças de maneira proporcional, problema este se encontra na ciência de cartografia.

A esta representação se dá o nome de planta topográfica.

A planta topográfica é gerada através da projeção ortogonal de todos os pontos mapeados sobre um plano horizontal. Este plano é tangente à área

sendo representada. Ao se remover a curvatura do plano as linhas verticais se tornam paralelas e as ortogonais ficam normais dentro do plano tangente.

### 2.3.1 Sistemas de Coordenadas Geodésicas

Sendo o objeto de estudo da Topografia o geóide denominado Terra, as coordenadas que formam o Sistema Fundamental de Coordenadas são chamadas de coordenadas geodésicas.

As coordenadas geodésicas são formadas por: latitude, longitude e altitude de precisão (determinada por processos geodésicos).

O sistema brasileiro de coordenadas usado nas cartografias e mapeamentos brasileiros é o SAD-69. A diferença entre o SAD-69 dentro do perímetro de Porto Alegre é de menos de 1 segundo conforme [30].

E o Instituto Brasileiro de Geografia e Estatística (IBGE) através de uma normativa está progressivamente mudando o sistema de coordenadas brasileiro para o sistema de coordenadas da rede GPS [31].

### 2.3.2 Sistema de Coordenadas Geográficas

São denominadas coordenadas geográficas básicas a latitude e longitude. Estas duas coordenadas são de três tipos diferentes: astronômica, geodésica e natural.

A determinação das coordenadas é feita através de vários processos e projeções destinados a mitigar as deformidades do geóide Terra.

A gravidade por ser uma força mais uniforme é usada inicialmente para nivelar o eixo vertical de um teodolito, que terá seu eixo orientado na direção da gravidade. Uma linha perpendicular (horizontal) é projetada para medições dos ângulos e curvaturas.

Existe uma diferença entre a linha vertical projetada e a linha física, mas este erro é ignorado por ser de pouca diferença em aplicações mais genéricas.

Como o geóide não é uma forma geográfica uniforme, apresentando desníveis e variações na superfície, matematicamente é usada a forma elipsóide para as projeções e cálculos. Inicialmente é escolhido um ponto onde coincidam a forma elipsóide e do geóide. A partir deste pontos, são feitas duas projeções:

uma vertical perpendicular ao geóide e outra perpendicular ao elipsóide. A diferença entre as duas projeções é denominada desvio da vertical.

O ângulo formado entre a perpendicular do geóide e a projeção do plano equatorial é chamado de latitude astronômica. Latitude esta que varia de 0° (no equador) até ±90° (nos pólos).

Denomina-se latitude geodésica o ângulo formado entre a perpendicular do elipsóide e sua projeção do plano equatorial. Este cálculo é feito através de uma localidade de referência denominada *datum*.

*Datum* é um ponto escolhido na superfície de preferencialmente onde as coordenadas elipsoidais e geodésicas se encontram, e no nível do mar para facilitar os cálculos de topografia e referenciais.

A longitude astronômica tem sua medição ligada estreitamente ao conceito de fuso horário. Partindo-se do observatório astronômico de Greenwich, onde todos os meridianos deste ponto possuem longitude nula de 0°. O ângulo diedro formado através do ponto no meridiano de Greenwich e o ponto de referencia a ser medido é a longitude astronômica, e possui uma variação de 0° a ±180. Positiva para Leste e negativa para Oeste.

Para a composição da longitude geodésica é usado como referência a elipsóide como superfície de referência.

### 2.3.3 GPS

O GPS tem origem no conceito de navegação que se utiliza de sinais de rádios emitidos por satélites artificiais. Desde o lançamento do satélite SPUTNIK I, da URSS em 1957. Os cientistas perceberam que era possível através das ondas de rádios transmitidas pelo satélite determinar a sua órbita. Após descobriu-se que o inverso também era possível, ou seja, determinar a localização geográfica do receptor desde que a órbita do satélite fosse conhecida[32].

Com a evolução seguinte dos sistemas de navegação em 1973 é formado o sistema NAVSTAR-GPS, designado como NAVigation, System with Time And Ranging - Global Positioning System. A partir de então, o seu uso se expandiu tanto na área de navegação global como uso em diversas áreas como

: geografia, cartografia e geodésia.

O sistema foi construído fundamentalmente que de qualquer ponto da Terra exista no mínimo 4 satélites disponíveis para recepção e medição.

### 2.3.4 Tipos de Sistemas GPS

Existem basicamente dois tipos de Serviços que o sistema GPS fornece:

1. Standard Positioning System (SPS): disponível a todos usuários de equipamentos GPS sem nenhuma cobrança ou custo adicional, permite a precisão de até 100 metros horizontais e 156 metros verticais.

2. Precise Positioning Service (PPS): sistema mais preciso basicamente de uso militar ou permitido pelos órgãos de defesa. Sistema fechado ao uso civil. Possui uma melhor precisão sendo de 22 metros horizontais e 27,7 verticais.

Neste estudo será estudo o sistema SPS de uso mais comum e disponível.

### 2.3.5 Composição do sistema GPS

O sistema GPS é composto basicamente de três sistemas:

1. Segmento Espacial: composto pelos satélites atualmente em órbita, tem-se ao total 24 satélites operando;

2. Segmento de Controle: composto pelas estações terrestre que zelam pelo bom funcionamento dos satélites e do sistema GPS como um todo. Existem atualmente 5 estações de controle(Hawaii, Kwajalein, Ascension Island, Diego Garcia, Colorado Springs) e três antenas permanentes(Ascension Island, Diego Garcia, Kwajalein) além da estação de controle mestre ;

3. Segmento dos Usuários: segmento formado pelos usuários do sistema GPS.

### 2.3.6 Descrição dos Sinais do Sistema GPS

Os satélites fazem a transmissão em duas bandas portadoras L, nas freqüências de L1 = 1575.42 MHz e L2 = 1227.6 MHz. Além destas são modulados códigos de controle nas seguintes freqüências[33]:

Código C/A (coarse/aquisition): na faixa de 1.023 MHz com período de 1 milissegundo(ms) usado para adquirir o código de precisão.

Código de precisão: na faixa de 10.23 MHz com um período de 7 dias usado para a navegação.

Código Y ou de segurança: é usado em conjunto com o código de precisão para evitar que a comunicação sofra algum ataque no sentido de modificar o sinal.

O código C/A esta disponível somente na banda L1 enquanto que o código de precisão esta disponível nas bandas L1 e L2.

### 2.3.7 Medição e Equações de Coordenadas através de GPS

Através da recepção dos dados de quatro satélites, é possível determinar as coordenadas do receptor de GPS. Teoricamente poderia-se fazer a triangulação com somente três satélites, com mas quatro satélites é possível que se faça a sincronização dos relógios do receptor e dos satélites ,permitindo assim, a sincronia de dados e das diferenças de tempo nas transmissões dos sinais dos satélites.

Através dos dados recebidos são feitos cálculos nas chamadas pseudo-distâncias, são chamadas deste modo pelas medidas reais geométricas serem influenciadas por erros (transmissão ou sincronismo) e outras interferências da atmosfera.

Na equação de distância do sinal temos:

$$d = c.\Delta t \tag{38}$$

Onde a distância é igual a velocidade de propagação pelo tempo.

Para se calcular a pseudo-distância tem-se a seguinte equação:

$$PR_{cd} = R + c.dt_r + c.dt_a + c.dt_s + \varepsilon \tag{39}$$

ainda que:

$$R = [(XS - XR)^2 + (YS - YR)^2 + (ZS - ZR)^2]^{\frac{1}{2}} \tag{40}$$

- R: distância geométrica satélite-receptor;
- $PR_{cd}$: pseudo-distância;
- XS,YS,ZS: coordenadas do satélite;
- XR,YR,ZR: coordenadas do receptor;
- $dt_r$: diferença do relógio do receptor em relação ao do sistema GPS;
- $dt_a$ : diferença de tempo na propagação do sinal;
- $dt_s$: diferença do relógio do satélite em relação ao sistema GPS;
- $\varepsilon$: erros diversos como multi-caminho e ruídos;
- $t_r$: tempo de recepção do sinal;
- $t_t$: tempo de transmissão do sinal;
- $c$: velocidade de propagação do sinal.

Estes conjuntos de equações irão formar o posicionamento absoluto do receptor

### 2.3.8 Geóide WGS-84

Assim como os outros sistemas de coordenadas, é necessário que o sistema GPS se baseie num modelo de geóide para seus cálculos de coordenadas.

O sistema de GPS é baseado no geóide WGS-84[34], este geóide é um modelo que busca ter mais precisão e melhor se adaptar ao mapeamento por via satélite.

Este geóide define as seguintes propriedades da Terra para cálculos de posição, distância e velocidade. Na tabela 7 temos estes valores definidos:

Tabela 7: Geóide WGS-84 Parâmetros

| Parâmetro | Representação | Valor |
|---|---|---|
| Eixo principal | a | 6378137.0 metros |
| Fator de achatamento | 1/f | 298.257223563 |
| Velocidade angular da terra | $\varphi$ | 7292115.0 x $10^{-11}$ rad/s |
| Constante Gravitacional | GM | 3986004.418 x $10^8 m^3/s^2$ |

### 2.3.9 Erros do sistema GPS

Dentro do sistema de posicionamento GPS existem algumas variantes que devem ser consideradas na avaliação de sua precisão. Tem-se imprecisões intencionalmente implementadas para evitar o uso por nações inimigas ou não aliadas.

Imprecisões estas também que possam advir de variações atmosférica ou do ambiente do receptor.

#### 2.3.9.1 Erros intencionais

Para evitar que nações inimigas se utilizem do sistema GPS com muita precisão o departamento de defesa dos Estados Unidos introduziu no sinal de GPS algumas falhas que diminuem consideravelmente a precisão do receptor GPS. São basicamente duas técnicas a SA (Selective Avaliability) e a AS (anti-Spoofing).

A técnica de SA ou disponibilidade seletiva se caracteriza como uma alteração dos sinais do satélites, visando a degradação do receptor de GPS, com as seguintes formas:

- Dither ($\delta$): esta técnica se baseia na adulteração das frequências dos relógios dos satélites;

- Epsilon ($\epsilon$): esta técnica adultera as efemérides transmitidas;

A técnica AS (anti-spoofing) ou mais conhecida como anti-fraude é uma técnica que transmite um código de precisão entre as duas fases de portadora (L1 e L2). Este código resultante é criptografado e denominado de código Y.

Com estas técnicas em uso a precisão do receptor de GPS cai para 100 metros aproximadamente.

Alguns esforços têm sido feito para diminuir estas imprecisões, porém isso requer outros receptores e um maior trabalho por parte dos interessados[32].

**2.3.9.2 Erro de Nos Relógios dos Satélites** Os satélites possuem relógios de alta precisão, contudo apresentam uma deriva em relação ao tempo GPS. Esta deriva é de 1 ms e ,sistematicamente, é calculada no tempo das pseudo-distâncias.

Erro nos relógios dos receptores

Para reduzir custos os fabricantes de receptores GPS geralmente utilizam relógios menos precisos que os dos satélites. Sendo assim, o relógio do receptor apresenta algumas diferenças como a deriva dos relógios dos satélites. Desta forma, os receptores ao mapearem quatro satélites fazem um ajustamento destas imperfeições diminuindo a deriva do receptor.

Interferência da Ionosfera e da Troposfera

Ao transmitirem os sinais GPS, os satélites enviam sinais que atravessam a ionosfera e a troposfera.

A ionosfera possui aproximadamente uma espessura de 200 km e se encontra mais distante da superfície. Enquanto que a troposfera que possui uma espessura de 50 km se encontra bem mais próxima da atmosfera.

Estas duas camadas são percorridas pelos sinais vindos dos Satélites GPS, causando distorções e retardamentos dos sinais, criando assim, distorções que possam se encontrar na faixa de erro de 1m a 100 metros.

Para minimizar este efeito alguns receptores GPS se utilizam das duas bandas de Transmissão a L1 e L2. Através de uma modelagem linear entre as duas o efeito das atmosferas é reduzido, gerando uma maior precisão.

**2.3.9.3 Efeito Multi-caminho** O efeito multi-caminho ocorre principalmente quando o sinal, antes de chegar a estação ou receptor GPS reflete em alguma superfície ou obstáculo. Ao mesmo tempo recebe um sinal diretamente, tendo assim uma recepção de sinais por caminhos diferentes.

Estes sinais acabam se sobrepondo e causando distorções nas leituras e cálculos das pseudo-distâncias.

Recomenda-se nestes casos a melhor escolha da posição da antena receptora, para o recebimento de um sinal, sem interferências de reflexão de sinal[32].

# 3 Proposta

A proposta desta dissertação é a de promover a junção de duas tecnologias sistemas de coordenadas geodésicas e criptografia.

Para as coordenadas geodésicas será usado o sistema de GPS, por ser um sistema de baixo custo, ampla aceitação e de relativa precisão para usos civis.

Na área de criptografia poder-se ia usar tanto sistemas assimétricos (RSA) quanto simétricos (AES). Optou-se utilizar o AES por ser um algoritmo que tem uma ótima portabilidade, desempenho e ,além disso, não possui nenhuma patente ou royalties sendo de domínio público[11, 4].

Através uma infra-estrutura de um servidor acoplado a um sistema GPS em conjunto com criptografia AES será criado uma nova forma de comunicação que utilizará as duas tecnologias.

Esta interação será através dos seguintes componentes: receptor GPS, servidor criptográfico, estação receptora e satélite.

No figura 2 abaixo é mostrada esta comunicação e seus componentes.

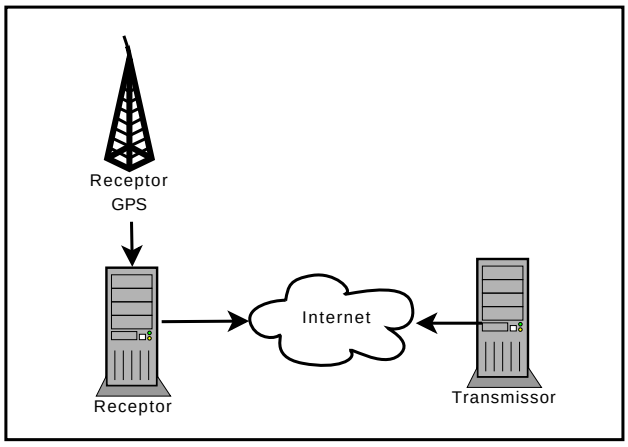


Figura 2: Componentes do Sistema

Este modelo ira funcionar na camada de dados da seguinte forma: através dos dados captados pelo receptor GPS o sistema criptográfico ira utilizar da criptografia AES para se comunicar utilizando em conjunto os dados do GPS para a criação da chave. Com isso teremos uma chave baseada nos dados do receptor GPS.

Dentro dos dados do GPS poderão ser utilizados: coordenadas geográficas, altitude e hora. Enquanto que o sistema de criptografia utilizará estes dados para compor uma comunicação segura.

Com isto será possível fazer com que o receptor e transmissor da mensagem somente consigam se comunicar através de alguma condição imposta pelo sistema podendo esta ser: hora, localidade, altura ou até mesmo velocidade.

Seu uso será o desde restringir a comunicação entre duas partes através da hora, localidade, velocidade ou altura ou a combinação destas variáveis.

Uma aplicação desta poderia ser com o transporte de cargas perigosas, utilizando este sistema um caminhão ou qualquer meio de transporte neste contexto poderia somente receber instruções para as próximas cargas ou destinos quando estivesse em determinado ponto de sua trajetória, evitando assim que o motorista utilizasse alguma rota não estabelecida ou então não fizesse as paradas necessárias em pontos estratégicos.

No campo militar poderá ser muito bem empregada esta tecnologia, por exemplo, enviando um grupo de soldados para uma área e os soldados só receberiam o resto das ordens no momento que estivessem naquela área, evitando assim que as ordens ou comunicados sejam utilizados previamente ou então fora do seu local pretendido.

## 3.1 Característica do Sistema Proposto

No sistema proposto será usado um receptor GPS para coleta de dados geográficos, estes dados serão usados para compor a chave de criptografia. Depois a mensagem ou comando será enviada por uma conexão segura para o receptor.

O protocolo de comunicação do receptor GPS será o padrão NMEA[35] onde no caso todas as mensagens são compostas de strings começando com $ neste caso estamos interessados nas mensagens com a identificação GPGGA que é descrita como "GPS Fixed data" ou dados de localização do GPS.

O formato desta sentença é:

$GPGGA,hhmmss.ss,ddmm.mmmm,n,

dddmm.mmmm,e,q,ss,y.y,a.a,z,g.g,z,t.t,iii*CC
Onde:

- hhmmss.ss: Horário no formato Universal;
- ddmm.mmmm,N: Latitude do GPS;
- dddmm.mmmm,W: Longitude do GPS;
- q: qualidade do sinal GPS;
- ss: número de satélites sendo usados;
- y.y: diluição horizontal da precisão;
- a.a,M: altitude da antena de GPS em metros;
- g.g,M: separação geodal em metros;
- t.t: idade de referencia dos dados de correção;
- iiii: ID da estação de referência;
- *CC: checksum da string

Nesta aplicação será usada a longitude, latitude, hora e minutos. Sendo assim a encriptação somente poderá ocorrer quando estes três dados estiverem corretos.

Na figura 3 é demonstrado o fluxo de dados para a criptografia da mensagem. Tem-se o algoritmo de criptografia recebendo os dados e coordenadas do GPS. Este atua em conjunto com uma semente pré-definida entre as partes, utiliza-se desta informação para codificar a mensagem.

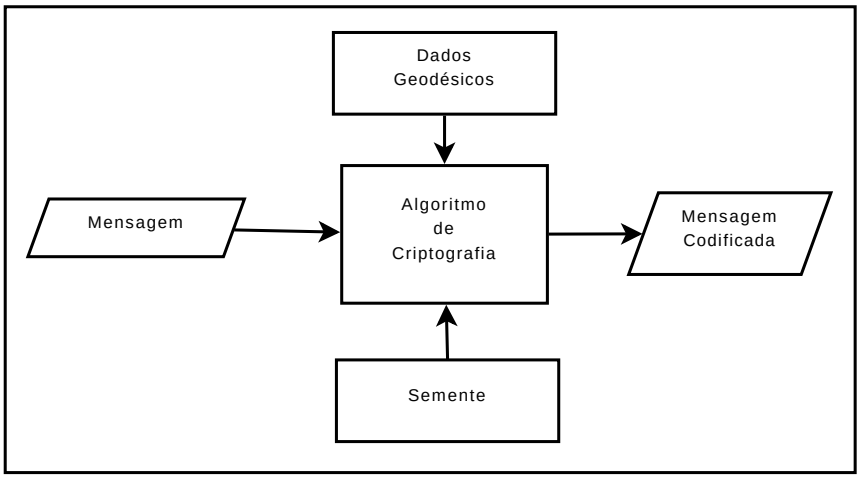


Figura 3: Fluxo da Mensagem Sendo Codificada

Sendo assim este protótipo irá se comunicar de forma segura, utilizando uma semente pré-definida e dados geodésicos como forma de restrição ou de funcionamento do receptor.

Criando assim novos requirimentos de autenticação como posição, hora ou velocidade.

O receptor irá se conectar através da internet ou qualquer rede de dados, através de um protocolo específico e vai receber do transmissor um pacote de dados, através de sua programação interna e os dados geodésicos recebidos do receptor GPS, este irá proceder para a decodificação do pacote.

Na decodificação do pacote de dados ele usará a semente pré-definida em conjunto com os dados geodésicos para decodificar o pacote de mensagem.

Caso esteja nas coordenadas corretas conseguirá decodificar com sucesso o pacote e mensagem ou comando interno, caso não irá decodificar somente dados espúrios.

Na figura 4 é demonstrada a recepção de decodificação do pacote de mensagem criptografada.

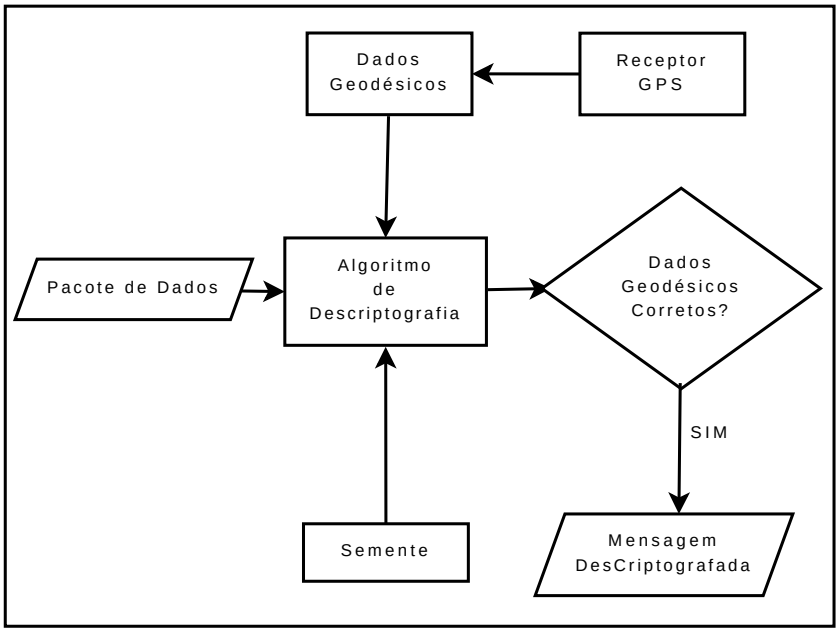


Figura 4: Diagrama da Decodificação

Conforme demonstrado, o pacote de dados é recebido pelo receptor. Os dados geodésicos são provenientes do receptor GPS. Após os dados geodésicos em conjunto com a semente randômica e o algoritmo de criptografia (AES) decodificam o pacote.

Caso os dados geodésicos e a semente randômica estejam corretos a mensagem é decodificada, caso contrário é decodificado somente dados espúrios.

# 4 Metodologia

Neste capítulo serão demonstradas as metodologias utilizadas para a implementação e testes realizados do sistema proposto. Assim também como as ferramentas, softwares e hardwares utilizados

## 4.1 Plataforma de Desenvolvimento

O sistema proposto foi desenvolvido em um servidor FreeBSD, localizado em um data Centre dos E.U.A.

A escolha de um servidor FreeBSD teve como principais motivos o baixo custo do sistema operacional, aliado a sua estabilidade e licenciamento liberal.

Foi desenhada uma interface em HTML para maior compatibilidade e facilidade de operação. Em conjunto foram utilizadas APIs do Google Maps para melhor visualização da estação receptora.

O centro do sistema foi desenvolvido em Python (versão 2.5) com bibliotecas de Criptografia OpenSSL[36].

A grande vantagem desta composição é que a camada de controle em linguagem Python oferece uma grande flexibilidade e rapidez na prototipagem. Enquanto que a biblioteca OpenSSL é reconhecida mundialmente por sua robustez e utilizada em grandes projetos. Inclusive é certificada pelo governo dos Estados Unidos da América[37]. Além disso, a biblioteca OpenSSL possui um licenciamento bem mais liberal, permitindo inclusive o uso comercial de seus softwares.

### 4.1.1 Sistema Receptor de GPS

Para este trabalho foi adquirido um receptor GPS da marca Holux modelo GR-213.

Este receptor tem uma interface USB de comunicação e possui as seguintes características:

- Capacidade de monitorar até 20 satélites;
- Recepção nas bandas L1, C/A;

- Antena interna;
- Precisão de 5 a 25 metros;
- Formato dos dados: NMEA 2.2

Na figura 4.1.1 é mostrado uma foto ilustrativa deste receptor, o qual possui dimensões pequenas e é bem prático para testes de campo.


Figura 5: Receptor GPS GR-213

Este receptor além de possuir a vantagem de ser pequeno e prático, possui um imã na sua capa inferior permitindo assim uma fixação em bases metálicas.

## 4.2 Fases de Desenvolvimento

No desenvolvimento do sistema proposto, o sistema foi desenvolvido progressivamente em três fases distintas:

- Fase de modelagem: fase de planejamento e levantamento de requisitos;
- Fase de prototipagem: nesta fase foi feito o protótipo do sistema;
- Fase de teste de campo: testes de campos foram realizados para verificação do sistema.

### 4.2.1 Fase de Modelagem

Esta foi a fase que considera-se o embrião do sistema proposto.

A modelagem de funcionamento, componentes e processos foram executados nesta fase.

Durante estas fases vários pontos foram mapeados e desenhados como por exemplo:

- Linguagem de programação: após alguns testes, para maior flexibilidade foi usado um modelo hibrido de programação, utilizando-se linguagens padrão como C , Python e HTML;
- Modelagem do processo de criptografia: modelagem dos dados, formatação, uso dos dados, interpretação dos dados;
- Modelagem do processo de comunicação: foram desenvolvidos processos de como o receptor e transmissor irão se comunicar, formas que essa comunicação ocorrerá e outros detalhes de processos de comunicação;
- Recepção e decodificação dos dados: modelagem de como o receptor irá tratar o pacote de dados recebidos, como ele irá proceder para decodificar e o que ele irá fazer com os dados decodificados com sucesso ou não;
- Dados geodésicos: definição de quais dados geodésicos serão usados e como serão interpretados.

Esta fase se caracterizou-se principalmente pelo desenho e lógica do sistema proposto, sendo um exercício importante para se evitar algum re-trabalho nas sucessivas fases e também para se maximizar o resultado final.

### 4.2.2 Fase de Prototipagem

Depois de feita a modelagem, iniciou-se a fase de prototipagem.

Nesta fase foi adquirido um receptor GPS para melhor prototipagem e para maior realidade do protótipo.

A interface de entrada de dados no transmissor foi modelada, com os requisitos de ser rápida e simples.

Foram feitos testes de recepção do GPS, comunicação do receptor GPS com o sistema proposto.

O sistema como um todo foi prototipado para funcionar numa situação real.

### 4.2.3 Fase de Teste de Campo

Esta fase foi caracterizada com extensivo testes de campo, medições e averiguações do sistema proposto.

Os testes de campo tiveram como objetivo principal, verificar o funcionamento e desempenho do sistema proposto numa situação real.

Foram feitas medições de campo, para averiguações do receptor GPS, de suas coordenadas e dos efeitos do ambiente nas coordenadas recebidas pelo receptor GPS.

A importância desta fase foi a de mapear possíveis problemas ou características que possam interferir no funcionamento do sistema proposto.

## 4.3 Descrição do Sistema

O objetivo desta seção é a de descrever o sistema proposto, com seus componentes, módulos e métodos.

Uma descrição do protocolo de comunicação, sessões e lógica também foram feitas para melhor detalhamento do sistema proposto.

### 4.3.1 Componentes do Sistema

O sistema é formado por basicamente quatro componentes:

- O transmissor de dados: aqui neste caso um servidor remoto;
- Chave de criptografia: baseada em dados geodésicos e randômicos;
- Receptor dos dados: a parte interessada em receber os dados;

- Protocolo de comunicação: camada de comunicação que permite a troca de dados de forma sigilosa e conforme os dados geodésicos.

O sistema utiliza como entrada para a criação da chave duas fontes de informações:

- Semente randômica pré-estabelecida entre as duas partes;
- Dados Geodésicos do leitor de GPS;

### 4.3.2 Transmissão de Dados

O transmissor dos dados é considerado o servidor Remoto, onde foi utilizado um servidor FreeBSD para tal tarefa. Neste servidor roda um serviço que recebe as requisições por sockets e transmite os dados com os parâmetros geodésicos inclusos.

Foi desenvolvida uma interface WEB para a inserção dos parâmetros geodésicos desejados, interface WEB acessada por método seguro (SSL).

A partir dos dados informados, a configuração é gravada e por conseguinte o transmissor transmite os dados criptografados utilizando o método de criptografia AES de 256 bits.

No processo de criação da chave, é utilizada uma semente, e uma forma de compor a chave a qual utiliza o seguinte método:

$$chave = R(semente) + dados(geodesicos) \tag{41}$$

Neste caso a chave é uma composição dos dados geográficos. A semente randômica e mais um processo interno de transformação destes dados, provendo assim uma maior confiabilidade. Isso evita algum ataque estatístico, ou até mesmo determinístico a partir do conhecimento das coordenadas.

Através da interface WEB e de um sistema em HTML as coordenadas geodésicas usadas para a codificação são digitadas e a mensagem ou comando também. Isso é melhor demonstrado na figura 6.


Figura 6: Tela de Entrada de Dados Do Transmissor

Após o acionamento do botão enviar comando o servidor abre uma porta de comunicação TCP e aguarda que o receptor entre em contato para que transmissor envie o pacote de dados.

O receptor ao se conectar e executar uma primeira transação de forma correta transforma a tela de entrada de dados, com um mapa da posição sendo utilizada. Nesta funcionalidade foi feito uso do sistema de mapeamento do Google, conhecido como Google Maps. Na figura 4.3.2 é demonstrado essa funcionalidade.


Figura 7: Conexão Estabelecida no Transmissor

### 4.3.3 Receptor de Dados

A recepção de dados é realizada em qualquer micro que tenha capacidade para rodar o aplicativo cliente desenvolvido em Python. No nosso caso foi usado um laptop rodando o sistema operacional Windows XP, com 1 GB de RAM e velocidade de clock de 2.7 GHZ

Na figura 8 é demonstrada a estação de testes usada no desenvolvimento do sistema proposto.


Figura 8: Estação Receptora

O receptor GPS é acoplado a porta USB após 42 segundos em média de estabilização, este é o tempo necessário para que ele possa receber os dados dos satélites. Após começa a transmitir ao Desktop através da porta USB os dados do receptor para o sistema.

O programa cliente, recebe esses dados, escolhe os campos necessários da sentença no padrão NMEA[35].

No nosso modelo, o programa recebe os dados de: latitude, longitude, hora, altura e velocidade.

Para transmissão e recepção dos pacotes foi utilizada a rede Wifi disponível na área.

Conforme o protocolo de comunicação requer os dados são usados ou não no processo de criação da chave.

### 4.3.4 Protocolo de Comunicação

Para que o transmissor e receptor funcionem adequadamente e de forma dinâmica foi necessário uma implementação de um protocolo de comunicação entre as duas partes.

Neste caso foi desenvolvido um protocolo que utiliza os seguintes componentes:

- Sessão Inicial: sessão inicial para conformidade da semente randômica;
- Sessão de configuração: neste sessão são enviados os requisitos e dados que deverão ser usados na transmissão de dados;
- Transmissão de dados: nesta sessão os dados são transmitidos;
- Manutenção de conexão: nesta sessão o receptor e transmissor se mandam pacotes simples, demonstrando estarem ativos.
- Finalização da seção: encerramento e conclusão de toda a comunicação.

Devido ao receptor transmitir as informações somente de segundo a segundo, as transmissões neste modelo serão feitas também de segundo a segundo. Isso não impede que em outros modelos de receptor este tempo de transmissão seja menor.

### 4.3.5 Inicialização do Protocolo

Na inicialização do protocolo de comunicação, ocorrem as principais definições e dados ao qual as futuras comunicações serão feitas.

Esta é a inicial e são enviados os seguintes dados:

1. Tipo de pacote: mensagem, comando, configuração;
2. Tamanho da chave;
3. Numero seqüencial;
4. Semente;

5. Tamanho em bytes do pacote;

Este pacote usa uma formatação interna para maior controle e e segurança.

Dentro do pacote de dados são enviado quais dados geodésicos serão utilizados e no final um número seqüencial de controle.

Exemplo de pacote:

| | | | | |
|---|---|---|---|---|
| Conf | 256 | 0 | xxxxxx | 16 |

Neste caso o pacote informa que uma mensagem de configuração esta sendo efetuada, indicando o uso de uma chave de 256 bits, na seqüência 0 e com a semente em conjunto.

### 4.3.6 Sessão de Configuração

Nesta sessão de dados o transmissor informa dentro do padrão previamente acertado os dados necessários para a comunicação entre as duas partes. Igualmente é transmitida a chave, os dados geodésicos utilizados e o número seqüencial de controle.

Nesta sessão o receptor se prepara para receber os dados utilizando a semente pré-estabelecida e os dados geodésicos estabelecidos. A semente previamente recebida será usada no processo de criptografia e descriptografia da mensagem.

### 4.3.7 Transmissão dos Dados

Na transmissão de dados o transmissor envia pacote e aplica o processo de criptografia. Neste caso ele faz o processo de criação de chave conforme descrito na equação abaixo:

$$Chave = G(semente) + processo + dados(geodesicos) \tag{42}$$

Logo após esta chave é usada para transmitir os dados, a estação receptora usará seus dados geodésicos para decodificar a mensagem, somente

funcionando caso ela tenha os dados geodésicos corretos.

Importante notar que a semente já foi previamente definida e será usada para compor a chave, em conjunto com os dados geodésicos.

O tamanho total de todos os pacotes transmitidos são definidos pelo tamanho do bloco do padrão AES de 128 bits.

### 4.3.8 Recepção dos dados

Neste processo o pacote de dados é recebido e devidamente decodificado.

A estação através da semente pré-estabelecida, tenta decodificar a mensagem com os dados geodésicos recebidos através do modulo receptor de dados GPS, processo demonstrado na figura 4 .

Neste momento é feito o processo inverso para decodificação da mensagem, utilizando-se do processo inverso que o transmissor usou para criar a chave de criptografia.

Caso não tenha sucesso a estação receptora não poderá decodificar a mensagem.

### 4.3.9 Manutenção e Finalização de Sessão

Dentro da Manutenção é feito somente um ping no servidor para checagem dele e do receptor. Neste caso o transmissor manda um comando de ping e o receptor devolve este comando demonstrando que ele esta comunicável.

A sessão de manutenção é importante para se manter as configurações correntes, e caso haja alguma mudança de parâmetro. Ex.: mudanças dos dados geodésicos de decodificação. Estes possam ser decodificados de acordo.

Após a transmissão de todos os dados é feita a sessão de finalização que interrompe todas as conexões e encerra os processos.

# 5 Resultados

Neste capítulo são demonstrados os resultados obtidos em testes de campo do sistema proposto.

## 5.1 Precisão do Receptor GPS

Como o receptor de GPS usado é de baixo custo, é importante limitarmos o seu limite de precisão e volatilidade em uso.

Para isso foram desenhados três cenários:

1. Estação Fixa em área urbana e rural;
2. Estação móvel em área urbana ;
3. Estação em área urbana reflexiva;

Dentro destes três cenários foram feitas medições, e coletados dados durante uma hora. A partir dos dados coletados estes mesmos foram analisados estatisticamente conforme tabela 8.

Tabela 8: Medição dos dados GPS

| | Lat. Média | Lon. Média | Var. Lat | Var. Lon |
|---|---|---|---|---|
| Área urbana reflexiva | 30° 01' 11" | 51° 10' 32" | 0° 00' 0.44" | 0° 00' 0,31" |
| Área urbana fixa | 30° 01' 41" | 51° 13' 42" | 0° 00' 0.15" | 0° 00' 0,13" |
| Área Rural Fixa | 30° 03' 25" | 51° 13' 47" | 0° 00' 0.05" | 0° 00' 0,13" |
| Área urbana Móvel | 30° 03' 27" | 51° 13' 48" | 0° 05' 0.57" | 0° 02' 32" |

Estes dados nos servem para medirmos a precisão do sistema e qual a margem de erro que se deve usar para evitar que o sistema se comunique com dificuldade. Sendo assim as seguintes considerações foram feitas nos seguintes cenários:

- Área urbana Reflexiva: nesta medição tentou-se simular erros de multi-caminho, interferências e avaliar qual a sua influência nas medições. A medição foi feita entre construções residenciais altas e de grande densidade. Nota-se que a maior diferença entre as medições máximas e

mínimas ocorreu justamente neste cenário, refletindo assim uma interferências do meio urbano nas medições;

- Área Urbana fixa: neste cenário foi escolhida o Marco Zero da cidade de Porto Alegre, a Prefeitura de Porta Alegre, . Mesmo sendo uma área de grande concentração de construções, a medição apresentou pouca variação entre a medição mínima e máxima das coordenadas;

- Área Rural Fixa: Neste caso foi feita a medição numa área com pouca densidade habitacional, poucas construções e com visibilidade para os horizontes. Esta foi a medição que obteve os menores índices de variação entre as máximas e mínimas medidas de coordenadas;

- Área urbana móvel: Neste cenário foi escolhida uma área de pouco fluxo, poucas habitações, e em conjunto com um automóvel foram feitas medições utilizando-se um percurso quadrangular. Este foi o cenário que demostrou maior diferença entre as medidas, devido a justamente o receptor estar em movimento.

Fazendo uma análise destes números pode-se chegar a algumas conclusões. Mesmo numa área urbana reflexiva a variação das leituras de coordenada não ultrapassou 1".

### 5.1.1 Precisão do receptor GPS frente a coordenadas cartográficas

Neste teste foi escolhida um ponto da cidade de Porto Alegre, conhecido como Marco Zero. Este ponto se encontra em frente à prefeitura Municipal de Porto Alegre em fronte a fonte Talavera de La Reina.

No marco existe um obelisco com as inscrições Lat. 30° 01' 39" e Long. 51° 13' 40" a medição do aparelho GPS deram as seguintes coordenadas Lat. 30° 01' 40" e Long. 51° 13' 41". Na tabela 9 estas diferenças são melhor demonstrada

Tabela 9: Diferença de Medição GPS e Marco Zero

| | Latitude | Longitude |
|---|---|---|
| GPS | 30° 01' 40" | 51° 13' 41" |
| Marco Zero | 30° 01' 39" | 51° 13' 40" |
| Diferença | 01" | 01" |

Uma aproximação que se pode fazer é que o geóide WGS-84 possui em seu eixo equatorial 6,378,137.0 metros o que em graus, minutos e segundos é equacionado como:

$$\frac{6,378,137.0}{60} = 106302.283m/ \tag{43}$$

$$\frac{106302.283}{60} = 1771.704m/minuto \tag{44}$$

que resulta em

$$\frac{1771.7047}{60} = 29,52m/segundo \tag{45}$$

Com isso a medição do GPS frente ao marco zero, possui um precisão de aproximadamente 29,52 metros ou de 1".

Devida a essa diferença no sistema de transmissão de dados criptografados foram retirados os segundos para minimizar qualquer erro e ou interferência na leitura das coordenadas.

Ao tirarmos os segundos estaremos tendo uma precisão de aproximadamente 1,7 km.

## 5.2 Testes de transmissão de dados criptografados

Para testar-se o sistema proposto foi utilizado cenários que pudessem mostrar as qualidades do sistema, e que fossem relevantes.

Dentro das possibilidades foram realizados testes com as seguintes restrições e capacidades:

- Transmissão e decodificação com localização fixa;

- Transmissão e decodificação com localização em uma área;

- Uso de Altura e hora como restrição de transmissão e recepção;

Através destas características foram utilizados cenários e testes para testar a robustez do sistema.

## 5.3 Resultado de Transmissão e Decodificação Com Localização Fixa

Neste caso uma localidade foi mapeada e suas coordenadas foram inseridas no sistema de criptografia.

No módulo transmissor, foram configuradas as coordenadas do módulo receptor e ativada a transmissão.

O módulo receptor ficou em um ciclo repetitivo tentando receber os dados do servidor transmissor e contando as tentativas com sucesso ou fracasso durante uma hora.

Tabela 10: Resultado Com Localização Fixa

| Sucesso | Falha | Pacotes transmitidos |
|---|---|---|
| 3600 | 0 | 3600 |

Este cenário se mostrou com grande confiabilidade, atingindo numa rodada de 3600 tentativas 100% de sucesso.

## 5.4 Resultado De Transmissão E Decodificação Com Localização Em Uma Área Delimitada

Neste cenário foi demarcado uma área de forma poligonal para facilitar a demarcação da área onde a transmissão e recepção de dados possa ocorrer.

No figura 9 são é demonstrados os pontos marcados.

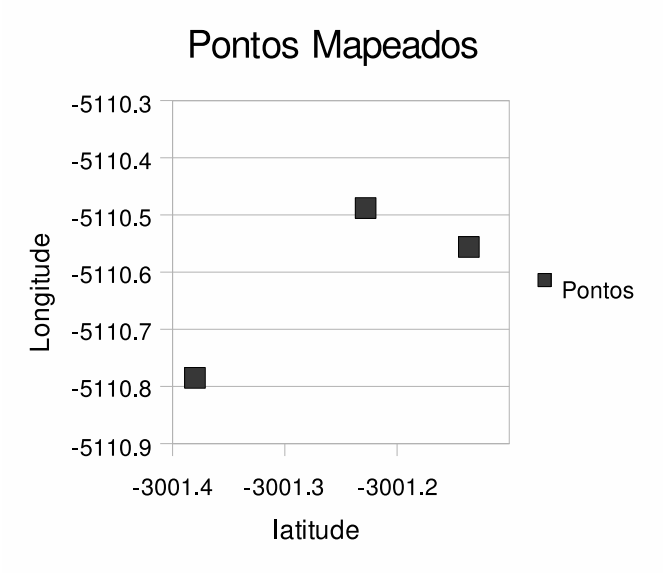


Figura 9: Pontos Mapeados

É necessário no minimo três pontos para se definir uma área a ser mapeada. Neste caso a transformação dos pontos em uma área a ser mapeada foi feita de através dos usos das máximas e mínimas coordenadas, conforme tabela 11.

Tabela 11: Coordenadas Mapeadas

| | Ponto-1 | Ponto-2 | Ponto-3 |
|---|---|---|---|
| Latitude | -3001.23 | -3001.38 | -3001.14 |
| Longitude | -5110.49 | -5110.79 | -5110.56 |
| Max. Lat | - | - | -3001.14 |
| Max. Long. | -5110.49 | - | - |
| Min. Lat | - | -3001.38 | - |
| Min. Long | - | -5110.79 | - |

Por se tratar de um ambiente urbano estas coordenadas máximas e mínimas fora usadas como variáveis no sistema de transmissão de dados criptografados.

O resultado disso foi uma área "quadrada" ao qual com grande margem de segurança a comunicação possa ser estabelecida.

Na figura 10é demonstrada esta área.

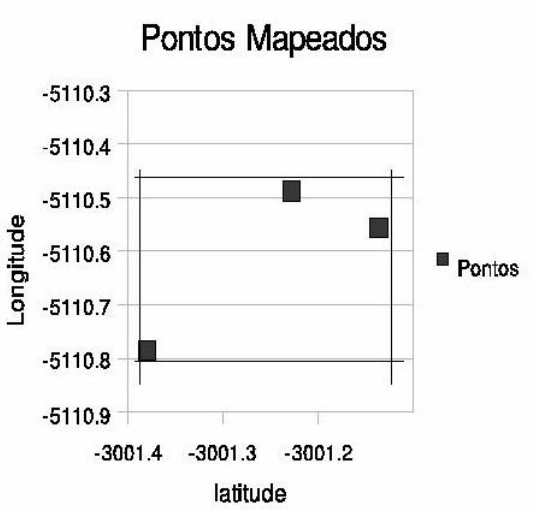


Figura 10: Área utilizando-se as máximas e mínimas coordenadas

Foram feitos testes de transmissão e recepção novamente num período de uma hora, mas neste caso foram feitas transmissões de dados dentro da área limitada pelas coordenadas máximas e mínimas.

Os resultados são demonstrados na tabela 12.

Tabela 12: Resultado Com Área Delimitada

| Sucesso | Falha | Total |
|---|---|---|
| 3600 | 0 | 3600 |

Não houve nenhuma falha de comunicação neste cenário de uso.

## 5.5 Resultado de Transmissão e Decodificação Numa Altura Determinada

Neste cenário, a altura foi usada como fator de codificação. Desta forma somente com o receptor numa altura determinada poderia ocorrer a recepção correta dos dados.

Neste caso o sistema foi programado para transmitir somente a uma altura de 20 a 25 metros do solo.

Durante uma hora, foram transmitidos os pacotes e foram obtidos os seguintes resultados.

Tabela 13: Resultado Com uso de Altura

| Sucesso | Falha | Total |
|---|---|---|
| 3537 | 63 | 3600 |

Importante notar-se que na tabela 5.5 apresentaram-se alguns pacotes com falha devido a mudança de um andar para outro para testes de recepção. Provavelmente devido a interferências da estrutura metálica (elevador). Neste caso também o sistema se provou de grande confiabilidade e praticidade.

# 6 Conclusão

Com base no trabalho desenvolvido, foram descritas as principais aplicações do sistema de criptografia com dados geodésicos.

Na fundamentação teórica foram descritas as principais tecnologias de criptografia, GPS e algumas fundamentações matemáticas para melhor acompanhamento do trabalho.

Depois na proposta do sistema foram delineados os principais pontos deste trabalho, como o funcionamento do sistema de criptografia com dados geodésicos, e algumas considerações de uso e modelagem do sistema propriamente dito.

A metodologia aplicada demonstra como o sistema proposto foi implementado e seus componentes.

Os resultados deste estudo foram obtidos através dos testes executados a campo para averiguação e aperfeiçoamento do sistema.

A partir dos dados demonstrados na tabela 3 foi escolhido o algoritmo AES por oferecer um ótimo nível de segurança, e em conjunto com a desempenho demonstrada nas tabelas 4 e 5.

Para melhor refletir a realidade, foram feitos testes de campos que primeiramente definiram a precisão do próprio leitor de GPS frente a si mesmo a a fatores atmosféricos conforme a tabela 10 . Inclusive medições foram feitos em pontos estratégicos como o marco zero de porto alegre conforme a tabela 9 .

Estas comparações e medições serviram de base para as medições do sistema proposto idealizado nos cenários conforme descrito na seção 6.2 da parte de resultados. Mesmo tendo o sistema uma precisão média de 29 metros, foi definida a não utilização dos segundos, diminuindo a precisão para 1700 metros aproximadamente. Com isso obteve-se uma margem de segurança nas medidas geodésicas para seu uso em territórios urbanos evitando qualquer distorção ou erro de multi-caminho

Conforme o cenário demonstrado pela tabela 11 fica demonstrado que o sistema tem uma robustez e capacidade de prover uma criptografia baseada em coordenadas geodésicas, bastando para isso um ajuste da precisão e/ou

compra de um receptor GPS mais preciso.

Para a grande maioria das aplicações mesmo uma precisão de 1,7 Km alcançados com o dispositivo de baixo custo usado e o sistema proposto poderão ter imensas possibilidades.

Os objetivos propostos deste trabalho foram atingidos, através deste trabalho foi criado um sistema de criptografia com dados geodésicos, permitindo novas aplicações e inovações nas áreas de segurança e tecnologia.

Na área de entretenimento poder-se-á ter a regionalização de sistemas de vídeo ou filmes baseada numa realidade geográfica ao invés de mercado. O usuário ao entrar em uma outra região poderia usar os filmes abertos para aquela região de forma transparente. Da mesma forma que custos seriam baixados, pois o tocador da mídia ter-ia em seu interior um receptor GPS com o sistema proposto para decodificar as zonas corretas. Caso não tivesse na zona correta não iria conseguir decodificar as funcionalidades da zona correta.Uso deste modelo poderia ser em DVDs e filmes aonde os estúdios de cinema, possuem táticas de mercado e marketing diferentes para cada região.

No transporte de cargas seria possível obrigar um motorista a seguir uma pré-determinada rota para entrega de mercadorias, sendo que ele somente saberia do próximo destino quando estivesse em determinada coordenada. Evitando-se assim inconformidades nas rotas ou que o motorista se utilizasse de rotas não permitidas pela empresa ou seguradora de cargas.

Neste sistema proposto foi usado o AES (Rijndael) como base para criptografia, mas nada impede que sejam usados outros sistemas de criptografia como RSA, ECC e outros. Algumas modificações terão que ser feitas mas tanto a biblioteca OpenSSL quando o sistema proposto podem suportar diversos algoritmos de criptografia. A escolha do AES se deu principalmente por sua robustez, velocidade, e por ser livre de patentes ou licenças. Além de ter sido avaliado numa comissão com os principais cientistas do campo da criptografia e segurança.

## 6.1 Proposições de Estudos Futuros

Mesmo este trabalho possuindo muitos resultados práticos e um forte embasamento teórico, ainda existem muitas possibilidades que podem ser exploradas em estudos futuros, podendo serem desenvolvidas em três enfoques principais:

**Análise Entre os Diversos Algoritmos de Criptografia:**

- Comparar a desempenho do sistema proposto com outros algoritmos de criptografia;
- Analisar e comparar os requerimentos mínimos dos algoritmos;
- Análise no quesito de segurança entre os diversos algoritmos dentro deste sistema proposto.

**Desenvolvimento do Sistema Proposto em Sistemas Embarcados:**

Uma das vantagens do sistema proposto é justamente a possibilidade de se limitar as transmissões conforme as coordenadas geodésicas do receptor. Uma gama de soluções móveis podem ser desenvolvidas neste sentido. Para isso é importante que o sistema proposto seja desenvolvido em sistemas embarcados para uma maior permeabilidade da tecnologia e facilidade de uso.

# A Especificações do Receptor GPS

- Até 20 satélites
- Receptor: L1, C/A code
- Taxa máxima de atualização: 1 HZ.
- Tempo de Aquisição
  - Reaquisição 0.1segundos
  - Hot start 1 seg., média
  - Warm start 38 seg., média
  - Cold start 42 seg., média
- Precisão Posicional:
  - Non DGPS (Differential GPS)
    - Position 5-25 m CEP sem SA
    - Velocidade 0.1 m/seg, sem SA
    - Tempo 1 nano segundo GPS Time
  - EGNOS/WAAS:
    - Posicional
    - $<$ 2.2 m, horizontal 95% do tempo
    - $<$ 5 m, vertical 95% do tempo
  - Condições de Operação:
    - Altitude 18,000 metros
    - Velocidade 515 metros / segundo
    - Aceleração 4 G, max
- Tipo de antena: embutida
- Sinal mínimo: -159dBm

- Dimensões: 2.54 × 1.65 × 0.7 Inch
- Peso : < 84g
- Prova d'agua: IPX7
- Funcionamento do LED:
  - Liga e Desliga
  - Atualização das Informações
- Temperatura de Operação:
  - -40 to +80
- Temperatura de Estocagem:
  - -45 to +100
- Umidade de Operação:
  - 5% to 95% sem condensação.
- Consumo de Energia
  - < 80mA at 4.5- 5.5V
- Protocolo e interface:
- NMEA output protocol: V.2.2
- Padrão:
  - Baud rate: 4800 bps
  - Data bit: 8
  - Parity: N
  - Stop bit: 1

  - Format: GGA,GSA,GSV, RMC.

- Opcionais:

  - Baud rate: 9600,19200,38400
  - Format: GLL,VTG, ZDA, SiRF
  - binary

- Interface:

  - RS232 + CMOS TTL Level, or
  - RS-232 + DGPS

# Referências


[1] A. D. Aleksandrov, A. Kolmogorov, and M. A. Lavrentev, *Mathematics: Its content, Methodos and Meaning*. General Publishing Company, 1999.

[2] J. J. Rushanan, *A Tutorial on Finite Fields and Binary m-Sequences*. MITRE, 1996.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *HandBook of Applied Cryptography*. CRC Press, 1997.

[4] F. I. P. Standards, "Federal information processing standards publication 197," tech. rep., Federal Information Processing Standards, 2001.

[5] S. C. Coutinho, *N?meros Inteiros e criptografia RSA*. IMPA, 2000.

[6] D. Salomon, *Data Privacy and Security*. Springer, 2003.

[7] B. Schneier, *Applied Cryptography Second Edition: protocols, algorithms, and source code in C*. Katherine Schowalter, 1996.

[8] J. Buchmann, *Introduction to Cryptography*. Springer, 2001.

[9] E. English, "Network security under siege: The timing attack," *Computer*, vol. I, pp. 95–97, 1996.

[10] E. F. Foundation, *Cracking des : secrets of encryption research, wiretap politics & chip design*. O'Reilly, 1998.

[11] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, "Report on the development of the advanced encryption standard," tech. rep., National Institute of Standards and Technology, 2000.

[12] J. Kelsey, T. Kohno, and B. Schneier, "Amplified boomerang attacks against reduced-round mars and serpent," in *Fast Software Encryption Workshop*, April 2000.

[13] J. Kelsey and B. Schneier, "Mars attacks! preliminary cryptanalysis of reduced round mars variants," in *The Third AES Candidate Conference*, (Gaithersburg), pp. 169–185, National Institute of Standards and Technology, April 13-14 2000.

[14] Fast Software Encryption Workshop, *A Statistical Attack on RC6*, April 10-12 2000.

[15] Fast Software Encryption Workshop 2000, *Correlations in RC6 with a Reduced Number of Rounds*, April 10-12 2000.

[16] *AES Proposal: Rijndael*, 1999.

[17] e. a. N. Ferguson, "Improved cryptanalysis of rijndael," tech. rep., April 10-12 2000.

[18] S. Lucks, "Attacking seven rounds of rijndael under 192-bit and 256-bit keys," vol. I, (Gaithersburg), pp. 215–229, Institute of Standards and Technology, April 13-14 2000.

[19] H. Gilbert and M. Minier, "A collision attack on 7 rounds of rijndael," in *The Third AES Candidate Conference*, pp. 230–241, National Institute of Standards and Technology, April 2000.

[20] T. Kohno, J. Kelsey, and B. Schneier, "Preliminary cryptanalysis of reduced round serpent," in *The Third AES Candidate Conference*, (Gaithersburg), pp. 195–214, National Institute of Standards and Technology, April 2000.

[21] N. Ferguson, "Twofish technical report 5: Impossible differentials in twofish," tech. rep., AES Round 2 public comment, October 1999.

[22] N. Ferguson, "Twofish technical report 6: A twofish retreat: Related-key attacks against reduced-round twofish," Tech. Rep. 6, AES Round 2 public comment, February 2000.

[23] B. Schneiner, T. Kohno, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, and M. Stay, "The twofish teams final comments on aes selecion," tech. rep., May 2000.

[24] R. Rivest, M. Robshaw, and Y. Yin, "Rc6 the elegant aes choice," in *Third AES Candidate Conference*, April 2000. submitter presentation.

[25] C. Parikh and P. Patel, "Performance evaluation of aes algorithm on various development platforms," in *Consumer Electronics, 2007. ISCE 2007. IEEE International Symposium on*, pp. 1–6, 20-23 June 2007.

[26] G. Zhou, H. Michalik, and L. Hinsenkamp, "Efficient and high-throughput implementations of aes-gcm on fpgas," in *Field-Programmable Technology, 2007. ICFPT 2007. International Conference on*, pp. 185–192, 12-14 Dec. 2007.

[27] M. Liberatori, F. Otero, J. Bonadero, and J. Castineira, "Aes-128 cipher. high speed, low cost fpga implementation," in *Programmable Logic, 2007. SPL '07. 2007 3rd Southern Conference on*, pp. 195–198, 28-26 Feb. 2007.

[28] C. Sivakumar and A. Velmurugan, "High speed vlsi design ccmp aes cipher for wlan (ieee 802.11i)," in *Signal Processing, Communications and Networking, 2007. ICSCN '07. International Conference on*, pp. 398–403, 22-24 Feb. 2007.

[29] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved cryptanalysis of rijndael," *Seventh Fast Software Encryption Workshop,*, 2000.

[30] C. A. M. de Almeida, F. G. Nievinski, and R. dos Santos da Rocha, "Avaliação da transformação de coordenadas geodésicas usando diferentes métodos e parâmetros no brasil," in *Congresso Brasileiro de Cadastro Técnico Multifinalitário*, (Florianopolis), Outubro 2002.

[31] I. B. de Geografia e Estatística, "Projeto mudança do referencial geodésico," tech. rep., IBGE, 2005. http://www.ibge.gov.br.

[32] C. Loch and J. Cordini, *Topografia Contemporanea: planimetria.* Editora da UFSC, 2000.

[33] D. of Defense, "Usno navstar global positioning system," tech. rep., USNO, 1994.

[34] N. Imagery and M. A. (NIMA), "Department of defense world geodetic system 1984, its definition and relationships with local geodetic systems," tech. rep., Department Of Defense, 1984.

[35] N. M. E. Association, "Nmea 0183 standard," tech. rep., National Marine Electronics Association, 2002.

[36] P. Chandra, M. Messier, and J. Viega, *Network Security with OpenSSL.* O'Reilly, 2002.

[37] "Openssl fips 140-2 validation certificate," Certificate 733, National Institute of Standards and Technology, 2007.