Centro Universitário Positivo – Unicenp
Núcleo de Ciências Exatas e de Tecnologia – NCET
Engenharia da Computação
Alfonso Diaz-Granados Marquez

SISTEMA ANTI-FURTO DE VEÍCULOS AUTOMOTIVOS

Curitiba
2006

Centro Universitário Positivo – Unicenp

Núcleo de Ciências Exatas e de Tecnologia – NCET

Engenharia da Computação

Alfonso Diaz-Granados Marquez

SISTEMA ANTI-FURTO DE VEÍCULOS AUTOMOTIVOS

Monografia apresentada à disciplina de Projeto Final, como requisito parcial à conclusão do curso de Engenharia de Computação. Orientador Prof. Alessandro Brawerman.

Curitiba

2006

TERMO DE APROVAÇÃO

Alfonso Diaz-Granados Marquez

SISTEMA ANTI-FURTO DE VEÍCULOS AUTOMOTIVOS

Monografia aprovada como requisito parcial à conclusão do curso de Engenharia de Computação do Centro Universitário Positivo, pela seguinte banca examinadora:

Professor Alessandro Brawerman (orientador)
Professor Edson Pedro Ferlin
Professora Adriana Cursino Thomé

Curitiba 11 de Dezembro de 2006

Sumário

I. Lista de Figuras

II. Lista de Tabelas

III. Lista de Siglas

AES – Ing. Sigla para Advanced Encryption Algorithm.

RF – Radio Frequency.

CI – Circuito Integrado.

PIC – Microchip Controller.

DES – Ing. Sigla para Data Encryption Standard.

GFSK – Gaussian Frequency Shift Keying.

FSK – Frequency Shift Keying.

Full-Duplex – Modalidade de transmissão de dados, no padrão Ethernet, em que a informação ocorre nos dois sentidos simultaneamente.

PDIP – Plastic Dual Inline Package

PLCC – Plastic Leaded Chip Carrier - Encapsulamento Plástico com Contatos

ICSP – In Circuit Serial Programming – Modo de programação do PIC sem necessidade de remoção do mesmo do circuito.

Prot-o-Board – Matriz de contatos utilizada para a montagem de circuitos.

LEDS – Diodos que emitem luminosidade.

IV. Lista de Símbolos

dBm – Esta unidade de medida se refere a atenuação medida em decibel/metro.

Kbps – kilo bit por segundo.

V – Volts.

RESUMO

Neste projeto, é especificado um protótipo de um mecanismo para a segurança de veículos automotores que utiliza em sua construção um dispositivo central embarcado no automóvel, capaz de emitir uma mensagem desafio via radiofreqüência. Esta mensagem é interpretada por um dispositivo portátil, seja ele, um relógio, um controle, ou algo similar, de tamanho reduzido, visando que o usuário esteja portando-o a todo o momento.

Este dispositivo portátil recebe a mensagem e a interpreta. Em seguida, uma resposta é gerada e encriptada. Após realizar a codificação da mensagem o dispositivo portátil retransmite a mesma ao dispositivo instalado no automóvel.

Após o recebimento da mensagem desafio pelo dispositivo no automóvel, é feita uma comparação entre a mensagem original gerada e a recebida. Se elas são iguais, o veículo autentica o seu proprietário e permite sua utilização. Caso o veículo já esteja acionado, ele permanece no mesmo estado em que se encontra e, caso a interpretação da mensagem detecte um erro, ou a ausência do dispositivo portátil, o automóvel é desativado.

ABSTRACT

This project presents a prototype of a security device to be added to the already existing security features on an automobile. This device uses a module attached to the main electronic-fuel injection system into the automobile.

This device is capable of transmitting a secure message using radiofrequency. This message will be received and interpreted by a portable device that could be a watch, a small remote or something similar with the objective that the user is carrying it at all times.

This portable device receives a secure message and process the information contained in this message. After this process, a response is generated and encrypted. This message is sent back to the device that originated the message into the automobile.

After this message being received by the embedded device, a comparison is made to check if the received message matches the original one generated. If the message happens to be the same the owner is authenticated and the automobile is ready to be used. If the message is not acknowledged or received the system will deactivate the automobile or make not available to use.

1. INTRODUÇÃO

Existe um número grande e crescente de roubos de automóveis em que o condutor do veículo é retirado do mesmo e seu veículo levado. Em grande parte das situações, o condutor não dispõe de recursos que o possibilitem agir de maneira ativa para que tal fato seja evitado. Na maioria dos casos, o veículo não é recuperado, e quando é, geralmente apresenta-se bastante danificado. Por esta razão, a existência de um sistema para prevenção de furtos de automóveis mostra-se atrativo e eficiente.

Encontra-se diversas tecnologias para a prevenção de roubos de automóveis, entretanto, não há ainda no mercado uma tecnologia simples e barata que permita a autenticação do usuário do veículo por seu computador de bordo.

A maioria dos dispositivos comercializados são projetados utilizando temporizadores, o que ajuda na proteção do veículo quando o mesmo é seqüestrado. Esta projeção dos dispositivos existentes realiza o corte do combustível ou ainda, o corte do fornecimento de energia à parte elétrica do mesmo.

Estes sistemas comerciais têm uma debilidade relacionada à falta de um dispositivo externo para que o veículo seja ativado, dado que, somente o conhecimento do dispositivo permitiria a desativação do mesmo e o veículo seria acionado facilmente.

Com o dispositivo projetado o condutor será removido do carro, no entanto este terá tempo suficiente para procurar auxílio, pois seu veículo será encontrado num raio próximo ao qual ele foi roubado, evitando assim, conseqüências mais drásticas.

2. TRABALHOS RELACIONADOS

2.1. Smart Call

O *Smart Call* é um sistema de alarme para carros com aviso pelo celular. É um sistema inteligente que monitora o alarme do veículo, avisando pelo celular toda vez que o alarme disparar. O *Smart Call* adiciona segurança contra roubos, furtos e seqüestros, além de fornecer mais comodidade e confiança ao proprietário do veículo. O produto é um sistema simples que após a instalação o veículo passa a ser monitorado pelo sistema acoplado ao alarme do veículo.

A simplicidade de seu circuito torna-o eficiente e confiável. O funcionamento do *Smart Call* é de fácil entendimento; quando o veículo dispara o alarme, seja por qualquer motivo, o celular do proprietário recebe uma chamada após o inicio do disparo, com a descrição no *display*: "Alarme do carro".

Este sistema não previne o roubo do carro, somente monitora se o alarme foi disparado. A partir disto o proprietário deverá tomar providências adequadas e certificar-se se que seu carro encontra-se seguro (Smart-Call, 2006).

2.2. SASCAR Celular

O Sascar GSM é um sistema de controle para frotas. O Sascar GSM se utiliza da tecnologia para gerenciar o deslocamento de veículos via Internet. Com ele é possível fazer o controle, monitoramento e rastreamento de cargas, veículos e mercadorias. Por isso, é o sistema ideal para empresas que operam em áreas metropolitanas e inter-metropolitanas, nos setores de logística e distribuição.

Já o Sascar Celular é um sistema que funciona com tecnologia celular (TDMA) Em caso de roubo ou furto, o Sascar Celular rastreia e localiza o veículo num raio de até 400 metros, bloqueando-o em seguida. Utiliza-se para isto uma carta vetorizada da cidade com mapas de localização das estações da rádio base.

Estes sistemas possuem dispositivo anti-seqüestro com “botão de pânico”. Ao ser acionado, o sistema envia um sinal para o Centro de Controle de forma imperceptível. Através de uma escuta interna, o Centro de Controle passa a monitorar e gravar tudo o que acontece no interior do veículo (Sascar, 2006).

Uma grande desvantagem deste sistema é o custo elevado para os usuários finais.

3. ESPECIFICAÇÃO

3.1. Descrição geral

O sistema completo é composto por dois módulos: um está embarcado em um lugar seguro dentro do automóvel e de difícil acesso; o outro é um módulo portátil de dimensões aproximadas as de um relógio ou controle de portão que deverá ficar sob custódia do proprietário do veículo.

O funcionamento do sistema basicamente consiste na troca de mensagens entre as duas partes. O dispositivo embarcado vai acoplado ao módulo de injeção eletrônica do veículo, controlando assim a sua ativação e travamento. Este dispositivo envia uma mensagem secreta ao dispositivo portátil que estará com o dono do veículo. Assim que a mensagem for verificada, responderá ao dispositivo embarcado com uma mensagem secreta contendo uma chave.

Caso esta mensagem secreta não seja recebida corretamente, não seja recebida por estar fora do alcance ou a chave estar incorreta, o sistema realiza novamente a tentativa de receber uma resposta do dispositivo portátil, realizando o envio da mensagem secreta novamente. Este procedimento se repetirá cinco vezes, até que por fim o sistema desativará o módulo de injeção eletrônica do veículo impossibilitando a sua movimentação.

Se o módulo embarcado desativar o sistema de injeção, pode-se assumir que o dispositivo portátil não esta presente ou que a chave contida nele, não é a chave correta para permitir a ativação do veículo.

3.2. Integração

Quando o sistema for acionado, a parte do sistema embarcada no automóvel gera uma mensagem e esta será criptografada e enviada ao equipamento que está sendo portado pelo proprietário do veículo. Para isso, é utilizada a transmissão de dados por RF. Esta mensagem desafio é criptografada utilizando AES 128 bits (NITS, 2001).

O módulo portado pelo proprietário recebe os dados e logo o processador realiza a decodificação para confirmar que a mensagem recebida é a correta. Depois de verificada a mensagem, é adicionada uma chave na mesma. Esta chave é a parte da mensagem que será verificada no módulo embarcado no veículo para garantir que o dono deste esteja presente.

Depois de adicionada a chave, a mensagem é codificada e enviada novamente ao módulo embarcado.

O módulo embarcado recebe a resposta desafio, que está criptografada. Este decodifica a mensagem e verifica se esta mensagem recebida contém a chave verificadora, enviada pelo módulo portátil. Caso a mensagem seja confirmada o sistema envia a mensagem novamente para o módulo do portador. Com isso o processo se repete ciclicamente, enquanto o veículo estiver acionado.

O comprimento da mensagem utilizado é de 128 bits (16 *bytes*). A chave codificada em 128 bits garante que o dispositivo portátil não pode ser duplicado já que o algoritmo de codificação, o AES, ainda não foi quebrado, fazendo que com que o sistema seja de alta confiabilidade.

Caso o módulo embarcado não receba a mensagem correta, pelo módulo do portador não ser o correto ou pela ausência de resposta devido a distância, o sistema desativa o veículo.

3.3. Módulos e sub-módulos

O módulo embarcado é alimentado pela bateria do automóvel, +12Vcc. Este módulo é composto por três sub-módulos. O primeiro sub-módulo (4) é a principal parte do sistema. Neste, o processador realiza a criptografia da mensagem desafio na memória. O processador é da fabricante Microchip – PIC modelo 18F458 (MICROCHIP, 2006).

Existe a conectividade deste primeiro sub-módulo (4) com um segundo sub-módulo (5), o qual realiza a transmissão via radiofreqüência – RF – utilizando um transceptor. Os dados são enviados em série do módulo de processamento, criptografados, ao módulo de transmissão que realiza toda a comunicação entre os dois módulos do sistema.

O terceiro sub-módulo (2) é a parte do mecanismo de acionamento para o desligamento do automóvel. Uma vez que um ciclo de informação é completado, este sub-módulo pode ou não ser acionado dependendo da resposta do sistema.

Na Figura 1 é mostrada a integração de todos os sub-módulos do sistema em uma única placa assim como detalhados acima.

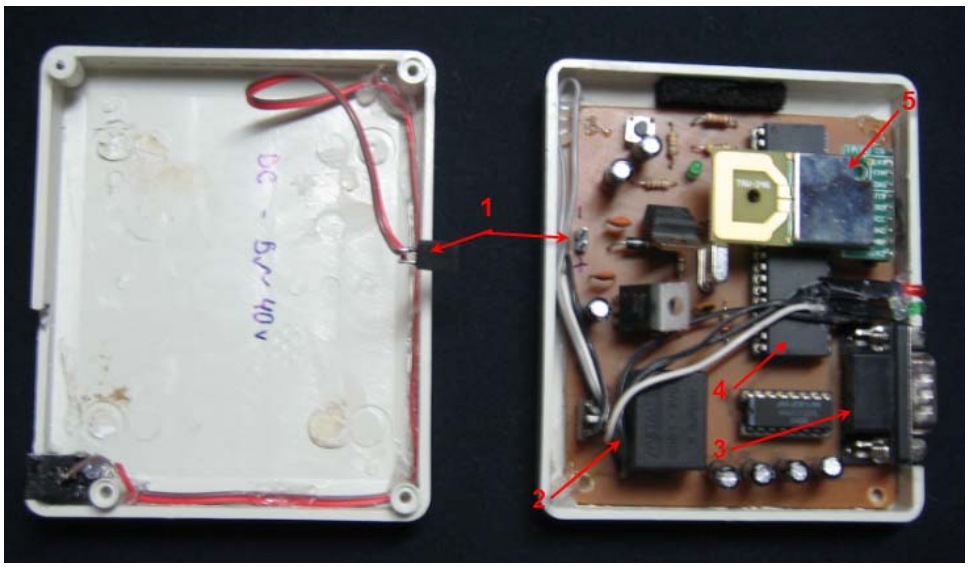

Figura 1 – Foto protótipo do módulo embarcado

A seguir uma breve descrição das setas enumeradas na Figura 1:

1 – Alimentação (pode variar de +5Vcc até +40Vcc)

2 – Relé de ativação – resposta do sistema

3 – Interface serial utilizada para gravação do PIC

4 – PIC 18F458

5 – Rádio TRW-24G

No módulo secundário, ou seja, no que deve ser portado pelo usuário, há apenas dois sub-módulos, sendo um deles o de comunicação RF utilizando um transceptor (2) e o outro sub-módulo com o processador (1).

Estes sub-módulos são alimentados por uma pequena bateria, para que seja possível a sua portabilidade. Este módulo realiza a decodificação da mensagem enviada pelo módulo principal, logo realizará a interpretação da mensagem recebida e adicionará uma chave verificadora a esta mensagem, devolvendo-a ao módulo principal via RF.

O módulo portátil é ilustrado na Figura 2.

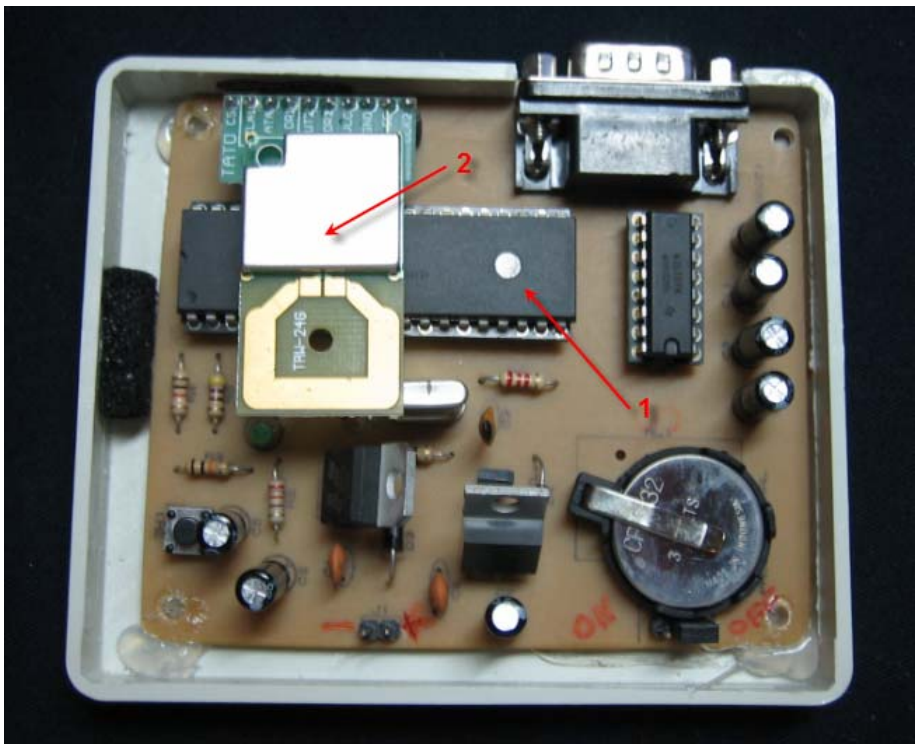

Figura 2 - Foto do protótipo do módulo portátil

3.4. Teoria

A teoria para a elaboração deste projeto compreendeu o estudo do método de criptografia AES128 bits e também estudo de hardware que compreende o processador PIC e suas funcionalidades assim como o estudo de transmissão usando radiofreqüência com o uso do rádio TRW-24G.

3.4.1. Criptografia

A criptografia utiliza o algoritmo do AES (NITS, 2001). Esta criptografia vem sendo utilizada há muito tempo e a comunidade científica ainda não encontrou erros relevantes.

Os resultados mostram que o AES pode ter um baixo perfil de consumo de memória com um bom desempenho e poderá orientar projetos de ambientes de segurança mais sofisticados para equipamentos de baixa capacidade computacional, e, por esta e outras qualidades do algoritmo ele foi escolhido para realizar a criptografia do sistema.

O AES surgiu em 1998, criado por Vincent Rijmen e Joan Daemen, consistindo de uma cifra de blocos baseado em uma rede de permutação em blocos de 128, 160, 192, 224, e 256 bits e chaves de 128, 160, 192, 224, e 256 bits, sendo submetido ao *National Institute of Standards and Technology* com o objetivo de ser aceito como padrão do governo americano em sucessão ao DES (NITS, 2001).

Em 2001, ao final do processo de seleção foi escolhido entre 12 algoritmos como padrão sob o nome de AES e somente com blocos de 128 bits e chaves de 128, 192 e 256 bits. O algoritmo é baseado em um trabalho anterior de Rijmen e Daemen chamado Square, que por sua vez é derivado do algoritmo Shark (NITS, 2001), também de ambos.

Os blocos consistem de matrizes de 4x4 bytes (blocos de Rijndael com mais de 128 bits usam matrizes maiores). As chaves de cada iteração são

calculadas em operações de campo finito (a maioria das operações dentro desse algoritmo são feitas dessa forma).

Cada iteração (com exceção da última) consiste em quatro etapas: primeiro cada *byte* da matriz é substituído em uma S-Box, então cada linha da matriz é deslocada N posições, em seguida as colunas são substituídas numa operação de campo finito (com exceção da última iteração) e então é aplicada a chave da iteração a matriz resultante. Este processo é repetido 10, 12 e 14 vezes dependendo do tamanho da chave utilizada (128, 192, 256).

A Figura 3 mostra o diagrama em bloco da arquitetura do AES, mostrando como o processo codifica um texto de 64 bits gerando um resultado de 64 bits criptografados.

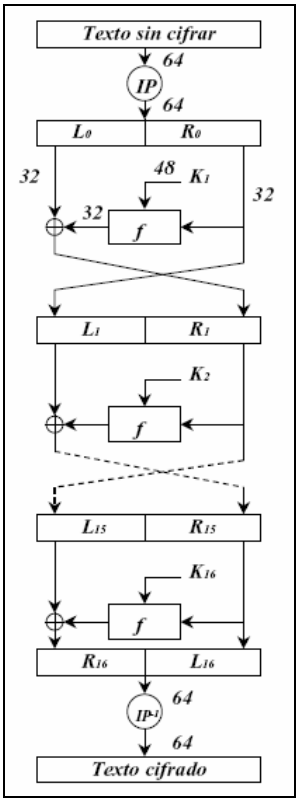

Figura 3 - Arquitetura do sistema AES

Não existem ataques efetivos conhecidos contra o AES, em 2002 um ataque teórico conhecido como “XLT attack” foi proposto por Nicolas Courtois, porém estudos conseqüentes não reproduziram os termos de Courtois, ataques “XLT” são considerados especulativos e nunca foram reproduzidos.

Em Abril de 2005 Daniel J. Bernstein propôs um ataque chamado “*cached timing*”, que devido a impraticidade de reprodução (foram usando 200 milhões de

textos sem criptografia) foi considerado impraticável. O governo americano considera AES como utilizável em proteção de dados considerados secretos (SLACKWAREZINE, 2005).

3.4.2. Processador

O processador utilizado em ambos os módulos será o PIC – 18F458 da fabricante Microchip – (MICROCHIP, 2006).

Este processador foi escolhido por ter uma capacidade de processamento de um código de criptografia com um bom tempo de resposta e conseguir controlar o rádio ao mesmo tempo, sem a necessidade de um processador adicional ou memória adicional.

O sistema será desenvolvido utilizando o componente versão PDIP por motivos de manuseabilidade. Este processador também tem a vantagem de poder ser alimentado com tensões variando entre +2Vcc. e +5Vcc. o que possibilita o uso de uma tensão única de alimentação no módulo portátil de +3Vcc.

A Tabela 1, mostra o desempenho do PIC (ERIC, 2003) semelhante ao PIC selecionado.

Tabela 1 - Velocidade de execução

Function	Performance on 20 MHz Microchip PIC16F84A		
	cycle count	time	bits per second
Key Setup	156	31.2 uS	n/a
Encryption	5694	1.14 mS	56.2 Kb/s
Decryption	5784	1.16 mS	55.3 Kb/s

Na Figura 4 se encontram os diagramas de pinos do PIC18F458, componente escolhido como processador do sistema. Esta mostra os dois modelos de encapsulamento do processador. A versão PDIP mostrada na Figura 4 ilustra a posição dos pinos do processador utilizado.

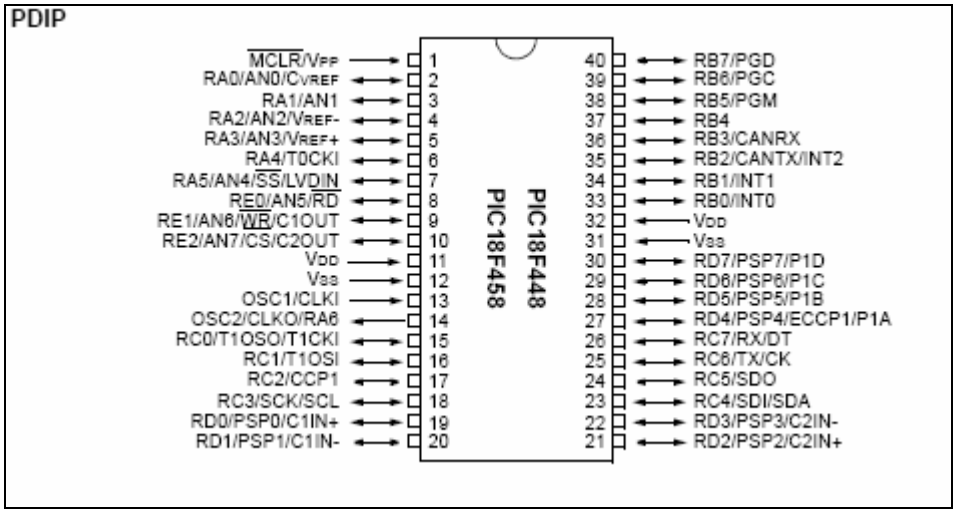

Figura 4 – Pinajem - PIC 18F458

Algumas características extras do PIC são mostradas na Tabela 2. Estas características mostram a capacidade do PIC18F458 para realizar o processamento.

O tamanho da memória de 1536 bytes foi suficiente para comportar as tabelas de codificação geradas pelo algoritmo de criptografia. Também pode-se verificar a capacidade de ser programado utilizado-se o ICSP – programação do processador sem a necessidade de remoção do circuito.

Tabela 2 - Características

Features		PIC18F458
Operating Frequency		DC – 40 MHz
Internal Program Memory	Bytes	32K
	# of Single-Word Instructions	16384
Data Memory (Bytes)		1536
Data EEPROM Memory (Bytes)		256
Interrupt Sources		21
I/O Ports		Ports A, B, C, D, E
Timers		4
Capture/Compare/PWM Modules		1
Enhanced Capture/Compare/ PWM Modules		1
Serial Communications		MSSP, CAN, Addressable USART
Parallel Communications (PSP)		Yes
10-bit Analog-to-Digital Converter		8 input channels
Analog Comparators		2
Analog Comparators VREF Output		Yes
Resets (and Delays)		POR, BOR, RESET Instruction, Stack Full, Stack Underflow (PWRT, OST)
Programmable Low-Voltage Detect		Yes
Programmable Brown-out Reset		Yes
CAN Module		Yes
In-Circuit Serial Programming™ (ICSP™)		Yes
Instruction Set		75 Instructions
Packages		40-pin PDIP 44-pin PLCC 44-pin TQFP

Na Figura 5, é mostrado o diagrama em blocos do PIC18F458 selecionado para ser o processador deste sistema.

Este diagrama ilustra como é o funcionamento interno do processador como máquina. Mostra também os blocos de memória interna, núcleos de processamento, interfaces de entrada e saída, e todas as características de micro processamento que este PIC possui.

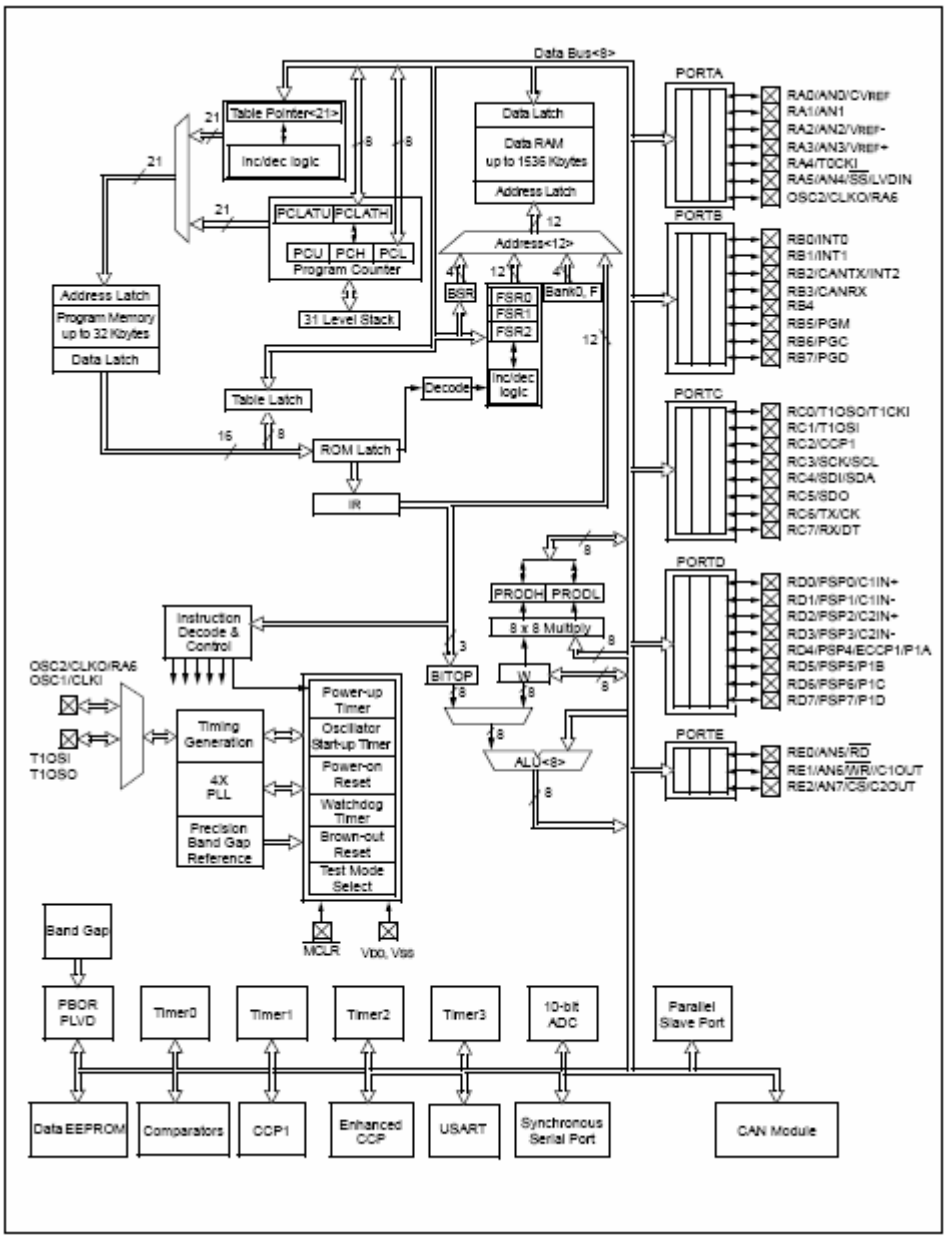

Figura 5 - Diagrama em blocos - PIC18F458

3.4.3. Transmissor / receptor

O transmissor e receptor foram colocados em um mesmo módulo, um transceptor (transmissor e receptor) de 2.4GHz. Este transceptor é de pequeno porte e baixo consumo (LAIPAC, 2005).

Na Figura 6, mostra-se o uma figura do rádio. Este tem dimensões reduzidas informadas nas características chave, facilitando a portabilidade do módulo do usuário.

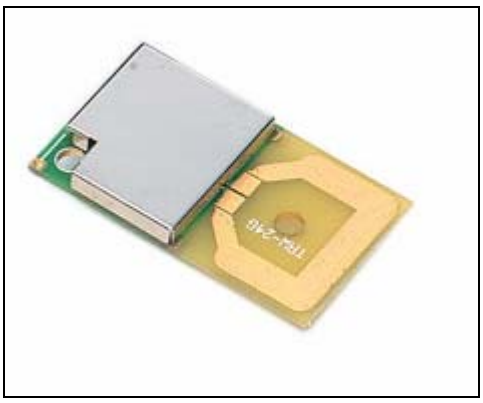

Figura 6 - Transceptor TRW-24G

Algumas características chave do TRW-24G

- Freqüência: 2,4 GHz Modulação: GFSK;
- Voltagem: +3Vcc;
- Potência: +4dBm;
- Data Rate: 1Mbps; 250Kbps;
- Tamanho: 20,0*36,7*2,4mm;
- Alcance: 280m (250Kbps); 150m (1Mbps);
- Transmissão *full-duplex*, incluindo codificação, decodificação e buffer de dados.

A Figura 7 mostra o diagrama de conexão do rádio utilizado.

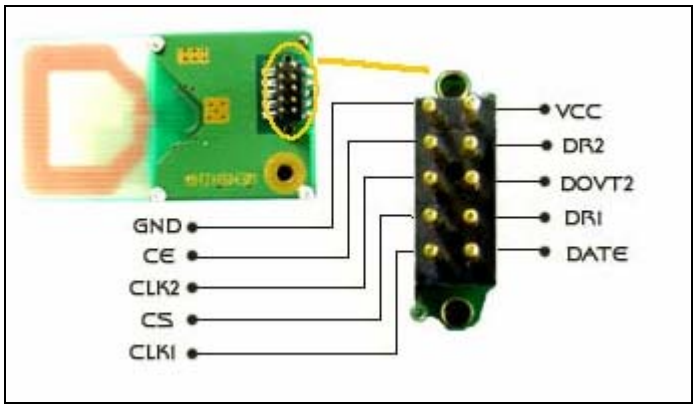

Figura 7 – Diagrama de conexão do transceiver TRW-24G

Na Figura 8 observa-se a vista frontal e lateral do rádio com as suas respectivas medidas. Estas medidas possibilitam realizar o estudo da localização do componente no sistema mesmo antes do desenho da placa.

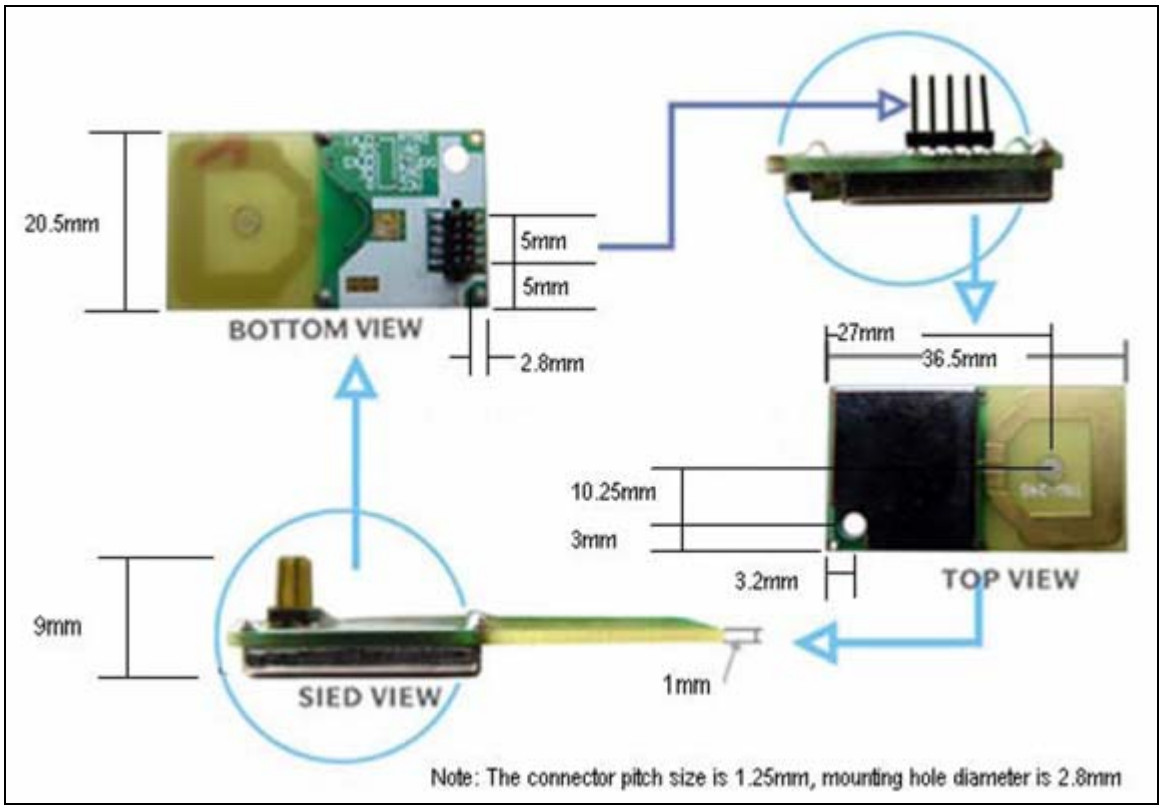

Figura 8 - Vista lateral e superior do TRW-24G

Este rádio funciona utilizando a modulação GFSK e uma freqüência de 2,4GHz.

Na modulação GFSK (Chave por alteração de freqüência gaussiana) os dados são codificados na forma de variações de freqüência em uma portadora, de maneira similar à modulação FSK (Chave por alteração de freqüência). Portanto, o modulador utilizado pode ser o mesmo que para a modulação FSK (EE TIMES, 2002).

Todavia, antes dos pulsos entrarem no modulador, eles passam por um filtro gaussiano, conforme a Figura 9, de modo a reduzir a largura espectral dos mesmos. O filtro gaussiano é uma espécie de formatador de pulso que serve para suavizar a transição entre os valores dos pulsos. A Figura 9 ilustra a transformação dos pulsos após passarem pelo filtro gaussiano.

Figura 9 - Modulação GFSK

A modulação GFSK é utilizada nos sistemas Bluetooth, uma vez que provê uma melhor eficiência espectral em relação à modulação FSK (MODULAÇÃO, 2004).

3.5. Hardware

3.5.1. Funções do sistema

O sistema será embarcado e somente realizará o controle da presença do dono do automóvel a certa distância.

A interação com o usuário é transparente uma vez que o sistema é automatizado. A única ação que o usuário tem que realizar é a de estar portando o módulo do sistema e estar próximo ou dentro do veículo e, em caso de pane no sistema efetuar o *reset* do mesmo.

3.5.2. Requisitos do sistema

O sistema embarcado utiliza o fornecimento de energia do próprio automóvel, não sendo necessário nenhum tipo de bateria auxiliar ou adaptação. Caso o sistema detecte que o proprietário do veículo não esta presente, é acionado e desliga o veículo. O acionador do sistema corta a energia do sistema de injeção eletrônica do veículo impossibilitado assim o seu acionamento.

O módulo portátil por sua vez, necessita de uma bateria para alimentar os sub-módulos de processamento e de transmissão. O sub-módulo de processamento foi programado para “hibernar” enquanto não estiver sendo usado, o que ajuda a economizar bateria.

A bateria deverá ser de lítio de +3Vcc, modelo CR2032 (modelo comercial).

3.5.3. Componentes

Para a confecção do sistema serão utilizados componentes comerciais, com a exceção do transceptor TRW-24G e do PIC 18F458 que não são tão fáceis de ser encontrados.

Os PICs foram recebidos como amostras solicitadas a Microchip e o módulo de transmissão terá que ser adquirido. Os outros componentes utilizados serão de fácil manuseio. Para o protótipo 1 não será levado em conta o tamanho dos módulos, e de acordo com o projeto, será verificada a possibilidade de realizar a miniaturização dos módulos para possibilitar a portabilidade.

Na Figura 10, é mostrado o diagrama em blocos do sistema. Este diagrama mostra como é a comunicação entre divisões internas do sistema. No dispositivo embarcado, existe o que realiza o corte da energia do sistema de injeção eletrônica, sendo este o sub-módulo acionador. Este por sua vez recebe as instruções do sub-módulo de processamento que está em constante comunicação com o sub-módulo de transmissão.

Como não existe a necessidade de economia de energia no módulo embarcado, o processador do sistema está sempre ativo e realizando a rotina de codificação das chaves para o envio ao dispositivo portátil.

No módulo portátil existem apenas dois sub-módulos, o de processamento e o de transmissão. O sub-módulo de transmissão está configurado para receber informações e a partir do momento que este recebe uma instrução, aciona o processador. Após terminada a rotina de processamento, o processador envia os dados de volta e retorna ao modo de hibernação.

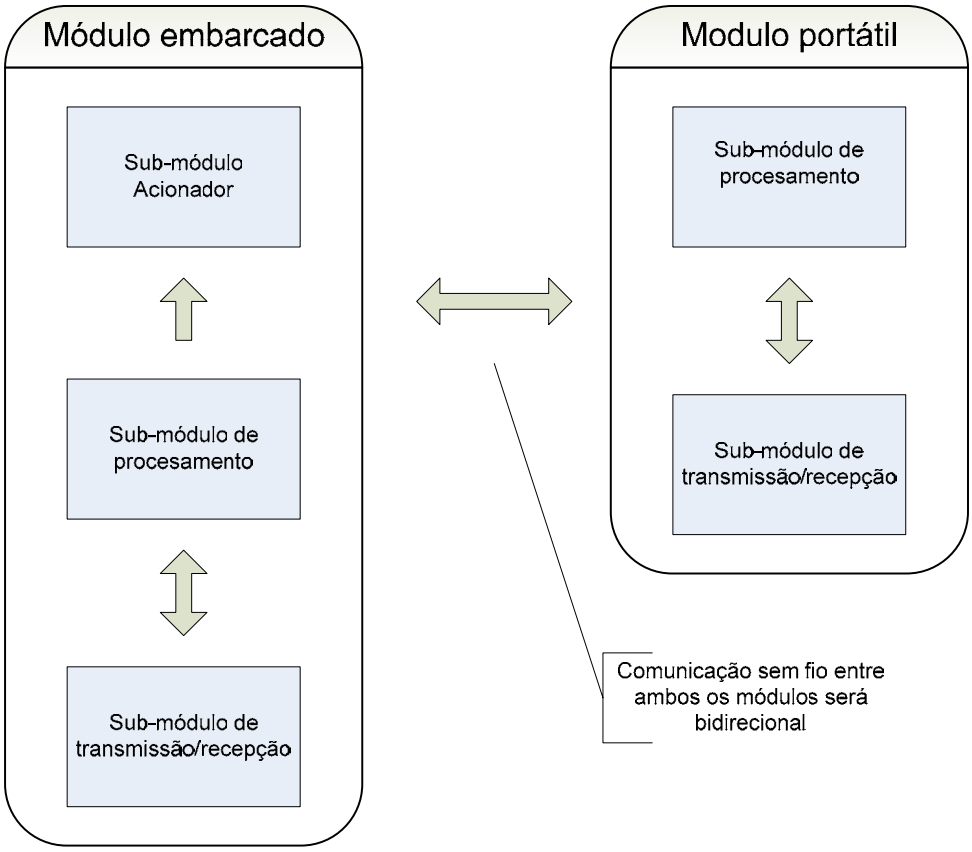

Figura 10 - Diagrama em blocos do sistema

3.5.4. *Software*

A parte do algoritmo do AES realizará a codificação e decodificação das mensagens, no entanto ainda apresenta-se em fase de testes. O código em C utilizado na programação do PIC pode ser vista no Anexo 2 (ERIC, 2003).

Este algoritmo é implementado utilizando a ferramenta PICC, específica para a elaboração de aplicativos para o PIC. Esta ferramenta possui diversos utilitários que possibilitam realizar um acompanhamento to progresso da criptografia da mensagem e também verificação das respostas do sistema.

Existe a necessidade da utilização deste pois o PIC demanda uma série de bibliotecas que devem ser incluídas no código para o correto funcionamento do mesmo.

O *software* que será utilizado neste projeto será resumido ao algoritmo de criptografia e decriptografia. Este algoritmo será executado pelo PIC 18F458 em

ambos os módulos. O algoritmo do AES funciona com blocos de 128 bits e chaves de 128, 192 e 256 bits.

Foi selecionado o tamanho de chave de 128 bits já que com 128 bits o número de dispositivos que podem ser criados é bastante significativo (2^{128} = 3,4 * 10^{38} dispositivos possíveis) além de esta criptografia ser bastante segura, não existindo registros de haver sido quebrada.

Na Figura 11 é mostrado como o AES realiza a criptografia do texto simples. Este texto é criptografado com a ajuda de 10 chaves auxiliares (Nr = 10 p/ 128 bits) (ANGEL, 2005)

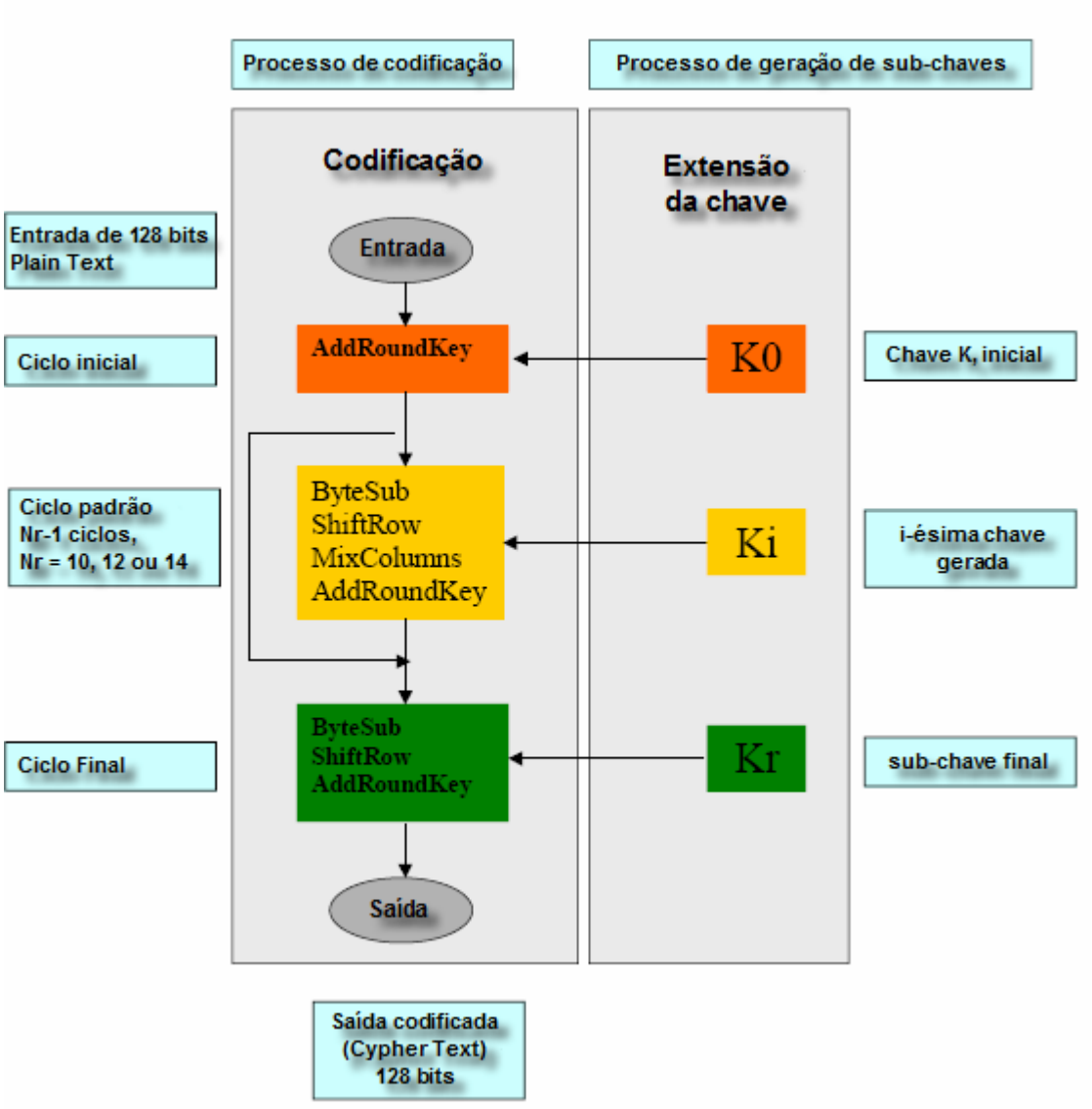

Figura 11 - Diagrama de funcionamento do AES

Na parte referente a codificação existem várias funções próprias do AES como AddRoundKey, ByteSub, ShiftRow, MixColumns e, assim, por diante. Estas funções podem ser encontradas no algoritmo do AES adicionado no Anexo 1.

Função AddRoundKey:

Esta transformação toma uma matriz e realiza um *xor* byte a byte com a correspondente matriz de chaves dependendo do ciclo em que estiver.

Por exemplo, a matriz ij[a] e ij[k] aonde sai como resultado a matriz ij[a⊕k], ou seja, é realizado uma operação binária *xor* entrada a entrada da matriz do bloco de texto com a matriz da sub-chave correspondente.

A matriz tem 4 colunas e toma a extensão da chave também 4 colunas. O programa de chaves gera as necessárias matrizes de chaves para todos os ciclos, conforme mostrado na Figura 12.

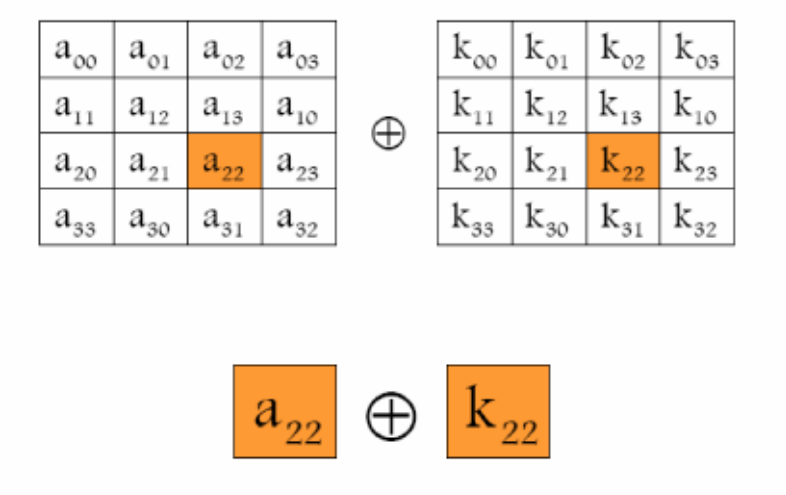

Figura 12 – Demonstração da função AddRoundKey

Função ByteSub:

Neste caso a cada elemento da matriz estado (byte) é substituído por outro byte, que depende do primeiro, conforme mostrado na Figura 13.

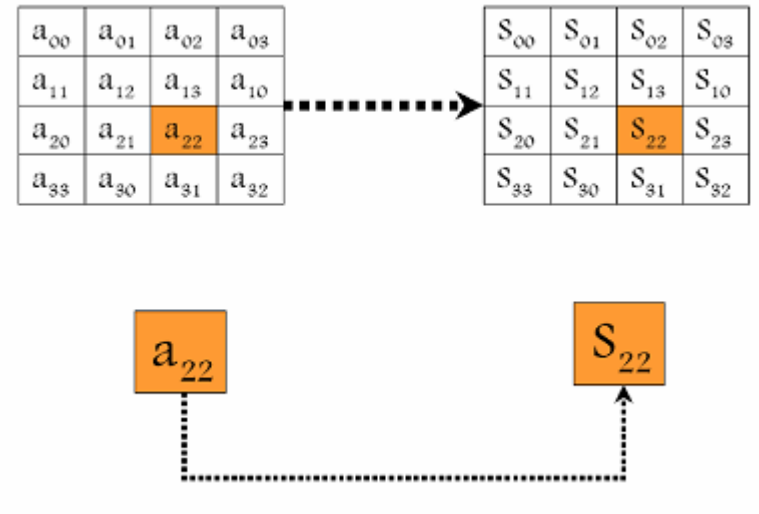

Figura 13 – Demonstração da função ByteSub

Função ShiftRow:

A transformação *ShiftRow* se aplica na matriz estado, aplicando-se deslocamentos em suas colunas. Se aplica na matriz [a_{ij}], *shifts* (deslocamentos para a esquerda circulares em bytes) nas colunas, da seguinte maneira, desloca 0 bytes a na primeira, 1 byte na segunda, 2 bytes na terceira, e 3 bytes deslocados na quarta, conforme mostrado na Figura 14.

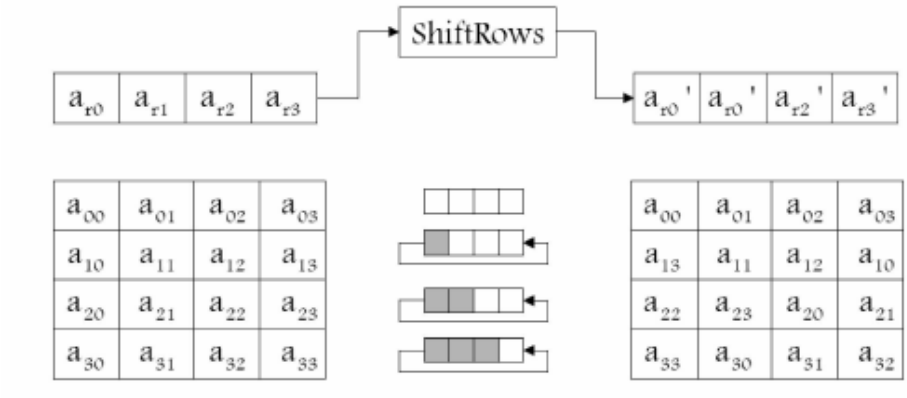

Figura 14 - Demonstração da função ShiftRow

Função MixColumns:

Cada coluna da matriz [a_{ij}] é multiplicada por uma coluna constante em $GF(2^8)[x]/(x^4+1)$, conforme mostrado na Figura 15.

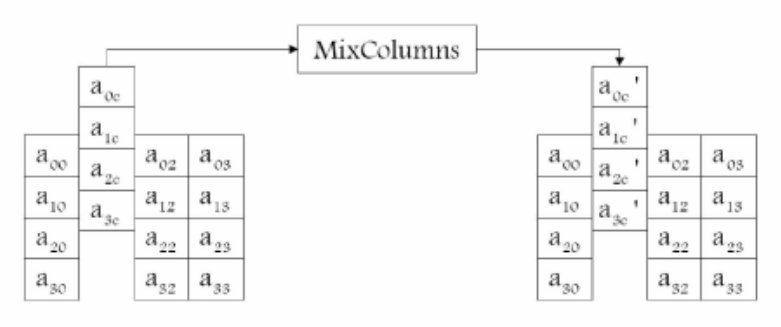

Figura 15 - Demonstração da função MixClumns

A função MixColumns toma cada coluna A, e envia a outra coluna A', que se obtém ao multiplicar A por um polinômio constante c(x) GF(2)[x]/(x 1), c(x) = 03 x +01 x +01 x + 02, então A' = A c(x), que pode ser representado na matriz mostrada na Figura 16.

$$\begin{bmatrix} a_0' \\ a_1' \\ a_2' \\ a_3' \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Figura 16 - Produto final da função MixColumns

Somando-se todas estas etapas, seguindo o fluxograma mostrado na Figura 11, temos como resultado o texto criptografado de 128 bits. É uma criptografia complexa, porém, rápida.

Em testes já realizados, mostra-se que o algoritmo sendo executado por um PIC 18F458 leva em torno de 1 segundo, que para objeto de estudo, tempo aceitável. O ambiente no qual este foi desenvolvido é voltado ao microprocessador PIC, já que este será a chave de todo o processamento do sistema.

O software do sistema é divido em varias secções. Uma destas secções é o *driver* do transceiver TRW-24G fornecido pelo fabricante – Laipac. (LAIPAC, 2005). Este *driver* é aonde o rádio é configurado para 16 bytes, e também, para o envio ou recepção dos dados.

Este *driver* foi testado com sucesso no PIC 18F458, com o código inserido no Anexo 1.

Após finalizado o código no PICC este é compilado e salvo no formato de arquivo .hex. Este formato de arquivo é o firmware do sistema.

Este *firmware* é gravado no PIC utilizando uma interface serial e com o auxílio do programa chamado "*Tiny*". Este programa reconhece o *firmware* e com o auxílio do botão *reset* do sistema, automaticamente grava o mesmo no chip sem a necessidade da remoção do PIC da placa.

4. IMPLEMENTAÇÃO

A implementação do projeto levou em vista a concepção de circuitos elétricos de baixo consumo, devido a necessidade de portabilidade.

4.1. Módulo principal

A montagem do módulo principal segue o diagrama elétrico ilustrado na Figura 17. Este diagrama mostra as conexões feitas entre cada sub-módulo do sistema.

Figura 17 - Diagrama elétrico do módulo embarcado do sistema

Esta montagem foi confeccionada nesta placa devido a nela já estar montado o gravador do PIC via serial, o que facilitou bastante nos testes de programação do módulo e, também, de depuração de erros.

O desenho da placa montada é mostrado na Figura 18. Podemos ver a possibilidade de redução na escala do projeto já que a maior parte deste é o PIC e a parte de alimentação. Assim como a parte serial de conexão com o PC também pode ser suprimida uma vez o PIC gravado.

Figura 18 - Diagrama da placa - PIC 18F458 com rádio TRW-24G

Com a confecção deste módulo foi possível verificar a possibilidade de gravação e correção dos programas testes elaborados.

4.2. Módulo de alimentação

O módulo foi construído devido à necessidade da redução da tensão de alimentação de +5Vcc para +3Vcc, já que o módulo de rádio é alimentado com o máximo de +3Vcc, e para a gravação do PIC, deve-se utilizar +5Vcc, existiu a necessidade de fazer o acoplamento das tensões na placa, sendo parte dela alimentada em +3Vcc e parte alimentada em +5Vcc. O esquema do módulo está mostrado na Figura 19.

Figura 19 - Módulo de alimentação do circuito em +5Vcc e +3Vcc

Este mesmo módulo foi utilizado como módulo de alimentação do circuito utilizado nos testes em *prot-o-board* e portado para o módulo portátil do sistema.

4.3. Módulo de gravação via serial

O módulo de gravação do PIC 18F458 utilizando a serial é um facilitador na hora da implementação dos testes já que ele utiliza a tensão de +5V e não requer que o PIC seja removido do circuito, o ICSP. O protótipo foi construído como e incluído o ICSP para auxiliar na gravação dos programas de teste no PIC (SLOTZ, 2005). O esquema do ICSP esta detalhado na Figura 20.

Pode-se verificar a conexão da porta serial padrão ao PIC com a utilização de um CI MAX232 para o controle da porta serial.

Figura 20 - Diagrama elétrico da funcionalidade ICSP do PIC18F458

4.4. Módulo portátil

O módulo portátil foi desenhado para melhor desempenho e portabilidade, utilizando alimentação de +3Vcc em todo o circuito. Como não existe o relé acionador que existe no primeiro módulo, este módulo é mais simplificado que o módulo embarcado. Este módulo está representado na Figura 21.

O módulo secundário foi projetado para utilizar +3Vcc na alimentação do circuito pensando na redução de tamanho e alimentação com baterias de lítio de +3Vcc no protótipo final do projeto.

No detalhamento do módulo mostrado na Figura 21, pode-se verificar a semelhança ao módulo embarcado, mostrado na Figura 17, somente existe a falta do sub-módulo de acionamento.

Figura 21 - Diagrama elétrico do módulo portátil

5. TESTES PRELIMINARES

Para a montagem do sistema vários testes foram efetuados. Logo que o processador foi selecionado, o primeiro teste realizado foi para a escolha do uso do rádio. Como os testes preliminares de implementação obtiveram sucesso o rádio escolhido foi o TRW-24G. Após a escolha do rádio alguns testes subseqüentes foram efetuados.

5.1. Teste 1 – Envio de mensagens de um módulo ao outro

O primeiro teste efetuado no sistema foi a realização da comunicação unilateral. Esta consiste no envio de uma simples mensagem de um módulo a outro do sistema.

A mensagem consiste em 2 bytes enviados do módulo embarcado ao módulo portátil. Este envio foi testado com certo sucesso. De acordo com o fabricante, o alcance seria de cerca de 100 metros, porém, o máximo alcançado foi uma distancia próxima a 70 metros.

Provavelmente a interferência eletromagnética e as paredes do local de testes dificultaram o envio da mensagem a maiores distâncias. O processo todo foi completado em menos de 1 segundo e a verificação da mensagem foi realizada utilizando *leds*.

O código utilizado para o envio e recepção das mensagens foi desenvolvido em C e adaptado ao ambiente utilizado na programação do PIC, o PICC.

Para o envio da mensagem foi gravado em um dos módulos o codigo:

5.2. Teste 2 – Envio de mensagem em ciclo

O segundo teste elaborado foi o envio de uma mensagem, também de 2 bytes do módulo embarcado ao módulo receptor e, assim que recebida pelo módulo portátil, essa mesma mensagem foi retransmitida ao módulo embarcado.

Este teste teve sucesso, levando em consideração a distância máxima entre os módulos. O processo todo foi completado em menos de 1 segundo e a verificação da mensagem foi realizada utilizando leds como no Teste 1.

Para realizar este teste foi realizada uma adaptação no código de recebimento e de envio da mensagem. O código de envio foi alterado para que assim que a mensagem fosse enviada, este alternasse o estado do rádio para receber a resposta.

A mensagem de recebimento por sua ver foi alterada para realizar o recebimento e comutar o transmissor para o envio da mesma novamente.

Quando a mensagem é recebida corretamente, o *led* verde é aceso. Este teste teve sucesso já que a mensagem era enviada e recebida corretamente nas 5 vezes que foi feito o teste.

5.3. Teste 3 – Alimentação reduzida

O terceiro teste foi a realização do teste de envio de mensagens de um módulo ao outro, porém utilizando a alimentação de +3Vcc.

Neste teste também foi obtido sucesso no envio das mensagens. Foi realizado um adicional no envio de uma mensagem de 16 bytes ao invés da mensagem de 2 bytes como nos testes anteriores.

O tempo de envio da mensagem foi inferior a 1 segundo e a verificação do envio e recebimento da mensagem foi realizada utilizando leds.

5.4. Teste 4 – Criptografia

O quarto teste foi conduzido utilizando o algoritmo de criptografia. Neste teste houve alguns problemas. Inicialmente o teste consistia na criptografia e da decriptografia de uma mensagem de 16 bytes.

Os problemas encontrados eram referentes ao tamanho da memória do PIC selecionado já que o AES tem matrizes alocadas que consomem muita memória do processador. Inicialmente o PIC 16F877 tinha um espaço muito pequeno de memória. Foi feita a troca do PIC para o atual 18F458, com muito mais memória e os problemas foram resolvidos.

Este resultou positivo já que o tempo de criptografia e decriptografia da mensagem foi inferior a 3 segundos. O tempo esperado, devido a complexidade do algoritmo era superior a 5 segundos. Tendo a resposta em menos de 3 segundos pôde ser considerado um teste efetivo. Este teste foi repetido 5 vezes para garantir uma maior precisão do resultado.

5.5. Teste 5 – Criptografia e Envio

O quinto teste foi conduzido utilizando o algoritmo de criptografia e a transmissão. Neste teste houve alguns problemas. Inicialmente o teste consistia

na criptografia de uma mensagem de 16 bytes e, logo, depois de criptografada a realização do envio. Ocorreram problemas nesta fase dos testes. Fazendo um estudo mais detalhado no material sobre o PIC e sobre o algoritmo de criptografia e foi verificado que o motivo do erro seria uma possível falta de memória interna no PIC.

Os erros ocorridos neste teste estavam relacionados a estouro de memória quando o algoritmo realizava a decriptografia. Ao chamar o método de decriptografia, as tabelas geradas excediam o tamanho da memória disponível, causando um erro.

Devido a este problema o PIC 16F877 foi substituído pelo PIC 18F458 resultando na solução dos problemas de memória ocorridos no PCI16F877. Os testes de criptografia e decriptografia foram efetuados 5 vezes em cada módulo do sistema utilizando o código de criptografia final mostrado nos Anexos 1 e 2.

6. CONCLUSÃO

Dado o crescente número de roubos de automóveis, foi projetado um dispositivo adicional aos atuais já existentes que tem por objetivo evitar o roubo do automóvel.

Este dispositivo melhora a segurança dos automóveis, já que no caso do roubo do veiculo, este, permanecerá acionado quando a distância for pequena.

O sistema foi desenvolvido para conter dois dispositivos, um que deve ser embarcado no veículo e o outro que deve ser portado pelo proprietário durante a utilização do veículo de maneira a ser autenticado quando próximo do mesmo.

Com a elaboração deste projeto conclui-se que é eletronicamente e financeiramente viável a adição deste dispositivo de segurança aos automóveis. Este é um sistema de fácil manutenção, no qual somente seria exigida a troca da bateria do sistema periodicamente.

Ele é eletronicamente viável, pois o dispositivo que verifica se o condutor ou proprietário está presente ou não durante a utilização do veículo é simples, eficiente e apresenta boa precisão.

A viabilidade financeira é verificada quando notamos que o custo do sistema mesmo na versão final não seria um custo significativo dentre o custo de um automóvel, portanto viável de ser implementado.

Os próximos passos na elaboração deste sistema seriam a miniaturização dos módulos do sistema que deve ser portado pelo proprietário, para que este possa sem embarcado em dispositivos menores, como relógios ou controles de portão por exemplo.

As melhorias que são necessárias para o sistema se referem a parte de controle de erros do sistema, sendo necessário o aprimoramento do programa e a instalação de sensores no veículo. Com isso pode-se ter um sistema mais seguro e preciso.

Outras aplicações do sistema seriam possíveis em operações que demandem a autenticação do usuário nas proximidades de operação do sistema.

Alguns exemplos práticos da aplicabilidade podem ser, automação de portões eletrônicos e abertura de portas, aonde o usuário é autenticado a distância sem a necessidade de interação.

7. REFERÊNCIAS

[1] **HAYKIN**, Simon, Communication Systems (4th edition) –Editora Wiley.

[2] **TANENBAUM**, Andrew S., Redes de Computadores (4ª edição) – Editora Campus.

[3] **EE TIMES**, EE Times: Covering the basics, 2002.
URL: http://www.eet.com/in_focus/communications/OEG20020201S0035

[4] **MODULAÇÃO**, Modulação, 2004
URL: http://www.gta.ufrj.br/grad/04_2/Modulacao/index.html

[5] **LAIPAC**, Laipac Technology Inc, 2005.
URL: http://www.laipac.com

[6] **ERIC**, Eric's Crypto Software, 2003.
URL: http://www.brouhaha.com/~eric/crypto

[7] **SLACKWAREZINE**. Slackwarezine Linux, 2005.
URL: http://www.slackwarezine.com.br/download/evento/cripto.pdf

[8] **NITS**, CSRC Cryptographic Toolkit, 2001.
URL: http://csrc.nist.gov/encryption/aes/

[9] **MICROCHIP**. Microchip Technology, 2006.
URL: http://www.microchip.com

[10] **SASCAR**. Sascar, 2006.
URL: http://www.sascar.com.br

[11] **SMART-CALL**,Smart-Call,
URL: http://www.sitengenharia.com.br/smart-call.htm

[12] **SLOTZ**, Lothar. Low-Voltage-Programming Cable.
URL: http://home.vrweb.de/~lotharstolz/stolz.de.be/lvpc/index.html

[13] **ANGEL**, Jose de Jesus. AES - Advanced Encryption Standard, 2005.
URL: http://csrc.nist.gov/publications