Processamento criptográfico em microcontroladores de 8 bits

FEUP
Universidade do Porto
Faculdade de Engenharia

http://www.fe.up.pt/~ee99043/aes

Este projecto consistiu na implementação da cifra AES *(Advanced Encryption Standard)* num microcontrolador de 8 bits. AES é baseada na cifra de bloco *Rijndael* e foi designada como sendo a sucessora da cifra DES *(Data Encryption Standard)*, que tem sido implementada em diversos módulos, por todo o mundo, desde 1977.

A Cifra AES

AES é uma cifra de bloco, de chave simétrica, com tamanho de blocos de 128, 192 e 256 bits e com uma chave de 128 bits.
Tem como características principais a resistência contra todos os ataques conhecidos, a velocidade de execução para diversas plataformas e um design relativamente simples.
Graficamente a cifra AES é representada pela Fig. 1.

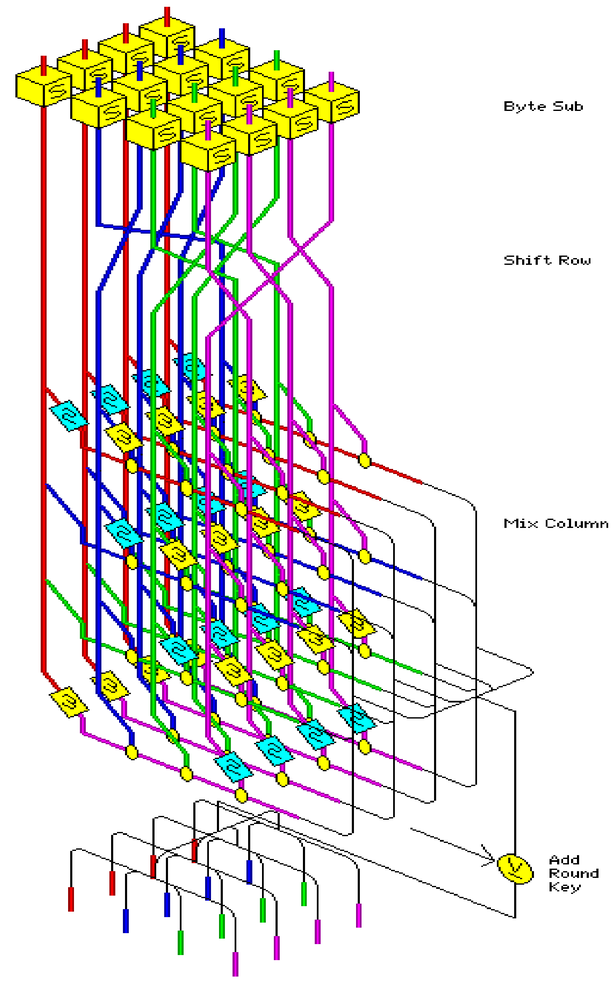

Figura 1: A estrutura da cifra AES.

Implementação

A implementação efectuada está conforme o standard (Ver Fig. 2 e 3), e é completamente funcional, sendo facilmente integrada noutras aplicações.
É assim facilitada a transição de comunicações (ou outras aplicações) de texto simples para texto cifrado.
Foi integralmente desenvolvida na linguagem C e, sem optimizações, ocupa cerca de 3Kb de código, correspondendo a um tempo de execução médio de 340ms no microcontrolador utilizado.

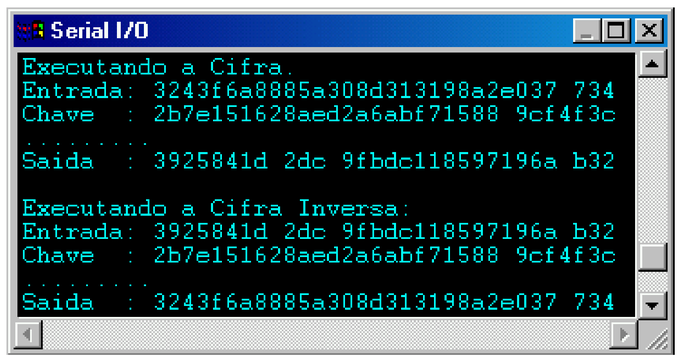

Figura 2: A cifra (no modo directo e inverso) em funcionamento.

Aplicação

Uma das várias aplicações da cifra é a comunicação segura entre dois canais (Ver Fig. 4).
Como é demonstrado, consegue-se assim a transmissão de dados em que apenas as partes intervenientes, conhecedoras da chave utilizada, conseguem reconhecer o conteúdo da comunicação.
É actualmente impossível (e estima-se que continue assim durante vários anos) para uma terceira parte, reconhecer qualquer pedaço dos dados transmitidos.

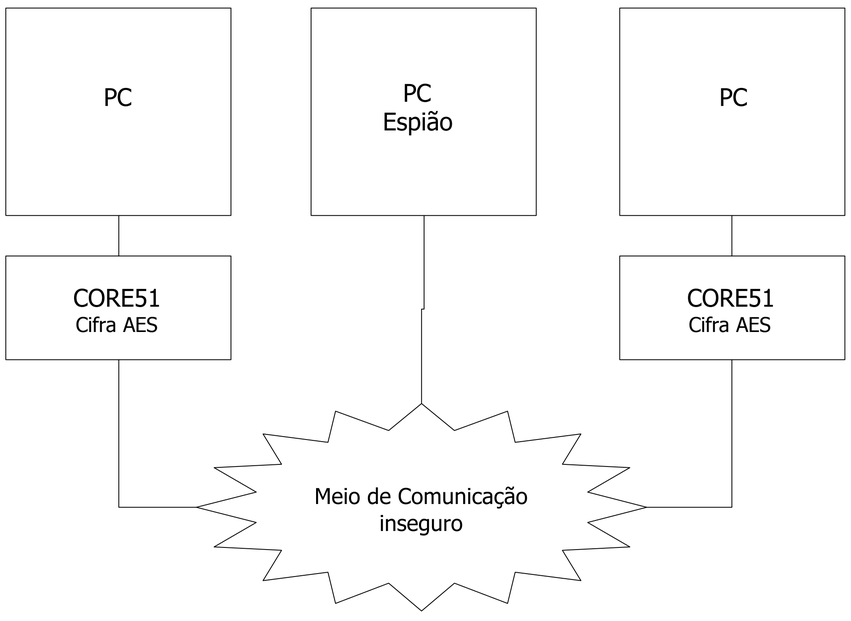

Figura 4: Possível Aplicação

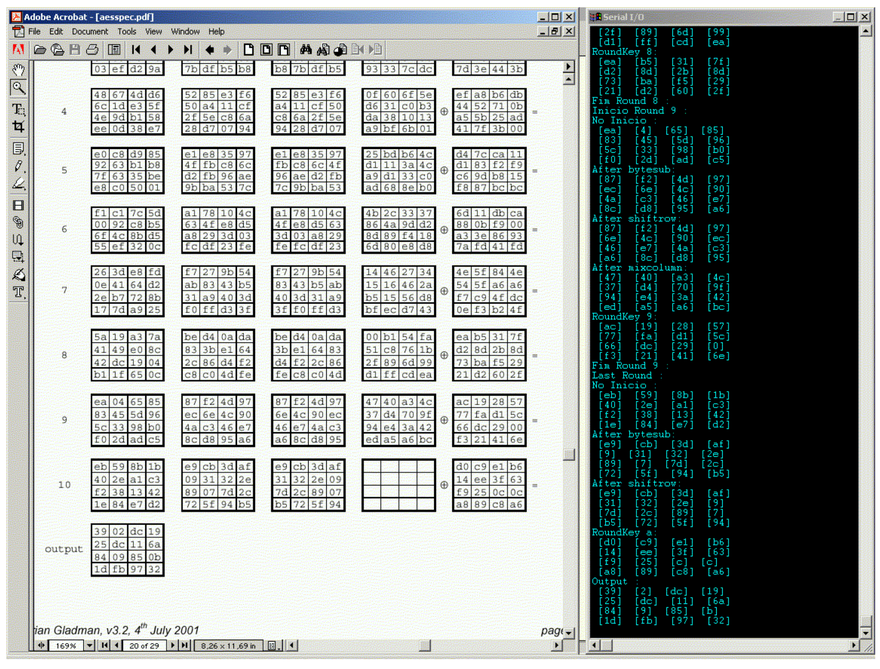

Figura 3: Passos intermédios da execução da cifra, e sua comparação com o standard.

Conhecimentos Adquiridos

Com este projecto reforcei os meus conhecimentos no desenvolvimento de aplicações para sistemas embutidos dada a complexidade da cifra e a limitação de recursos do microcontrolador. A utilização de linguagens de alto nível e a utilização de um sistema de controlo de versões (Ver Fig. 5) mostrou-se essencial para a organização de todo o código gerado.
Para a conclusão dos objectivos deste projecto, foi essencial um conhecimento claro da família de microcontroladores em questão, a placa de desenvolvimento e também do ambiente de desenvolvimento utilizado.
Os conhecimentos a nível de criptografia foram também melhorados, dado que, para a correcta implementação e para o posterior estudo da cifra, foi necessário um conhecimento aprofundado da operação da cifra, seus modos de funcionamento e particulariedades. Conceitos relativos à criptografia em geral e a esta cifra em particular tiveram de ser adquiridos.

Futuras Evoluções

A implementação efectuada é completamente funcional.
O código é modular sendo apropriada a sua utilização em outras aplicações.
A operação de cifra e de cifra inversa, por si só, tem uma aplicação prática reduzida.
É na interligação da cifra efectuada com as diversas aplicações que a implementação efectuada encontra o seu futuro.

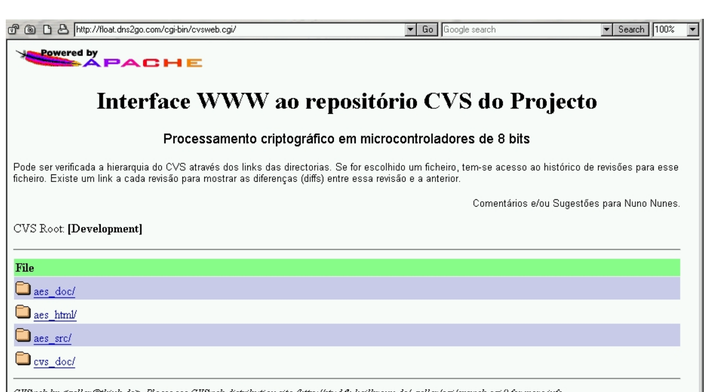

Figura 5: Interface ao sistema de controlo de versões utilizado.

Projecto realizado por Nuno Manuel Cabral Nunes, sob a orientação do Prof. Dr. João Paulo Sousa, no âmbito da disciplina de Projecto Final de Curso, no ano lectivo de 2001/2002.