ESTUDO E IMPLEMENTAÇÃO DE ALGORITMOS CRIPTOGRÁFICOS PARA MICROCONTROLADORES DA FAMÍLIA MSP430

Plínio Pierry Borges Mota[1] e Dr. José Luiz de Freitas Júnior (Orientador)[2]
Núcleo de Pesquisa em Computação – Departamento de Computação
Universidade Católica de Goiás

Este trabalho apresenta o estudo, implementação e aplicação de algoritmos criptográficos tradicionais, Stream Cipher e AES, em microcontroladores da família MSP430. Tais algoritmos foram adequados para a arquitetura específica dos microcontroladores, levando em consideração os recursos escassos desses tipos de componentes eletrônicos, visando aplicações seguras e práticas. Como fonte de dados para cifragem, foi utilizado um circuito de aquisição de ECG (eletrocardiograma). Os dados obtidos desse circuito foram cifrados e decifrados com quantidades de variações, ou pontos de ECG, no melhor e pior caso, para avaliar o tempo gasto com a segurança de tais dados em condições extremas de coleta de dados. Os dados ou sinais coletados no paciente, através de sensores, são convertidos de analógico para digital em um conversor AD de 12 bits. Após esta conversão, são enviados para um segundo circuito onde são organizados em estruturas de dados adequadas para posteriormente serem submetidos aos algoritmos implementados. Os algoritmos, por sua vez, cifram os sinais digitais, utilizando-se uma chave secreta, deixando-os totalmente ilegíveis caso sejam interceptados por alguma pessoa não autorizada. Quando tais sinais chegam ao destino, são novamente submetidos aos algoritmos, juntamente com a chave secreta, e assim decifrados, sem perda de fidelidade das informações.

Com esse sistema, torna-se seguro, por exemplo, a implantação de uma rede de sensores sem fio que coletam informações dos pacientes de um hospital, e enviam-nas automaticamente para um computador, celular ou PDA do médico. As informações dos pacientes ficam protegidas pelos algoritmos implementados e, caso sejam interceptadas, não serão interpretadas pelo interceptador.

Palavras Chave: criptografia, AES, Strem Cipher, microcontroladores.

[1] E-mail: Plínio.pierry@gmail.com
[2] E-mail: jluiz@ucg.br