A – 3

CRIPTOGRAFIA ASSIMÉTRICA: ESTUDO, IMPLEMENTAÇÃO E APLICAÇÕES

Renan Rodrigues de Oliveira (Acadêmico), Dr. José Luiz de Freitas Júnior (Orientador).
Curso de Ciência da Computação – Universidade Católica de Goiás
Contato: cmp.renan@gmail.com, jluiz@ucg.br

Criptografia de dados é a ciência do sigilo. Ela pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto legível em um texto ilegível, sendo possível mediante o processo inverso, recuperar as informações originais. Este trabalho teve como objetivo estudar e implementar protocolos criptográficos, utilizando a criptografia assimétrica como principal requisito para que se tornasse possível oferecer importantes serviços de criptografia, como privacidade, integridade, autenticidade e não repúdio. Destaca-se o estudo e implementação dos seguintes algoritmos: AES, SHA-1 e RSA. Com relação às implementações realizadas, destaca-se: implementação da aplicação para cifragem e decifragem de dados utilizando o algoritmo AES, permitindo a seleção de 128, 192 ou 256 bits como tamanho de bloco ou chave, possibilitando a escolha entre os modos de encadeamento de blocos EBC, CBC ou PCBC; implementação da aplicação responsável por gerar e verificar hash e códigos de autenticação de mensagens, permitindo a manipulação de Hash SHA-1, HMAC SHA-1 e MAC AES; implementação da aplicação responsável por gerar números primos, permitindo a escolha do tamanho médio em bits e da quantidade de números primos gerados; implementação da aplicação responsável por gerar chaves RSA; implementação da aplicação para cifragem e decifragem de dados utilizando o algoritmo RSA, onde o processo de decifragem pode ser executado pelo modo originalmente proposto por seus criadores ou pelo método Quisquater-Couvreur; implementação da aplicação responsável por gerar e verificar assinaturas digitais não secretas, utilizando o algoritmo RSA e SHA-1; implementação da aplicação responsável por gerar e verificar assinaturas digitais secretas, utilizando o algoritmo RSA, AES e SHA-1. Todas as aplicações foram desenvolvidas para serem utilizadas em ambiente gráfico do Sistema Operacional GNU Linux. A linguagem escolhida para as implementações foi a Linguagem C, com compilador GNU GCC. Para o desenvolvimento das interfaces em ambiente gráfico, utilizou-se o Glade2 e a biblioteca GTK. Para manipular inteiros de tamanho arbitrário, em aplicações que necessitam utilizar o algoritmo RSA, utilizou-se a biblioteca GMP.

Palavras-chaves: 1) Segurança de Dados; 2) Criptografia; 3) Teoria dos Números