A – 3

CRIPTOGRAFIA: CRIAÇÃO DE UMA APLICAÇÃO CLIENTE-SERVIDOR IMPLEMENTANDO CERTIFICAÇÃO, ASSINATURA DIGITAL E ALGORITMOS CRIPTOGRÁFICOS.

Denis Francis de Oliveira (Acadêmico), Dr. José Luiz de Freitas Júnior (Orientador).
Departamento de Computação – Universidade Católica de Goiás
Contato: denis.engineer@gmail.com, jluiz@ucg.br

A criptografia (do grego kryptos=escondido e grapho=escrita) pode ser entendida como um conjunto de métodos e técnicas para cifrar informações por meio de um algoritmo e uma chave, convertendo um texto original (legível) em um texto cifrado (ilegível) sendo possível, mediante o processo inverso, recuperar as informações originais através de uma chave (privada) e de um algoritmo (público). São objetivos da criptografia garantir: a confidencialidade, a integridade dos dados, a Autenticidade e o não repúdio.
A implementação destes algoritmos foi importante para aprimorar a teoria estudada e confirmar as expectativas em relação ao funcionamento dos mesmos. Dentre estes algoritmos foi dada uma atenção especial para o AES, pois este ser tornou o novo padrão mundial de criptografia a pouquíssimo tempo.
Durante o projeto foram utilizados os algoritmos criptográficos implementados no primeiro ano de iniciação científica para fornecerem serviços de criptografia na comunicação entre o software cliente-servidor implementado, para isso foi estudado e implementado os principais algoritmos de assinatura e certificação digital considerados importantes.
Em uma outra parte do projeto foi adaptado alguns algoritmos simétricos (AES, DES e Stream Cipher) para serem usados em um micro-controlador da *Texas Instruments* como parte de um sistema de aplicação médica (maiores detalhes podem ser vistos no artigo anexo ao relatório final de pesquisa).
A execução dos algoritmos mencionados acima no micro-controlador foi discutida seus resultados foram comparados levando-se em conta a complexidade do algoritmo e sua segurança.

Palavras-chaves: 1) Computação; 2) Redes de Computadores; 3) Segurança; 4) Criptografia