IX congresso interno de iniciação científica da unicamp
27 e 28 de setembro 2001
pibic/cnpq e sae

ALGORITMO DE CRIPTOGRAFIA RIJNDAEL EM AMBIENTES COMPUTACIONAIS RESTRITOS

João Pedro Alves Penteado do Nascimento e Prof. Dr. Marco Aurélio Amaral Henriques (Orientador), Faculdade de Engenharia Elétrica e de Computação - FEEC, UNICAMP.

Com o crescimento da utilização de aparelhos de telefonia celular, *smart-cards* e *pagers* é cada vez mais importante o desenvolvimento de sistemas de criptografia para a proteção das informações transmitidas e recebidas por estes equipamentos. Tais sistemas devem ser capazes de trabalhar eficientemente utilizando os limitados recursos de memória e processamento oferecidos por estes aparelhos e proporcionar um alto grau de proteção contra possíveis tentativas de violação do sigilo das informações. Nos sistemas de criptografia modernos é comum a utilização de técnicas de chave pública (assimétrica) associada a técnicas de chave secreta (simétrica). Um novo padrão de criptografia de chave secreta, chamado Rijndael, foi recentemente adotado pelo NIST/USA e deverá tornar-se o padrão de fato na indústria, por ter um bom nível de segurança, dentre outras qualidades. Este trabalho investigou características de desempenho e consumo de memória de Rijndael para diversas combinações de seus parâmetros. O objetivo foi oferecer subsídios para projetos que pretendam adotar este algoritmo em sistemas de criptografia para equipamentos com recursos limitados. Os resultados mostram que Rijndael pode ter um baixo perfil de consumo de memória com um bom desempenho e poderão orientar projetos de ambientes de segurança mais sofisticados para equipamentos de baixa capacidade computacional.

Criptografia - Ambientes restritos - Algoritmo Rijndael