



Ministério da Educação e do Desporto
Universidade Federal do Ceará
Pró-Reitoria de Graduação

Curso: Engenharia de Teleinformática		Código: 27 e 68	
Modalidade(s): Graduação		Currículo(s): 2009	
Departamento: Engenharia de Teleinformática			
Código	Nome da Disciplina		
TI0101	Introdução à Criptografia		
Pré-Requisitos: TI0056			
Carga Horária		Número de Créditos	Carga Horária Total
Teórica:	(X)	4.0	64
Prática:	()		
Obrigatória () Optativa (X) Eletiva ou Suplementar ()			
Regime da disciplina: Anual() Semestral (X)			
Justificativa: Em um mundo altamente interligado pelas redes de computadores, o tráfego seguro e sigiloso de informações é um desafio. Por exemplo, sistemas de metrô e usinas de energia controlados remotamente por computador, precisam reconhecer, sem falhas, o seu controlador remoto de forma a não permitir que usuários não autorizados tenham acesso a tais sistemas. Por outro lado, a troca de informações sigilosas governamentais, militares ou empresariais, precisam estar protegidas da espionagem de adversários ou inimigos.			
Objetivos: 1. Fornecer ao estudante a compreensão dos principais protocolos criptográficos para segurança e sigilo de informações tais como cifragem, identificação, autenticação, assinatura digital, voto eletrônico e dinheiro eletrônico, bem como a implementação de tais protocolos em hardware dedicado.			
Descrição do Conteúdo: Ementa: Conceitos Matemáticos, Fatoração, Logaritmos discretos, Codificação Criptográfica, Criptografia de Chave Pública, Funções Criptográficas de Hash, Autenticação e Identificação, Assinaturas Digitais, Protocolos Criptográficos, Hardware Especializado em Segurança.			
Programa: 1. Conceitos Matemáticos - Divisibilidade, máximo divisor comum, números primos, fatoração em primos, geração de números primos, grupos, anéis, campos, polinômios, entropia e segurança perfeita, números aleatórios e pseudoaleatórios, testes estatísticos. 2. Fatoração – Divisão por tentativas, método p-1, crivo quadrado. 3. Logaritmos Discretos – Problemas do logaritmos discretos, algoritmos de passos mínimos e passos gigantes de Shanks, algoritmo de Pollard, algoritmo de Pohlig-Hellman. 4. Codificação Criptográfica – criptosistemas simétricos e assimétricos, permutações.			

one-time pad de Vernam, Data Encryption Standard – DES, International Data Encryption Algorithm – IDEA, RC5, RC6.

5. **Criptografia de Chave Pública** – Criptossistema RSA, Diffie-Hellmann, Algoritmo Rabin, codificação criptográfica de El Gamal, curvas elípticas.
6. **Funções Criptográficas de hash** – Funções de hash e funções de compressão, MD4, MD5 e Secure Hash Algorithm – SHA, amplificação de privacidade.
7. **Autenticação e Identificação** – Senhas, senhas descartáveis, identificação de desafio-resposta, protocolo de identificação Fiege, Fiat e Shamir, protocolo de identificação Schnorr.
8. **Assinaturas Digitais** – Assinaturas RSA, assinatura Fiege-Fiat-Shamir, assinatura de El Gamal, algoritmo de assinatura digital (DAS).
9. **Protocolos Criptográficos** – Comprometimento de informações, provas de conhecimento nulo, jogo de par ou ímpar remoto, eleições eletrônicas, dinheiro eletrônico.
10. **Hardware Especializado em Segurança** – Conceito de circuitos programáveis - FPGAs e VHDL, arquitetura e desempenho de criptoprocessadores.

Bibliografia Básica:

1. Introdução à Álgebra, A. Gonçalves IMPA, 2007.
2. Segurança de Dados – Criptografia em Redes de Computadores, R. Terada, Edgard Blüncher, 2000.
3. Introdução à Criptografia, J. A. Buchmann, Berkeley, 2002.
4. Criptografia em Software e Hardware, E. D. Moreno, F. D. Pereira, R. B. Chiaramonte, Novatec, 2005.
5. Cryptography and Network Security – Principles and Practice, William Stallings, 3ª Ed. Prentice Hall, 1998.
6. Criptografia Métodos e Algoritmos, D. B. de Carvalho, Book Express, 2000.