Disciplina MC889: Introdução à Criptografia

Plano de aulas

Mês	Dia	Aula	
Fevereiro	28	1	O que é criptografia
Março	4	2	Revisão de probabilidade. Sigilo perfeito
	6	3	Funções (e permutações) pseudoaleatórias
	11	4	Definições CPA e CCA
	13	5	Modos de operação (com PRF)
	18	6	Construindo PRF: AES (confusão e difusão; corpos)
	20	7	Construindo PRF: AES
	25	8	Criptografia de chave pública (assimétrica)
	27		Grupos e DLP
Abril	1	9	ElGamal (DDH e prova)
	3	10	Algoritmos para o DLP e parâmetros para ElGamal
	8	11	Funções de resumo criptográfico (hash)
	10	12	Funções de resumo criptográfico (hash)
	15	13	**Prova 1**
	17		Sem aula
	22	14	RSA: versão simples (trapdoor function)
	24	15	RSA: PKCS e geração de primos
	29	16	Gerenciamento e distribuição de chaves
Maio	1		Dia Internacional dos Trabalhadores
	6	17	Troca de chaves: protocolo Diffie-Hellman
	8	18	Diffie-Helmman sobre curvas elípticas
	13	19	Assinaturas digitais (RSA-FDH)
	15	20	Assinaturas digitais (baseadas no DLP)
	20	21	Certificados digitais
	22	22	MACs (HMAC, Poly1305)
	27	23	MACs e cifras CCA

	29	24	Secure Shell: OpenSSH
Junho	3	25	Infraestrutura de chave pública
	5	26	Introdução à criptografia pós-quântica
	10	27	Introdução à criptografia pós-quântica
	12	28	Tópicos a serem decididos com a turma
	17		NTNU
	19		NTNU
	24	29	**Seminários**
	26	30	**Seminários**
Julho	1	31	**Seminários**
	3		Semana de estudos para exame
	8		Semana de estudos para exame
	13	32	**Exame**

Horários e sala

Segundas e quartas, das 08 às 10h, sala CC53

Critérios de avaliação

Uma prova, listas de exercício e um projeto (com apresentação)

L = média das lista		
P = prova		
S = seminário		
M = média pré rec		M := 0.2*L + 0.4*P + 0.4*S
Média final:	se 2.5 <= M < 5:	MAX(MIN(REC, 5), M)
	cc: M	

Observações

Fraudes nas provas ou listas (incluindo plágio) implicarão em média final igual a ZERO	
Não haverá listas ou provas substitutivas	
Bibliografia	
2021 - Katz and Lindell - Introduction To Modern Cryptography	
2019 - Stinson and Paterson - Cryptography: Theory And Practice	
2014 - Hoffstein, Pipher and Silverman - An Introduction to Mathematical Cryptography	
2010 - Christof Paar - Understanding Cryptography	