



Plano de Ensino

Universidade Federal do Espírito Santo

Pólo Universitário de São Mateus

Curso: Ciência da Computação - São Mateus

Departamento Responsável: Departamento de Computação e Eletrônica

Data de Aprovação (Art. nº 91): 03/11/2021

DOCENTE PRINCIPAL : GUILHERME FERNANDES DE SOUZA MIGUEL

Matrícula: 1086148

Qualificação / link para o Currículo Lattes: <http://lattes.cnpq.br/4318918422918138>

Disciplina: TÓPICOS ESPECIAIS EM REDES DE COMPUTADORES I

Código: DCE08455

Período: 2021 / 2

Turma: 3704

Carga Horária Semestral: 60

Distribuição da Carga Horária Semestral

Créditos: 4	Teórica	Exercício	Laboratório
	60	0	0

Ementa:

Objetivos Específicos:

Conteúdo Programático:

- 1 - Introdução à criptografia e segurança de dados
- 2 - Cifras de fluxo
- 3 - O Data Encryption Standart (DES) e seus alternativos
- 4 - O Advanced Encryption Standart (AES)
- 5 - variações dos algoritmos de criptografia de bloco
- 6 - Introdução à criptografia de chave público privada
- 7 - Sistemas de criptografia RSA
- 8 - Problemas de sistemas de criptografia baseados em logaritmos discretos
- 9 - Assinaturas digitais
- 10 - Funções HASH
- 11 - Message Authentication Codes (MAC)
- 12 - Criação de chaves

Metodologia:

1. Metodologias a serem adotadas:

A disciplina será ministrada através de aulas teóricas utilizando o ambiente de aprendizagem Google Classroom como plataforma de aprendizagem e ambiente de construção de conhecimento coletivo. Alunos e professores utilizarão fóruns, chats e conferências web para trocarem opiniões e dúvidas sobre os conteúdos ministrados. A cada semana será proposto um encontro síncrono para realização de tarefas e esclarecimento de dúvidas a respeito do conteúdo passado.

As linguagens C/C++, JAVA, Java Script e Python serão adotadas para implementação dos algoritmos de criptografia e suas variantes. Os alunos realizarão aulas de laboratórios virtuais, utilizando o compiladores, interpretadores etc.

O aluno poderá implementar e testar os algoritmos estudados através de roteiros oferecidos pelo professor, em casa no próprio computador.

2. Recursos de ensino:

Será disponibilizado para o aluno na plataforma classroom: textos, áudios, vídeos entre outros. Esses recursos servirão de base ou de apoio para atingir o objetivo da disciplina. As aulas síncronas utilizarão a plataforma meet da google. As aulas práticas (de laboratório virtual) utilizarão o compiladores, interpretadores e o ambiente de desenvolvimento integrado de código aberto e multiplataforma Code::Blocks

Crítérios / Processo de avaliação da Aprendizagem :

A avaliação parcial da disciplina será composta por oito atividades avaliativas (A1 a A4). A Média Parcial (MP) será a média aritmética das notas das atividades.

$$MP = (A1 + A2 + A3 + A4)/4$$

Os alunos com média parcial do semestre (MP) igual ou superior a 7,0 (sete) e com frequência regimental mínima serão automaticamente aprovados. Caso contrário, o aluno executará uma prova final (PF) não presencial. Essa prova abordará

todo o conteúdo ministrado da disciplina ao longo do período letivo.

A média final (MF) será calculada da seguinte forma:

$$MF = (MP + PF)/2.$$

Os alunos com média igual ou superior a 5,0 (cinco) serão aprovados.

Bibliografia básica:

Bibliografia complementar:

Cronograma:

Aula	Data	Descrição	Exercícios	Observações
01	03/11/2021	Introdução à disciplina		
02	05/11/2021	Introdução à criptografia e segurança de dados: Criptografia simétrica, Criptoanálise		
03	10/11/2021	Introdução à criptografia e segurança de dados: Aritmética modular e outras cifras históricas		
04	12/11/2021	Cifra de fluxo: Introdução, Geração de números Randômicos		
05	17/11/2021	Cifras baseadas em deslocamento de registradores.		
06	19/11/2021	Trabalho 1		
07	24/11/2021	Introdução ao Data Encryption Standart (DES)		
08	26/11/2021	Estrutura interna do DES		
09	01/12/2021	Alternativas ao DES		
10	03/12/2021	O Advanced Eryption Standart		
11	08/12/2021	Estrutura interna no AES		
12	10/12/2021	Mais sobre criptografia de blocos		
13	15/12/2021	Mais sobre criptografia de blocos		
14	17/12/2021	Trabalho II		
15	26/01/2022	Introdução à criptografia de chave pública		
16	28/01/2022	Introdução à criptografia de chave pública		
17	02/02/2022	Sistema de criptografia RSA		
18	04/02/2022	Sistema de criptografia RSA		
19	09/02/2022	Sistemas de criptografia baseados no problema do logaritmos discreto		
20	11/02/2022	Trabalho III		
21	16/02/2022	Assinaturas Digitais		
22	18/02/2022	Assinaturas Digitais		
23	23/02/2022	Funções Hash		
24	25/02/2022	Funções Hash		
25	09/03/2022	Códigos de autenticação de Mensagens		
26	11/03/2022	Códigos de autenticação de mensagens		
27	16/03/2022	Criação de Chaves		
28	18/03/2022	Criação de chaves		

Aula	Data	Descrição	Exercícios	Observações
29	23/03/2022	Criação de Chaves		
30	25/03/2022	Trabalho IV		

Observação:



UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

PROTOCOLO DE ASSINATURA



O documento acima foi assinado digitalmente com senha eletrônica através do Protocolo Web, conforme Portaria UFES nº 1.269 de 30/08/2018, por
MARCUS VINICIUS DE ALMEIDA - SIAPE 1993319
Departamento de Computação e Eletrônica - DCE/CEUNES
Em 27/04/2022 às 11:13

Para verificar as assinaturas e visualizar o documento original acesse o link:
<https://api.lepisma.ufes.br/arquivos-assinados/457024?tipoArquivo=O>