Plano de Ensino – Atividades Remotas Emergenciais – 2020/1

Código	DCC 030 Turma B / DCC 049 Turma B / DCC 831 PG 8
Disciplina	Criptografia Teórica
Turma	
Professor	Jeroen van de Graaf

Ementa

Criptografia é a ciência de comunicação e computação confiável na presença de partes maliciosas. Esta área proporciona propriedades básicas de segurança, como o sigilo, a integridade e a irretratabilidade de dados e transações. A criptografia tem um papel imprescindível, posto que é a única técnica que propicia segurança e privacidade quando o canal de comunicação é aberto - Internet e canais sem fio, por exemplo. Os objetivos principais desta disciplina são:

-- estudar os princípios e primitivas básicas da criptografia

-- estudar os princípios matemáticas por tras

-- estudar como, com rigor matemático, é possível provar a segurança de algoritmos e protocolos matemáticos.

-- em particular, fornecer ao aluno formas de se distinguir entre segurança incondicional, segurança computacional e segurança ad-hoc.

Programa

Aula	**Data**	**Conteúdo previsto**	**Modalidade**	**Interação**
1	03 / 03	Introdução	Presencial	Presencial
2	05 / 03	Cap 1 K&L – historia criptografia	Presencial	Presencial
3	10 / 03	Cap 2 K&L – one-time pad	Presencial	Presencial
4	12 / 03	Cap 2 K&L – one-time pad	Presencial	Presencial
5	**04 / 08**	Revisão objetivos disciplina, Cap 2 K&L	Síncrona, Interativa	Interação, whatsapp, moodle
6	06 / 08	continuação livro de K&L	idem	idem
7	11 / 08	idem	idem	idem
8	13 / 08	idem	idem	idem
9	18 / 08	idem	idem	idem
10	20 / 08	idem	idem	idem
11	25 / 08	idem	idem	idem
12	27 / 08	idem	idem	idem
13	01 / 09	idem	idem	idem
14	03 / 09	idem	idem	idem
15	**08 / 09**	P1	idem	idem
16	10 / 09	continuação livro de K&L	idem	idem
17	15 / 09	idem	idem	idem
18	17 / 09	idem	idem	idem
19	22 /09	idem	idem	idem
20	24 / 09	idem	idem	idem
21	29 / 09	idem	idem	idem
22	01 / 10	idem	idem	idem
23	06 / 10	idem	idem	idem
24	08 / 10	idem	idem	idem
25	13 / 10	aulas alunos	idem	idem

26	15 / 10	aulas alunos	idem	idem
27	20 / 10	aulas alunos	idem	idem
28	22 / 10	aulas alunos	idem	idem
29	27 / 10	P2	idem	idem
30	29 / 10	fechamento disciplina	idem	idem

Bibliografia
Katz&Lindell, Introduction to Modern cryptography, 2nd edition

Material de apoio
Moodle e Googledocs (slides e outros materiais)
Youtube (para guardar os vídeos)

Avaliações

1	P1: prova escrita	15 pontos	08 / 09
2	P2: prova escrita	20 pontos	27 / 10
3	Lista de exercícios semanais	50 pontos	Semanal
4	Aula: cada aluno deve apresentar uma aula de 40-50 minutos focando em um técnico criptográfico	15 pontos	Meados de outuro
5			

Observações:

- A disciplina tem um formato bastante matemático, i.e. “giz e quadro”. Na modalidade online a intenção é copiar esse formato no máximo possível, fazendo aulas expositivas usando um quadro branco, permitindo interação contínua com os alunos.
- O foco da avaliação são os exercícios. As provas servem para confirmar o conhecimento obtido pelas listas.
- Nas provas escritas o aluno tira foto das suas respostas e envia ao Moodle
- As perguntas das provas e das listas serão discutidos no formato de reunião virtual.
- O professor pode optar por fazer entrevistas complementares online sobre as perguntas das provas e das listas para avaliar o conhecimento do aluno.

Definições

Modalidade: tipo de atividade didática, sempre remota. Exemplos: reunião virtual, video, exercícios, avaliação.

Interação: forma de interação prevista para exposição de conteúdo, discussões, esclarecimento de dúvidas, promoção de debates, resolução de exercícios.

Videos (aulas): conteúdo expositivo preparado em vídeo, com utilização dos slides disponíveis e outros recursos. Tópicos serão divididos em vários vídeos curtos para melhor acompanhamento e para facilitar a produção.

Reunião virtual: Reunião virtual no horário de aula, para discussões e esclarecimento de dúvidas.