MCZB015-13 Introdução à Criptografia 2023 Q3

Geral

Característica do curso -- **IMPORTANTÍSSIMO, LEIAM!**

ESTE NÃO É UM CURSO PRÁTICO / APLICADO, a não ser por uma única atividade, que não é obrigatória! É um curso para tratar de como se desenvovle Criptografia: tomamos objetos matemáticos, mostramos que servem a propósitos da Criptografia, e demonstramos teoremas sobre eles (que são seguros de acordo com certos parâmetros etc). Deverá haver um único momento do curso em que haverá alguma implementação, quando tratarmos de Criptanálise, mas não é o modo como o resto do curso se dará.

Os cursos que abordam os aspectos concretos e aplicados da Criptografia são, por exemplo, "Segurança de Dados" e "Segurança em Redes" -- e nestes, a Criptografia não é ponto central, estando inserida em um contexto mais amplo.

Aulas

Sala **S-301-2**

- 3ª 21:00 -- 23:00
- 6ª 19:30 -- 21:00

Atendimento (horário para dúvidas)

- 3ª 20:30 -- 21:00
- 6ª 18:30 -- 19:00

Forma de comunicação com o professor

- Pelo Moodle
- Pelo email institucional (jeronimo.pellegrini@ufabc.edu.br)

Período

De 19/09 a 08/12

Reposições previstas no calendário:

- 13 de outubro (sexta-feira) para 12 de dezembro (terça-feira)
- 03 de novembro (sexta-feira) para 15 de dezembro (sexta-feira)

No dia 12/12 não haverá novos tópicos, mas discussão dos trabalhos e resolução de dúvidas pendentes.
No dia 15/12 será aplicada a prova substitutiva.

Recomendações

PERGUNTE! PEÇA QUE EU EXPLIQUE NOVAMENTE! NÃO DEIXE SUAS DÚVIDAS SE ACUMULAREM!

Não creia que poderá sanar as dúvidas uma semana antes da prova ou da entrega do trabalho!
O conteúdo inclui conceitos abstratos e maneiras diferentes de raciocinar.
Isso significa que esforço não basta -- você precisa de ***TEMPO*** e ***NOITES DE SONO*** para absorver e digerir as ideias, e tentar condensar isso em uma semana não funciona!

EMENTA

Geradores pseudoaleatóreos. Cifras de fluxo. Cifras de bloco simétricas e modos de operação. Resumos criptográficos. Teoria dos Números e criptografia assimétrica. Autenticação de mensagens. Assinaturas digitais. Protocolos criptográficos.

PROGRAMA

- O programa ***NÃO*** está dividido em "semanas", mas em tópicos. Alguns podem demorar mais ou demorar menos, dependendo de diversos fatores que não há como prever (como por exemplo dificuldades específicas da turma em dados momentos).
- **PARA DISCENTES DE MATEMÁTICA** - ou que tem muita afinidade com matemática: se quiserem se adiantar, estudem Complexidade de Algoritmos (Apêndice C das notas de aula)
- **PARA DISCENTES DE COMPUTAÇÃO** - ou que tem muita afinidade com Computação: se quiserem se adiantar, estudem um pouco de Álgebra (Apêndice B das notas de aula)

Manterei um indicador aqui, mostrando (i) o que já foi visto, e que material foi usado; (ii) qual o próximo tópico a ser trabalhado, e que material usaremos.

1. Visão geral dos problemas abordados pela Criptografia ⟵ **PRÓXIMA AULA** (Notas de aula, cap. 1)
2. Criptossistemas e noções de segurança
3. Noções de complexidade de algoritmos
4. Sigilo perfeito e o teorema de Shannon
5. Funções de mão única e Criptografia Pós-Quântica
6. Geradores pseudoaleatóreos e cifras de fluxo
7. Funções pseudoaleatóreas e cifras de bloco
8. Noções de Criptanálise
9. Resumos criptográficos (hashing)
10. MAC (autenticação de mensagens)
11. Cifras assimétricas
12. Assinaturas digitais
13. Protocolos com dois participantes
14. Provas de conhecimento zero
15. Autenticação de entidades (identificação)
16. Compartilhamento de segredos

AVALIAÇÃO

Teremos:

- Duas provas, P_1 e P_2, valendo 4 pontos cada
- Um trabalho prático, T, valendo 2 pontos

As notas são **INTEIRAS**.

Datas das provas:

- P_1: 31/10
- P_2: 05/12
- SUB: 15/12

Critérios para avaliação nas provas: Clareza, corretude, rigor, e concisão (i) A redação das respostas deve ser clara. (ii) Todo o raciocínio desenvolvido na resposta deve estar correto. (iii) O nível de rigor nas respostas deve ser próximo ao usado nas notas de aula e bibliografia básica. (iv) As respostas não devem ser mais longas que o necessário.
Critérios para avaliação do trabalho: o trabalho de Criptanálise será feito em grupo (máximo 4 participantes), e envolverá: (1) a criação de uma cifra de bloco bem simples, e (2) a quebra de cifra de outro grupo. Cada tarefa vale um ponto.

Seja $N = P1 + P2 + T$. O conceito final será:

- $N \in [0, 5) \rightarrow$ F
- $N \in [5, 7) \rightarrow$ C
- $N \in [7, 8) \rightarrow$ B
- $N \in [8, 9] \rightarrow$ A
- $N = 10 \rightarrow$ A com flores, estrelas e aroma de baunilha

(Vejam que a criação da cifra resume-se a sua ***descrição*** apenas, e que portanto ***não é necessário implementar absolutamente nada para passar com A***. Mas eu tentaria!)

Vista e Revisão de Provas

Haverá oportunidade para vista e revisão de provas, conforme resolução ConsEPE 120.

Prova substitutiva

Somente para os casos previstos em lei e na resolução 181 do ConsEPE!
Caso o aluno perca uma das provas e apresente justificativa, poderá fazer uma substitutiva no final do quadrimestre.

Exame

Para alunos com F (sobre o exame, veja a resolução 182 do ConsEPE). O exame será realizado no próximo quadrimestre.
A nota final será $0.6n + 0.4e$, onde n é a nota dos testes e e é a nota do exame.

BIBLIOGRAFIA BÁSICA

- Notas de aula
- **KATZ, J.; LINDELL, Y.** Introduction to Modern Cryptography.Boca Raton: Chapman&Hall/CRC, 2008.
- **ROGAWAY, P.** The Moral Character of Cryptographic Work.

BIBLIOGRAFIA COMPLEMENTAR

- **BALDONI, M.; CILIBERTO, C.; CATTANEO, G.** Elementary Number Theory, Cryptography and Codes. Berlin-Heidelberg: Springer-Verlag, 2009.
- **BARAKAT, M.; EDER, C.; HANKE, T.** An Introduction to Cryptography, 2018.
- **BERNSTEIN, D.; BUCHMANN, J.; DAHMEN, E.** Post-Quantum Cryptography. Berlin-Heidelberg: Springer-Verlag, 2009.
- **BONEH, D. SHOUP, V. A. A Graduate Course in Cryptography Livro disponível livremente: https://toc.cryptobook.us/**
- **CATALANO, D.** et al. Contemporary Cryptology.Basel: Birkhäuser, 2005.
- **GOLDREICH, O.** Fundamentals of Cryptography, v. I: Basic Tools. Cambridge: Cambridge University Press, 2001.
- **GOLDREICH, O.** Fundamentals of Cryptography, v. II: Basic Applications. Cambridge: Cambridge University Press, 2004.
- **HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. H.** An Introduction to Mathematical Cryptography. New York: Springer-Verlag, 2008.
- **SHOUP, V. A.** Computational Introduction to Number Theory and Algebra.Cambridge: Cambridge University Press, 2005.
- **STINSON, D.** Cryptography: theory and practice. Boca Raton: Chapman&Hall/CRC, 2006.

BIBLIOGRAFIA - ASSUNTOS CORRELATOS

- **CORMEN, L.; RIVEST, S.** Algoritmos-Teoria e Prática. Rio de Janeiro: Campus, 2002.
- **DASGUPTA, S.; PAPADIMITRIOU, C. H.; VAZIRANI, U. V.** Algoritmos.Porto Alegre: McGraw-Hill/Artmed, 2009.
- **SIPSER, M.** Introdução à Teoria da Computação. São Paulo: Thomson Learning, 2007

Avisos

Contato

Av. dos Estados, 5001. Bairro Bangu - Santo André /SP – Brasil. CEP 09210-580.

Siga-nos

Português - Brasil (pt_br)
- English (en)
- Português - Brasil (pt_br)

Obter o aplicativo para dispositivos móveis