UNIVERSIDADE FEDERAL DO ABC - PLANO DE ENSINO E DE AULA

Disciplina: MCZB015-13 – Introdução à criptografia
Turma: TNA1MCZB015-13SA
Carga horária: 4-0-4
Horário: 3ª feira – das 21h às 23h; 5ª feira – das 19h às 21h.
Sala: S-302-1
Quadrimestre: 2022.3
Professora: Sara Díaz Cardell (CMCC)
email: s.cardell@ufabc.edu.br

EMENTA

Criptografia clássica. Criptografia simétrica. Geradores pseudoaleatórios. Cifras de fluxo. Cifras de bloco simétricas. Resumos criptográficos. Criptografia assimétrica. Autenticação de mensagens. Assinaturas digitais. Protocolos criptográficos.

OBJETIVOS

Objetivos gerais:
Entender a diferença entre criptografia simétrica e assimétrica.
Entender as principais diferenças entre cifradores de fluxo e cifradores de bloco.
Conhecer os principais algoritmos da criptografia assimétrica e simétrica
Conhecer os conceitos de assinatura digital e resumo criptográfico.

Objetivos específicos:
Cifrar e decifrar mensagens com cifradores assimétricos.
Assinar mensagens digitalmente com criptografia assimétrica.
Entender o funcionamento interno de algoritmos simétricos de bloco: DES, AES.
Conhecer as propriedades de uma sequência criptográfica.
Conhecer o conceito de resumo criptográfico.
Entender as bases da segurança de cada algoritmo.

METODOLOGIA

O conteúdo teórico será ministrado em aulas presenciais através de presentações em beamer.
Serão distribuidas listas de exercícios que os /as estudantes deverão resolver em casa. A professora dedicará um tempo cada semana a resolver os exercícios solicitados pelos alunos/as.

AVALIAÇÃO

Haverá duas provas presencias e 4 atividades de avaliação curtas.
O conceito final será calculado a partir de uma média final numérica (Média) calculada como:

$$\text{Média} = 0{,}4\, P_1 + 0{,}5\, P_2 + A,$$

onde P_1, P_2 serão avaliadas de 0 a 10 e são definidas como

- P_1: Prova 1 (Conteúdo até semana 5),
- P_2: Prova 2 (Conteúdo a partir da semana 6),

e A corresponde à nota das atividades de avaliação (máximo 1 ponto, 0,25 pontos cada atividade).

Haverá 1 (uma) avaliação substitutiva, segunda chamada, para aqueles/as que faltarem ao exame final com justificativa (a ser entregue até uma semana depois do dia da prova).

As notas serão convertidas em conceitos conforme segue abaixo:

- A (8,75 - 10) - Desempenho excepcional, demonstrando excelente compreensão da disciplina.
- B (7 - 8,74) - Bom desempenho, demonstrando boa capacidade de uso dos conceitos da disciplina.
- C (5,26 - 6,9) - Desempenho mínimo satisfatório.
- D (4,75 – 5,25) - Aproveitamento mínimo não satisfatório dos conceitos da disciplina. Nesse caso, o/a aluno a é aprovado/a na expectativa de que obtenha um conceito melhor em outra disciplina, para compensar o conceito D no cálculo do CR.
- F (Abaixo de 4,75) – Reprovado/a.
- O - Reprovado/a por falta (presença inferior a 75%).

Os alunos e alunas com conceito D ou F têm direito à recuperação. Sugere-se que a recuperação seja uma avaliação abordando todo o conteúdo da disciplina.
Para poder fazer a recuperação, o aluno/a deve poder mostrar que participou da disciplina, sendo necessária uma frequência de mínimo 75%.

Pré-Rec	Rec	Final
D	A	C
D	B	C
D	C	C
D	D	D
D	F	D
F	A	C
F	B	C
F	C	D
F	D	F
F	F	F

Datas das avaliações:

P_1: 3 de novembro (Conteúdo até semana 5)
P_2: 8 de dezembro (Conteúdo a partir da semana 6)
Recuperação: 16 de dezembro

Atividade de avaliação 1: 3-10 de outubro
Atividade de avaliação 2: 17-24 de outubro
Atividade de avaliação 3: 7-14 de novembro
Atividade de avaliação 4: 21-28 de novembro

As avaliações (P_i) serão de forma presencial, em forma escrita, e consistirão de resoluções de exercícios e/ou questões e/ou problemas, os quais estarão de acordo com os conteúdos ministrados nas aulas e/ou listas de exercícios.

As atividades de avaliação serão disponibilizadas via Moodle. Cada aluno/a receberá uma ou várias questões a partir de um banco de questões elaborado previamente. Os/as alunos/as terão um período de uma semana em que as questões estarão disponíveis. Após resolver as questões, deverão escaneá-las e enviá-las à professora responsável.
Em nenhum caso, serão aceitas resoluções fora do prazo estabelecido.

CRONOGRAMA

Semana 1 (20-22 de setembro):
Apresentação da disciplina.
Primeiros conceitos (Segurança da informação, esteganografia, criptografia, texto plano, texto cifrado, chave)
Conceitos básicos da matemática para criptografia (arimética modular, algoritmo de Euclides, representação binária, representação hexadecimal, código ASCII)

Semana 2 (27-29 de setembro):
Criptografia clássica: (Revisão histórica dos métodos cripto-gráficos usados ao longo dos séculos)

Semana 3 (4-6 de outubro):
Criptografia simétrica e assimétrica (definição e diferenças entre a criptografia simétrica e a criptografia assimétrica)
Criptografia simétrica (definição e diferenças entre cifra de bloco e cifra em fluxo)
Atividade de avaliação 1

Semana 4 (11-13 de outubro):
Cifras de fluxo (definição e principais algoritmos, LFSRs, PN-sequência, propriedades criptográficas de uma sequência: período, complexidade linear, autocorrelação)

Semana 5 (18-20 de outubro):
Geradores de sequências pseudoaleatórias (geradores baseados em decimação irregular, geradores baseados em uma combinação não linear mediante uma função booleana, LFSRs dinâmicos)
Atividade de avaliação 2

Semana 6 (25-27 outubro):
Cifras de bloco (definição e principais algoritmos: redes de Feistel, DES, AES)

Semana 7 (1-3 de novembro):
Aula de dúvidas (1 novembro) / P1 (3 novembro)

Semana 8 (8-10 de novembro):
Criptografia assimétrica (definição, intercâmbio de chave de Diffie-Hellman, RSA)
Atividade de avaliação 3

Semana 9 (17 de novembro):
Criptografia assimétrica: (ElGamal, Rabin, outros)

Semana 10 (22-24 de novembro):
Assinatura (definição, principais algoritmos: RSA, DSA, ElGamal)
Funções Hash (definição, propriedades, segurança, MD5, SHA-1, SHA-2, SHA-3, SHA-256)
Atividade de avaliação 4

Semana 11 (29 de novembro - 1 de dezembro):
Funções Hash (definição, propriedades, segurança, MD5, SHA-1, SHA-2, SHA-3, SHA-256)
Autenticação (PKI, HMAC, Kerberos)

Semana 12 (6-8 de dezembro):
Aula de dúvidas (dia 6) / P2 (dia 8)

ATENDIMENTO

O atendimento presencial será feito toda quinta feira das 18h às 19h.
Os/as estudantes também poderão resolver dúvidas via email e poderão marcar reuniões virtuais com a professora se assim precisarem (consultar disponibilidade por email).

BIBLIOGRAFIA

- Christof Paar and Jan Pelzl. Understanding Cryptography. A Textbook for Students and Practitioners.
- A. Menezes, P. van Oorschot and S. Vanstone.Handbook of Applied Cryptography.
- KATZ, J.; LINDELL, Y. Introduction to Modern Cryptography. Boca Raton: Chapman&Hall/CRC, 2008.
- MAO, W. Modern Cryptography: theory and practice. Upper Saddle River: Prentice Hall, 2004.
- SANTOS, P. Introdução à Teoria dos Números. Rio de Janeiro: IMPA, 2010.
- STINSON, D. Cryptography: theory and practice. Boca Raton: Chapman&Hall/CRC, 2006.
- TALBOT, J.; WELSH, D. Complexity and Cryptography: an introduction. Cambridge: Cambridge University Press, 2006.
- TRAPPE, W.; WASHINGTON, L. Introduction to Cryptography with coding theory. Upper Saddle River: Prentice Hall, 2006.

BIBLIOGRAFIA COMPLEMENTAR

- Curso online de Chistof Paar: https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg
- ANDREWS, G. Number Theory. New York: Dover Publications, 1994.
- BALDONI, M.; CILIBERTO, C.; CATTANEO, G. Elementary Number Theory, Cryptography and Codes. Berlin-Heidelberg: Springer-Verlag, 2009.
- BERNSTEIN, D.; BUCHMANN, J.; DAHMEN, E. Post-Quantum Cryptography. Berlin-Heidelberg: Springer-Verlag, 2009.
- CATALANO, D. et al. Contemporary Cryptology. Basel: Birkhäuser, 2005.
- 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.
- GOLDREICH, O. Fundamentals of Cryptography, vol. I: Basic Tools. Cambridge: Cambridge University Press, 2001.
- GOLDREICH, O. Fundamentals of Cryptography, vol. 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.
- SIPSER, M. Introdução à Teoria da Computação. São Paulo: Thomson Learning, 2007.