Pró-Reitoria de Graduação

Plano de Ensino – Quadrimestre 2 de 2021

Caracterização da disciplina									
Código da disciplina:	MCZB015-13	Nome da disciplina:	Introdução à criptografia						
Créditos (T-P-I):	(4-0-4)	Carga horária:	48 horas	Aula prática:	0	Campus:	Santo André		
Código da turma:	NAMCZB015-13SA NBMCZB015-13SA	Turma:	-	Turno:	Noturno	Quadrimestre:	2	Ano:	2021
Docente(s) responsável(is):	Sara Díaz Cardell								

Alocação da turma

	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
8:00 - 9:00						
9:00 - 10:00						
10:00 - 11:00						
11:00 - 12:00						
12:00 - 13:00						
13:00 - 14:00						
14:00 - 15:00						
15:00 - 16:00						
16:00 - 17:00						
17:00 - 18:00						
18:00 - 19:00						
19:00 - 20:00		NAMCZB015-13SA			NBMCZB015-13SA	
20:00 - 21:00		NAMCZB015-13SA			NBMCZB015-13SA	
21:00 - 22:00		NBMCZB015-13SA			NAMCZB015-13SA	
22:00 - 23:00		NBMCZB015-13SA			NAMCZB015-13SA	

Planejamento da disciplina

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.

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.

Conteúdo programático

Semana	Conteúdo	Atividades	
Semana 1 25/05/21 28/05/21	**Apresentação da disciplina.** **Conceitos básicos da matemática para criptografia** (arimética modular, algoritmo de Euclides, representação binária, representação hexadecimal, código ASCII) **Primeiros conceitos** (Segurança da informação, esteganografia, criptografia, texto plano, texto cifrado, chave)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	**Aula síncrona:** Aula no Google Meet para apresentar o curso.
		Atividade de avaliação assíncrona: Lista L_1 no Moodle	
Semana 2 01/06/21 04/06/21	**Criptografia clássica:** (Revisão histórica dos métodos criptográficos usados ao longo dos séculos)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	
		Atividade de avaliação assíncrona: Lista L_2 no Moodle	
Semana 3 08/06/21 11/06/21	**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)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	
		Atividade de avaliação assíncrona: Lista L_3 no Moodle	
Semana 4 15/06/21 18/06/21	**Cifras de fluxo** (definição e principais algoritmos, LFSRs, PN-sequência, propriedades criptográficas de uma sequência: período, complexidade linear, autocorrelação)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	
		Atividade de avaliação assíncrona: Lista L_4 no Moodle	
Semana 5 22/06/21 25/06/21	**Geradores de sequências pseudoaleatórias** (geradores baseados em decimação irregular, geradores baseados em uma combinação não linear mediante uma função booleana, LFSRs dinâmicos)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	
		Atividade de avaliação assíncrona: Lista L_5 no Moodle	
Semana 6 29/06/21 02/07/21	**Cifras de bloco** (definição e principais algoritmos: redes de Feistel, DES, AES)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	
		Atividade de avaliação assíncrona: Lista L_6 no Moodle	
Semana 7 06/07/21 09/07/21	**Criptografia assimétrica** (definição, intercâmbio de chave de Diffie-Hellman, RSA)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube.	
		Atividade de avaliação assíncrona: Lista L_7 no Moodle	

Semana 8 13/07/21 16/07/21	**Criptografia assimétrica:** (ElGamal, Rabin, outros)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube. **Atividade de avaliação assíncrona:** Lista L_8 no Moodle
Semana 9 20/07/21 23/07/21	**Funções Hash** (definição, propriedades, segurança, MD5, SHA-1, SHA-2, SHA-3, SHA-256)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube. **Atividade de avaliação assíncrona:** Lista L_9 no Moodle
Semana 10 27/07/21 30/07/21	**Assinatura digital** (definição, principais algoritmos: RSA, DSA, ElGamal)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube. **Atividade de avaliação assíncrona:** Lista L_{10} no Moodle
Semana 11 03/08/21 06/08/21	**Autenticação** (PKI, HMAC, Kerberos) **Revisão da matéria** (resolução de dúvidas e exercícios)	**Aula de teoria assíncrona:** Vídeo-aula disponível no Youtube. **Aula síncrona:** Aula no Google Meet para resolver dúvidas.
Semana 12 10/08/21	**Avaliação de aprendizagem (A)**	**Atividade assíncrona**: Será disponibilizada via Moodle avaliação para todos/as os/as alunos/as com questões abertas. Cada aluno/a receberá uma sequência de questões a partir de um banco de questões elaborado previamente. Todo o processo será gerenciado pelo Moodle. Os/as alunos/as poderão iniciar as avaliações dentro de um período mínimo de 72 horas em que as questões estarão disponíveis. A partir do momento em que comecem a resolver terão até três horas para solucionar as questões. Após a resolução das questões, deverão escaneá-las e enviar à professora responsável.
Semana 13 17/08/21	**Avaliação de aprendizagem recuperação (A_{rec})**	**Atividade assíncrona**: Será disponibilizada via Moodle avaliação para todos/as os/as alunos/as com questões abertas. Cada aluno/a receberá uma sequência de questões a partir de um banco de questões elaborado previamente. Todo o processo será gerenciado pelo Moodle. Os/as alunos/as poderão iniciar as avaliações dentro de um período mínimo de 72 horas em que as questões estarão disponíveis. A partir do momento em que comecem a resolver terão até três horas para solucionar as questões. Após a resolução das questões, deverão escaneá-las e enviar à professora responsável.

Descrição dos instrumentos e critérios de avaliação qualitativa

A avaliação (A), na forma escrita, consistirá em 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.

Será realizada durante o curso, 1 (uma) avaliação e 10 listas de exercícios semanais do moodle.

O conceito final será calculado a partir de uma média final numérica (Média) calculada como:

Média = 0,7 A + 0,3L_{Moodle},

onde A e L_{Moodle} serão avaliadas de 0 a 10 e são definidas como:

• A: Conteúdo completo.
• L_{Moodle}: Listas semanais do Moodle com um ou vários exercícios personalizados para cada estudante.

Em nenhum caso, serão aceitas resoluções fora do prazo estabelecido.

Haverá 1 (uma) avaliação substitutiva (A_{SUB}), segunda chamada, para aqueles que faltarem à prova A com justificativa (a ser entregue no dia da prova), conforme as normas da Universidade.

As notas serão convertidas em conceitos, conforme regulamento oficial da universidade. A conversão de conceitos segue abaixo:

- A (8,5 - 10) - Desempenho excepcional, demonstrando excelente compreensão da disciplina.
- B (7 - 8,4) - Bom desempenho, demonstrando boa capacidade de uso dos conceitos da disciplina.
- C (6,0 - 6,9) - Desempenho mínimo satisfatório.
- D (5,0 – 5,9) - Aproveitamento mínimo não satisfatório dos conceitos da disciplina. Nesse caso, o aluno é aprovado na expectativa de que obtenha um conceito melhor em outra disciplina, para compensar o conceito D no cálculo do CR.
- F (Abaixo de 5,0) - Reprovado.
- O - Reprovado por falta (presença inferior a 75%). Não aplicável neste quadrimestre.

Os alunos e alunas com conceito D ou F têm direito à recuperação (A_{REC}). Sugere-se que a recuperação seja uma avaliação abordando todo o conteúdo da disciplina.
Para poder fazer a A_{REC}, o aluno/a deve poder mostrar que participou da disciplina sendo necessário um mínimo de nota 3 na Pré-Rec.

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

Cronograma das avaliações:

Início: 28/05/2021 – L_{Moodle} 1 (Preliminares)
Início: 04/06/2021 – L_{Moodle} 2 (Criptografia clássica)
Início: 11/06/2021 – L_{Moodle} 3 (Criptografia simétrica)
Início: 18/06/2021 – L_{Moodle} 4 (LFSRs)
Início: 25/06/2021 – L_{Moodle} 5 (Geradores fluxo)
Início: 02/07/2021 – L_{Moodle} 6 (Bloco)
Início: 09/07/2021 – L_{Moodle} 7 (RSA,DH)
Início: 16/07/2021 – L_{Moodle} 8 (ElGamal, Rabin, outros)
Início: 23/07/2021 – L_{Moodle} 9 (Hash)
Início: 30/07/2021 – L_{Moodle} 10 (Assinatura digital)
Início: 10/08/2021 - A – Avaliação
Início: 17/08/2021 - A_{REC}– Avaliação (recuperação)

Obs.: A A_{SUB} - Segunda Chamada será realizada em data a ser confirmada com os alunos/as que porventura não realizarem a avaliação A.

Feedback: Geral (nas aulas síncronas, foros do Moodle, etc) e Individual (por email e/ou nos momentos de dúvidas com a professora).

Atendimento: Online de forma síncrona através do Google Meet toda terça-feira e toda sexta-feira (não feriados) das 19h às 20h.

Avaliação: A avaliação (A) será disponibilizada via Moodle com questões abertas. Cada aluno/a receberá uma sequência de questões a partir de um banco de questões elaborado previamente. Os/as alunos/as poderão iniciar as avaliações dentro de um período mínimo de 72 horas em que as questões estarão disponíveis. A partir do momento que comecem a prova terão até três horas para resolver as questões. Após resolver as questões, deverão escaneá-las e enviar à professora responsável. Em nenhum caso serão aceitas resoluções depois da finalização das três horas de prova.
As listas L_{moodle} serão disponibilizadas por um período de duas semanas.
Os/as alunos/as serão comunicados/as das respostas das atividades após o envio das soluções podendo comentar os resultados por mensagem individual ou publicamente em uma aula síncrona se for necessário.

Referências bibliográficas básicas

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

Referências bibliográficas complementares

1. Curso online de Chistof Paar: https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg
2. **ANDREWS, G. Number Theory. New York: Dover Publications, 1994.**
3. BALDONI, M.; CILIBERTO, C.; CATTANEO, G. **Elementary Number Theory, Cryptography and Codes**. Berlin-Heidelberg: Springer-Verlag, 2009.
4. BERNSTEIN, D.; BUCHMANN, J.; DAHMEN, E. **Post-Quantum Cryptography**. Berlin-Heidelberg: Springer-Verlag, 2009.
5. CATALANO, D. et al. **Contemporary Cryptology**. Basel: Birkhäuser, 2005.
6. CORMEN, L.; RIVEST, S. **Algoritmos - Teoria e Prática**. Rio de Janeiro: Campus, 2002.
7. DASGUPTA, S.; PAPADIMITRIOU, C. H.; VAZIRANI, U. V. **Algoritmos**. Porto Alegre: McGraw-Hill/Artmed, 2009.
8. GOLDREICH, O. **Fundamentals of Cryptography, vol. I**: Basic Tools. Cambridge: Cambridge University Press, 2001.
9. GOLDREICH, O. **Fundamentals of Cryptography, vol. II**: Basic Applications.

Cambridge: Cambridge University Press, 2004.

10. HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. H. **An Introduction to Mathematical Cryptography**. New York: Springer-Verlag, 2008.
11. SHOUP, V. A. **Computational Introduction to Number Theory and Algebra**. Cambridge: Cambridge University Press, 2005.
12. SIPSER, M. **Introdução à Teoria da Computação**. São Paulo: Thomson Learning, 2007.