Universidade Federal de Goiás
INSTITUTO DE MATEMÁTICA E ESTATISTICA
Campus Samambaia - 74001-970 - Goiânia
http://www.ime.ufg.br - (62) 3521 1742 - (62) 3521-1208 - secretaria.ime@ufg.br

Plano de Ensino

01. Dados de Identificação da Disciplina:

Semestre:	2022.2	**Curso:**	Matemática
Turma:	B	**Código Componente:**	IME0188
Componente:	INTRODUÇÃO À CRIPTOGRAFIA	**UA Responsável:**	IME
Carga Horária:	64	**UA Solicitante:**	IME
Teórica/Prática:	64/-	**EAD/PCC:**	-/-
Horários:	24n45	**Docente:**	Prof(a) Mario Jose De Souza

02. Ementa:

TEOREMA CHINÊS DO RESTO. CRIPTOGRAFIA COM CHAVE PÚBLICA: MÉTODO RSA. TESTES DE PRIMALIDADE; PSEUDOPRIMOS; HIPÓTESE DE RIEMANN; TEOREMA DOS NÚMEROS PRIMOS; PRIMOS DE FERMAT E MERSENNE. FATORAÇÃO: MÉTODO DE FERMAT, MÉTODO DE POLLARD. FRAÇÕES CONTINUAS

03. Programa:

1. Introdução Histórica.
2. Congruência.
3. Teorema Chinês do Resto.
4. Aplicações: Sistema de Congruência Linear; Resolução do Segundo Grau; Partilha de Senha.
5. Criptografia com Chave Pública: Método RSA.
6. Testes de Primalidade.
7. Pseudoprimos.
8. Hipótese de Riemann.
9. Teorema dos Números Primos.
10. Primos de Fermat e Mersenne.
11. Fatoração: Método de Fermat/ Método de Pollard.
12. Frações Contínuas.

04. Cronograma:

Aula 1 (17/10/2022) Atividade de Acolhimento dos Estudantes do IME

Aula 2 (19 /10 / 2022) Apresentação do plano de ensino.

Aula 3 (26/ 10/ 2022) Introdução Histórica

Aula 4 (31/ 10/ 2022) Congruência

Aula 5 (07/ 11/ 2022) Aula de exercícios

Aula 6 (09/ 11/ 2022) Teorema Chinês do Resto

Aula 7 (14 /11 / 2022) Aula de exercícios

Aula 8 (16/11 / 2022) Aplicação

- Sistema de Congruência Linear

Aula 9 (21/ 11/ 2022) CONPEEX

Aula 10 (23 /11 / 2022) CONPEEX

Aula 11 (28 /11 / 2022) Aplicação

- Resolução do Segundo Grau

Aula 12 (30/11/ 2022) Aplicação

- Partilha de Senha

Aula 13 (05/12/ 2022) Criptografia com Chave Pública: Método RSA

Aula 14 (07/12/ 2022) Testes de Primalidade

Aula 15 (12 /12 / 2022) Primeira Avaliação

Aula 16 (19/12 / 2022) Pseudoprimos

Aula 17 (19/ 12/ 2022) A Função Zeta

Aula 18 (21/ 12/ 2022) A Função Gama

Aula 19 (09/ 01/ 2023) A Representação de Gauss

Aula 20 (11 / 01/ 2023) A Função Gama e a Trigonometria

Aula 21 (16/ 01/ 2023) Função Beta

Aula 22 (18/ 01/ 2023) Fórmula de Duplicação de Legendre

Aula 23 (23 /01 / 2023) Equação Funcional de Riemann

Aula 24 (25/ 01/ 2023) Hipótese de Riemann

Aula 25 (01 /02 / 2023) Teorema dos Números Primos

Aula 26 (06/ 02/2023) Primos de Fermat e Mersenne

Aula 27 (08/ 02/2023) Fatoração: Método de Fermat

Aula 28 (13/ 02/ 2023) Fatoração: Método de Pollard

Aula 29 (15/ 02/ 2023) Frações Contínuas

Aula 30 (20/ 02/2023) Aula de Revisão

Aula 31 (22/02 / 2023) Segunda Avaliação

Aula 32 (27 / 02/ 2023) Entrega da Segunda Avaliação e Entrega das Médias

05. Objetivos Gerais:

- Compreender a história da Criptografia da Antiguidade à atualidade.
- Oferecer uma introdução ao estudo de técnicas criptográficas modernas e suas aplicações.
- Dar uma visão geral da Criptografia, partindo de seus fundamentos.

06. Objetivos Específicos:

- Mostrar como a Criptografia se relaciona com o nosso cotidiano.
- Estabelecer as principais formas de se criptografar uma mensagem.
- Estudar ferramentas de criptografia simétrica e assimétrica.

07. Metodologia:

Para a apresentação do conteúdo haverá aulas expositivas e dialogadas, utilizando-se quadro giz.
Serão propostos exercícios individuais e em conjunto tanto na sala de aula quanto extraclasse, visando à fixação e análise dos conteúdos abordados.
Poderá ser disponibilizado videoaulas através da plataforma SIGAA.
* O acesso à plataforma deve ser feito utilizando o e-mail institucional (...@discente.ufg.br).

08. Avaliações:

Serão aplicadas duas avaliações para verificar a evolução do conhecimento e aprendizado adquiridos pelo estudante ao final de tópicos definidos, conforme cronograma apresentado.

$\mathbf{A}_1-$ Primeira Avaliação: 12/12 /2022 - Conteúdo: itens – 1 à 6

$\mathbf{A}_2-$ Segunda Avaliação: 22/02 /2023 - Conteúdo: itens – 7 à 12

A Média Final MF será a média aritmética das notas A_1 e A_2, isto é,

$$MF = \frac{(A_1 + A_2)}{2}$$

Observações:

- As datas das avaliações poderão sofrer eventuais mudanças, que serão comunicadas antecipadamente aos alunos.
- Provas de ^{a} chamada seguirão as orientações do RGCG;
- Fica proibido o uso de celulares ou equipamentos eletrônicos durante as avaliações, salvo consentimento prévio do professor;
- Durante as avaliações o professor poderá pedir documento de identificação dos alunos;
- A frequência será computada a partir da presença nas aulas e será medida via plataforma SIGAA, durante o horário de aula.
- De acordo com a RESOLUÇÃO - CEPEC N^o 1557, Capítulo IV sessão I, as notas das avaliações serão disponibilizadas no sistema, SIGAA, até cinco dias letivos antes da próxima avaliação.
- Será considerado aprovado o aluno com frequência igual ou superior a setenta e cinco por cento da carga horária total da disciplina e média, igual ou superior a 6,0 (seis).

09. Bibliografia:

[1]: COUTINHO, S.C. Números primos e criptografia RSA. Atual IMPA/SBM. 1997.
[2]: CARVALHO, D. B.. Segurança de Dados com Criptografia. Book Express. 2001.
[3]: STALLINGS, W. Criptografia e Segurança de Redes princípios e práticas. 4a. edição. Pearson Prentice-Hall. 2008.

10. Bibliografia Complementar:

[1]: MENEZES, A. J. et al.. Handbook of applied cryptography. CRC Press. 1997.
[2]: PIPHER, J.; SILVERMAN, J. H. An introduction to Mathematical Cryptography. Springer. 2008.
[3]: KATZ, J.; LINDELL, Y. Introduction to Modern Cryptography. Chapman Hall/CRC. 2008.
[4]: STALLINGS, W. Cryptography and Network Security: Principles and Practice. 2^a Ed. Prentice Hall. 1999.

11. Livros Texto:

[1]: COUTINHO, S.C. Números primos e criptografia RSA. Atual IMPA/SBM. 1997.
[2]: CARVALHO, D. B.. Segurança de Dados com Criptografia. Book Express. 2001.
[3]: STALLINGS, W. Criptografia e Segurança de Redes princípios e práticas. 4a. edição. Pearson Prentice-Hall. 2008.

12. Horários:

Dia	Horário	Sala Distribuida
2^a	N4	203, CAC (50)
2^a	N5	203, CAC (50)
4^a	N4	203, CAC (50)
4^a	N5	203, CAC (50)

13. Horário de Atendimento do(a)s Professor(a):

1. Segunda-feira: 19:00 - 20:00 SALA 112 - IME
2. Quarta-feira: 19:00 -20:00 SALA 112 - IME

14. Professor(a):

Mario Jose De Souza. Email: mario_jose_souza@ufg.br, IME

Prof(a) Mario Jose De Souza