Plano de Ensino

01. Dados de Identificação da Disciplina:

Semestre:	2022.2	**Curso:**	Matemática
Turma:	C	**Código Componente:**	IME0188
Componente:	INTRODUÇÃO À CRIPTOGRAFIA	**UA Responsável:**	IME
Carga Horária:	64	**UA Solicitante:**	IME
Teórica/Prática:	64/-	**EAD/PCC:**	-/-
Horários:	24t56	**Docente:**	

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:

05. Objetivos Gerais:

06. Objetivos Específicos:

07. Metodologia:

08. Avaliações:

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:

12. Horários:

Dia	Horário	Sala

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

14. Professor(a):

Prof(a). Aline De Souza Lima