

Universidade Federal de Pernambuco (UFPE)
Centro de Informática (CIn)
Graduação em Ciência da Computação e Engenharia da Computação

Introdução à Criptografia Moderna **Regras gerais para condução da disciplina**

1. O curso está dividido em duas unidades. Cada unidade se encerra com uma avaliação que inclui todos os assuntos da respectiva unidade.
2. Após alguns anos de experiência no ensino dessa disciplina, decidimos que a melhor forma de aprendizado por parte dos alunos se dá quando acontece uma avaliação progressiva. Dessa forma, temos as mini-provas, que são provas com no máximo duas questões. Por serem aplicadas durante todo o curso, elas também avaliam a participação do aluno no curso.
3. A primeira unidade possui 3 (três) mini-provas. Cada uma vale 1,5 (um v. cinco) pontos. A primeira prova vale 6,0 (seis) pontos.
4. A segunda unidade possui 2 mini-provas. Cada uma vale 1,5 (um) ponto. O projeto (em duplas), a ser escolhido entre os temas:
 1. *Assinaturas Seguras na Prática*
 2. *Geradores (Pseudo)-Aleatórios*
 3. *Exponenciação Rápida*
 4. *Segurança em SSL*
 5. *Segurança em GSM*
 6. *Algoritmos de Fatoração*
 7. *Logaritmos Discretos*
 8. *Segurança com Texto-Cifrado Escolhido*
 9. *Criptografia com Curvas Elípticas*vale 3 (três) pontos.
A segunda prova vale 4,0 (seis) pontos.
5. As mini-provas são realizadas sempre das 12:00hs às 13:00hs.
6. Não haverá segunda chamada de todas as mini-provas. Caso o aluno falte apenas uma mini-prova, poderá fazer uma questão extra na avaliação da unidade, valendo como segunda chamada da mini-prova.
7. A segunda chamada de qualquer uma das provas inclui todos os assuntos e deve ser solicitada na secretaria do curso. Ela será feita no final do curso, antes da prova final, conforme mostra o plano.

8. A revisão da prova só será feita mediante pedido na secretária do curso. A data e hora da revisão é marcada pelo professor. Após essa data, não será feita qualquer revisão.
9. As notas não serão aproximadas. Por exemplo, o aluno que precisa de 0,5 (meio ponto) para passar por média, deve fazer o exame final. Várias chances já foram dadas ao longo das unidades. Além disso, a realização da prova final deve ser encarada como uma oportunidade para o aluno aprender o assunto da disciplina.
10. A chamada será feita a qualquer momento após 15 (quinze) minutos da aula iniciada. O aluno ausente receberá uma falta. Ao final da aula, o aluno que não estava no momento da chamada, deve se dirigir ao professor para não receber a segunda falta. Lembramos que uma aula corresponde a duas faltas.
11. As faltas serão atualizadas no SIGA mensalmente.