



UNIVERSIDADE ESTADUAL DE CAMPINAS
EDITAL
CARGO DE PROFESSOR DOUTOR – MS-3.1

O Diretor do Instituto de Computação da Universidade Estadual de Campinas, através da Secretaria Geral, torna pública a abertura de inscrições para o concurso público de provas e títulos, para provimento de 1 (um) cargo de Professor Doutor, nível MS-3.1, em RTP, com opção preferencial para o RDIDP, nos termos do item 2, na área de Criptografia Computacional, nas disciplinas MC889 - Introdução à Criptografia, MC938 - Algoritmos Criptográficos e MO422 - Algoritmos Criptográficos, do Departamento de Teoria da Computação do Instituto de Computação da Universidade Estadual de Campinas.

1. DO REQUISITO MÍNIMO PARA INSCRIÇÃO

1.1. Poderá se inscrever no concurso o candidato que, no mínimo, seja portador do Título de Doutor.

1.2. É desejável que o candidato tenha o seguinte perfil:

1.2.1. Demonstrar capacidade de pesquisa em computação

1.2.2. A inscrição de candidato que deixar de atender ao perfil desejável não será indeferida por este motivo.

2. DO REGIME DE TRABALHO

2.1. Nos termos do artigo 109 do Estatuto da UNICAMP, o Regime de Dedicação Integral à Docência e à Pesquisa (RDIDP) é o regime preferencial do corpo docente e tem por finalidade estimular e favorecer a realização da pesquisa nas diferentes áreas do saber e do conhecimento, assim como, correlatamente, contribuir para a eficiência do ensino e para a difusão de ideias e conhecimento para a comunidade.

2.2. Ao se inscrever no presente concurso público o candidato fica ciente e concorda que, no caso de admissão, poderá ser solicitada, a critério da Congregação da Unidade, a apresentação de plano de pesquisa, que será submetido à Comissão Permanente de Dedicação Integral à Docência e à Pesquisa – CPDI – para avaliação de possível ingresso no Regime de Dedicação Integral à Docência e à Pesquisa – RDIDP.

2.3. O Regime de Dedicação Integral à Docência e à Pesquisa (RDIDP) está regulamentado pela Deliberação CONSU-A-02/01, cujo texto integral está disponível no sítio:

http://www.pg.unicamp.br/mostra_norma.php?consolidada=S&id_norma=2684.

2.4. O aposentado na carreira docente aprovado no concurso público somente



poderá ser admitido no Regime de Turno Parcial (RTP), vedada a extensão ao Regime de Dedicação Integral à Docência e à Pesquisa (RDIDP), conforme Deliberação CONSU-A-08/2010.

2.5. A remuneração inicial para o cargo de Professor Doutor, MS-3.1, da Carreira do Magistério Superior é a seguinte:

- a) RTP – R\$ 2.315,38
- b) RTC – R\$ 5.877,38
- c) RDIDP – R\$ 13.357,49

3. DAS INSCRIÇÕES

3.1. As inscrições deverão ser feitas exclusivamente por meio do link <https://www.sis.cgu.unicamp.br/solicita/concurso/formulario> no período de 40 (quarenta) úteis, a contar de 9 horas do primeiro dia útil subsequente ao da publicação deste edital no Diário Oficial do Estado (DOE), até 23 horas e 59 minutos do último dia do prazo de inscrição.

3.2. No momento da inscrição deverá ser apresentado, por meio do sistema de inscrição, requerimento dirigido ao Diretor do Instituto de Computação, contendo nome, domicílio e profissão, acompanhado dos seguintes documentos:

a) prova de que é portador do título de doutor de validade nacional. Para fins de inscrição, o candidato poderá apresentar apenas a Ata da defesa de sua Tese de Doutorado, ou documento oficial equivalente, sendo que a comprovação do título de Doutor será exigida por ocasião da admissão. O candidato que tenha obtido o título de Doutor no exterior, caso aprovado, deverá obter, durante o período probatório, o reconhecimento do referido título para fins de validade nacional, sob pena de demissão;

b) documento de identificação pessoal, em forma digital (pdf, máximo 10MB);

c) um exemplar de memorial, em forma digital (pdf, máximo 10MB), com o relato das atividades realizadas e a comprovação dos trabalhos publicados e demais informações, que permitam avaliação dos méritos do candidato, a saber:

c.1. títulos universitários;

c.2. *curriculum vitae et studiorum*;

c.3. atividades científicas, didáticas e profissionais;

c.4. títulos honoríficos;

c.5. bolsas de estudo em nível de pós-graduação;

c.6. cursos frequentados, congressos, simpósios e seminários dos quais participou.

d) um exemplar ou cópia de cada trabalho ou documento mencionado no memorial, em forma digital (pdf, máximo 10MB cada);

e) Plano de Pesquisa - descrição, em até 20 (vinte) páginas, das atividades de



pesquisa que o candidato pretende desenvolver no Instituto de Computação, explicitando como tais atividades estão ligadas à experiência acadêmica do candidato, em forma digital (pdf, máximo 10MB cada);

3.2.1. O memorial poderá ser aditado, instruído ou completado até a data fixada para o encerramento das inscrições.

3.2.2. O candidato portador de necessidades especiais, temporária ou permanente, que precisar de condições especiais para se submeter às provas deverá solicitá-las por escrito no momento da inscrição, indicando as adaptações de que necessita.

3.2.3. No ato da inscrição o candidato poderá manifestar por meio do sistema de inscrição a intenção de realizar as provas na língua inglesa. Os conteúdos das provas realizadas nas línguas inglesa e portuguesa serão os mesmos.

3.2.4. A Unicamp não se responsabiliza por solicitação de inscrição pela internet não recebida por motivos de ordem técnica dos computadores, falhas de comunicação, congestionamento de linhas de comunicação, bem como outros fatores que impossibilitem a transferência de dados.

3.2.5. Após realizar a inscrição no link indicado no item 3.1, com envio dos documentos solicitados, o candidato confirmará a inscrição e receberá um protocolo de recebimento de seu pedido de inscrição.

3.3. Recebida a documentação e satisfeitas as condições do edital, a Secretaria da Unidade encaminhará o requerimento de inscrição com toda a documentação ao Diretor do Instituto de Computação, que a submeterá ao Departamento ou a outra instância competente, definida pela Congregação da Unidade a que estiver afeta as áreas em concurso, tendo este o prazo de 15 dias para emitir parecer circunstanciado sobre o assunto

3.3.1. O parecer de que trata o subitem anterior será submetido à aprovação da Congregação da Unidade, instância que deliberará sobre o deferimento de inscrições.

3.3.2. A Unidade divulgará no sítio www.ic.unicamp.br/ a deliberação da Congregação referente às inscrições e composição da Comissão Julgadora.

3.4. Os candidatos que tiveram os requerimentos de inscrição deferidos serão notificados a respeito da composição da Comissão Julgadora e seus suplentes, bem como do calendário fixado para as provas e do local de sua realização, por meio de edital a ser publicado no Diário Oficial do Estado e divulgado no sítio www.ic.unicamp.br/, com antecedência mínima de 20 (vinte) dias úteis do início das provas.

3.5. O prazo de inscrição poderá ser prorrogado, a critério da Unidade, por igual período, devendo ser publicado no Diário Oficial do Estado até o dia do



encerramento das inscrições.

3.6. A critério da Unidade, o prazo de inscrições poderá ser reaberto, por igual período, até o final do dia útil imediatamente posterior ao do encerramento das inscrições.

4. DA COMISSÃO JULGADORA

4.1. A Comissão Julgadora será constituída de 05 (cinco) membros titulares e 02 (dois) suplentes, portadores, no mínimo, do Título de Doutor, cujos nomes serão aprovados pela Congregação da Unidade, e sua composição deverá observar os princípios constitucionais, em particular o da impessoalidade.

4.1.1. Pelo menos dois membros da Comissão Julgadora deverão ser externos à Unidade ou pertencer a outras instituições.

4.2. Caberá à Comissão Julgadora examinar os títulos apresentados, conduzir as provas do concurso e proceder às arguições a fim de fundamentar parecer circunstanciado, classificando os candidatos.

4.3. A Comissão Julgadora será presidida pelo membro da Unidade com a maior titulação. Na hipótese de mais de um membro se encontrar nesta situação, a presidência caberá ao docente mais antigo na titulação.

5. DAS PROVAS

5.1. O concurso será realizado em duas fases, sendo a primeira fase de caráter eliminatório e classificatório, e a segunda fase de caráter classificatório.

5.1.1. A primeira fase do concurso constará da seguinte prova:

a) prova escrita (peso 1).

5.1.2. A segunda fase do concurso constará das seguintes provas:

a) prova específica, referente ao Plano de Pesquisa (peso 1);

b) prova de títulos (peso 2);

c) prova de arguição (peso 2);

d) prova didática (peso 2).

5.1.3. As notas atribuídas na prova escrita por cada um dos examinadores aos candidatos aprovados serão computadas ao final do concurso público para fins de classificação, nos termos do item 6.3 deste edital, obedecidos os critérios previstos no item 6.1.1.

5.2. Na definição dos horários de realização das provas será considerado o horário oficial de Brasília/DF.

5.2.1. O candidato deverá comparecer ao local designado para a realização das provas com antecedência mínima de 30 (trinta) minutos da hora fixada para o seu início.

5.2.2. Não será admitido o ingresso de candidato no local de realização das



provas após o horário fixado para o seu início.

5.3. O não comparecimento às provas, por qualquer que seja o motivo, caracterizará desistência do candidato e resultará em sua eliminação do certame.

5.4. A prova escrita, de caráter eliminatório e classificatório, ocorrerá no início do concurso e seus resultados divulgados antes da sequência das demais provas.

5.4.1. Participarão das demais provas apenas os candidatos aprovados nas provas eliminatórias.

Prova escrita

5.5. A prova escrita será dissertativa com uma ou mais questões, que verificará(ão) o conhecimento do candidato sobre o conteúdo do programa das disciplinas do concurso. Estas questões poderão abordar tanto itens específicos do programa quanto aspectos gerais básicos, relativos ao papel dessas disciplinas dentro de um curso de Computação.

5.5.1. A(s) questão(ões) da prova escrita serão elaboradas pela Comissão Julgadora.

5.5.2. No início da prova escrita, a Comissão Julgadora fará a leitura da(s) questão(ões), concedendo o prazo de 30 (trinta) minutos para que os candidatos consultem seus livros, anotações pessoais ou outros documentos bibliográficos.

5.5.3. Apenas as anotações efetuadas pelo candidato durante o período de consulta poderão ser utilizadas no decorrer da prova. Tais anotações serão feitas em papel rubricado pela Comissão Julgadora e deverão ser anexadas à resolução da prova.

5.5.4. Findo o prazo de consulta, não será mais permitida a consulta de qualquer material e a prova escrita deverá ser realizada por todos os candidatos, iniciando-se em um mesmo horário, com duração máxima de 2 (duas) horas para a redação das respostas.

5.5.5. É vedado o uso de quaisquer meios eletrônicos, inclusive durante a fase de consulta.

5.5.6. Cada examinador atribuirá uma nota de 0 (zero) a 10 (dez) à prova escrita.

Prova específica

5.6. A prova específica baseia-se na análise e julgamento de um Plano de Pesquisa elaborado pelo candidato e será dividida em duas partes. Na primeira parte o candidato terá até 15 minutos para fazer uma apresentação sobre seu Plano de Pesquisa. Em seguida, na segunda parte, o candidato será interpelado pela Comissão Julgadora sobre seu Plano de Pesquisa apresentado na inscrição.

5.6.1. Cada integrante da Comissão Julgadora disporá de até 15 (quinze) minutos para arguir o candidato que terá igual tempo para responder às



questões formuladas.

5.6.2. Havendo acordo mútuo, a arguição poderá ser feita sob a forma de diálogo, respeitando, porém, o limite máximo de 30 (trinta) minutos para cada arguição.

5.6.3. Havendo mais de um candidato, proceder-se-á, no dia e horário marcado para realização da prova específica e na presença de todos os candidatos, ao sorteio da ordem de apresentação.

5.6.4. Ao final da prova, cada examinador atribuirá ao candidato nota de 0 (zero) a 10 (dez).

Prova de títulos

5.7. Na prova de títulos a Comissão Julgadora apreciará o memorial elaborado e comprovado pelo candidato no ato da inscrição.

5.7.1. Para fins de julgamento da prova de títulos serão considerados os seguintes documentos:

- a) Título de Graduação;
- b) Título de Especialização;
- c) Título de Mestrado;
- d) Título de Doutorado;
- e) Título de Mestrado Profissional;
- f) Pós-Doutorado;
- g) Publicações acadêmico-científicas (artigos, livros, capítulos de livros, etc);
- h) Publicações em revistas de circulação nacional/indexadas;
- i) Publicações em revistas de circulação internacional/indexadas;
- j) Experiência docente;
- k) Experiência profissional;
- l) Participação em atividades de extensão;
- m) Atividades acadêmicas durante a graduação (iniciação-científica, monitoria, estágio);
- n) Recebimento de bolsa ou apoio para pesquisa;
- o) Participação ou coordenação em projeto de pesquisa;
- p) Premiação e distinção acadêmica;
- q) Assessoria e consultoria;
- r) Produções artístico-culturais;
- s) Patentes ou propriedades intelectuais registradas;

5.7.2. A Comissão Julgadora adotará os seguintes critérios para julgamento da prova de títulos, considerando a qualidade e o interesse da produção do candidato:

- a) A Relevância do tema da produção do candidato na comunidade de especialistas;



- b) Dificuldade, raridade e valor que os resultados da produção do candidato têm perante a comunidade científica;
- c) Relevância, contribuição e aderência da produção do candidato para a área do concurso;
- d) Impacto científico, artístico, social e de inovação da produção do candidato;
- e) Criatividade, inovação e abertura de novas técnicas/temas de pesquisa para a área do concurso;
- f) Conhecimento, domínio e maturidade na área do concurso;
- g) Compreensão global da área e do impacto da sua pesquisa em áreas vizinhas;
- h) Legibilidade e qualidade da difusão dos teoremas/resultados dos textos escritos, e/ou alcance da produção das atividades artístico-culturais do candidato;

5.7.3. Os membros da Comissão Julgadora terão o prazo máximo de 24 (vinte e quatro) horas para emitir julgamento da prova de títulos.

5.7.4. Cada examinador atribuirá uma nota de 0 (zero) a 10 (dez) à prova de títulos, elaborando parecer circunstanciado que indique os critérios de julgamento e a pontuação atribuída a cada candidato.

Prova de arguição

5.8. Na prova de arguição o candidato será interpelado pela Comissão Julgadora sobre a matéria do programa da disciplina ou conjunto de disciplinas em concurso e/ou sobre o memorial apresentado na inscrição.

5.8.1. Na prova de arguição cada integrante da Comissão Julgadora disporá de até 30 (trinta) minutos para arguir o candidato que terá igual tempo para responder às questões formuladas.

5.8.2. Havendo acordo mútuo, a arguição poderá ser feita sob a forma de diálogo, respeitando, porém, o limite máximo de 01 (uma) hora para cada arguição.

5.8.3. Havendo mais de um candidato, proceder-se-á, no dia e horário marcado para realização da prova de arguição e na presença de todos os candidatos, ao sorteio da ordem de apresentação.

5.8.4. Ao final da prova, cada examinador atribuirá ao candidato nota de 0 (zero) a 10 (dez).

Prova didática



5.9. A prova didática versará sobre o programa de disciplina ou conjunto de disciplinas em concurso (Anexo I) e nela o candidato deverá revelar cultura aprofundada no assunto.

5.9.1. A matéria para a prova didática será sorteada com 24 (vinte e quatro) horas de antecedência, de uma lista de 10 (dez) pontos, organizada pela Comissão Julgadora.

5.9.2. A prova didática terá duração de 50 (cinquenta) a 60 (sessenta) minutos, e nela o candidato desenvolverá o assunto do ponto sorteado, vedada a simples leitura do texto da aula, mas facultando-se, com prévia aprovação da Comissão Julgadora, o emprego de roteiros, apontamentos, tabelas, gráficos, dispositivos ou outros recursos pedagógicos utilizáveis na exposição.

5.9.3. Ao final da prova, cada examinador atribuirá ao candidato nota de 0 (zero) a 10 (dez).

5.10. As provas orais do presente concurso público serão realizadas em sessão pública. É vedado aos candidatos assistir às provas dos demais candidatos.

5.11. A Comissão Julgadora poderá ou não descontar pontos quando o candidato não atingir o tempo mínimo ou exceder o tempo máximo pré-determinado para as provas didática e de arguição.

6. DA AVALIAÇÃO E JULGAMENTO DAS PROVAS

6.1. As provas de títulos, arguição, didática, escrita e específica terão caráter classificatório.

6.1.1. A prova escrita, além de caráter classificatório, terá também caráter eliminatório.

6.1.1.1. Ao final da prova escrita, cada examinador atribuirá uma nota de 0 (zero) a 10 (dez) à prova escrita.

6.1.1.2. Após a atribuição das notas, o resultado da prova escrita será imediatamente proclamado pela Comissão Julgadora em sessão pública.

6.1.1.3. Serão eliminados os candidatos que obtiverem nota na prova escrita inferior a 7,0 (sete), em uma escala de zero a dez, da maioria dos membros da Comissão Julgadora.

6.1.1.4. Os candidatos não eliminados por nota na prova escrita serão ordenados, para fins de seleção para a fase seguinte, por ordem decrescente da média aritmética das notas dadas por cada membro da Comissão Julgadora.

6.1.1.5. A média da prova escrita será calculada até a casa dos centésimos, desprezando-se o algarismo de ordem centesimal, se inferior a cinco e aumentando-se o algarismo da casa decimal para o número subsequente, se o algarismo da ordem centesimal for igual ou superior a cinco.



6.1.1.6. Somente participarão das demais provas do concurso público os candidatos aprovados na prova escrita.

6.1.1.7. As notas atribuídas na prova escrita por cada um dos examinadores aos candidatos aprovados serão computadas ao final do concurso público para fins de classificação, nos termos do item 6.3 deste edital.

6.2. Ao final de cada uma das provas previstas no subitem 5.1.2 deste edital, cada examinador atribuirá ao candidato uma nota de 0 (zero) a 10 (dez).

6.2.1. As notas de cada uma das provas previstas no item 5.1.2. serão atribuídas individualmente pelos integrantes da Comissão Julgadora em envelope lacrado e rubricado, após a realização de cada prova e abertos ao final de todas as provas do concurso em sessão pública.

6.3. A nota final de cada examinador será a média ponderada das notas atribuídas por ele ao candidato em cada prova.

6.3.1. Cada examinador fará uma lista ordenada dos candidatos pela sequência decrescente das notas finais. O próprio examinador decidirá os casos de empate, com critérios que considerar pertinentes.

6.3.2. As notas finais serão calculadas até a casa dos centésimos, desprezando-se o algarismo de ordem centesimal, se inferior a cinco e aumentando-se o algarismo da casa decimal para o número subsequente, se o algarismo da ordem centesimal for igual ou superior a cinco.

6.4. A Comissão Julgadora, em sessão reservada, depois de divulgadas as notas e apurados os resultados, emitirá parecer circunstanciado sobre o resultado do concurso justificando a indicação feita, do qual deverá constar tabela e/ou textos contendo as notas, as médias e a classificação dos candidatos. Também deverão constar do relatório os critérios de julgamento adotados para avaliação de cada uma das provas. Todos os documentos e anotações feitas pela Comissão Julgadora para atribuição das notas deverão ser anexados ao processo do concurso público.

6.4.1. Ao relatório da Comissão Julgadora poderão ser acrescentados relatórios individuais de seus membros.

6.5. O resultado do concurso será imediatamente proclamado pela Comissão Julgadora em sessão pública.

6.5.1. Serão considerados habilitados os candidatos que obtiverem, da maioria dos examinadores, nota final mínima sete.

6.5.2. A relação dos candidatos habilitados é feita a partir das listas ordenadas de cada examinador.

6.5.3. O primeiro colocado será o candidato que obtiver o maior número de indicações em primeiro lugar na lista ordenada de cada examinador.

6.5.4. O empate nas indicações será decidido pela Comissão Julgadora,



prevalecendo sucessivamente a maior média obtida na prova didática e a maior média obtida na prova de títulos. Persistindo o empate a decisão caberá, por votação, à Comissão Julgadora. O Presidente terá voto de desempate, se couber.

6.5.5. Excluindo das listas dos examinadores o nome do candidato anteriormente selecionado, o próximo classificado será o candidato que obtiver o maior número de indicações na posição mais alta da lista ordenada de cada examinador.

6.5.6. Procedimento idêntico será efetivado subsequentemente até a classificação do último candidato habilitado.

6.6. As sessões de que tratam os itens 6.2.1 e 6.5 deverão se realizar no mesmo dia em horários previamente divulgados.

6.7. O parecer da Comissão Julgadora será submetido à Congregação da(o) Faculdade/Instituto, que só poderá rejeitá-lo em virtude de vícios de ordem formal, pelo voto de 2/3 (dois terços) de seus membros presentes.

6.8. O resultado final do concurso será submetido à apreciação da Câmara Interna de Desenvolvimento de Docentes (CIDD), e encaminhada à Câmara de Ensino, Pesquisa e Extensão (CEPE) para deliberação.

6.9. A relação dos candidatos aprovados será publicada no Diário Oficial do Estado, com as respectivas classificações.

7. DA ELIMINAÇÃO

7.1. Será eliminado do concurso público o candidato que:

- a) Deixar de atender às convocações da Comissão Julgadora;
- b) Não comparecer ao sorteio do ponto da prova didática;
- c) Não comparecer a qualquer uma das provas, exceto a prova de títulos.

8. DO RECURSO

8.1. O candidato poderá interpor recurso contra o resultado do concurso, exclusivamente de nulidade, ao Conselho Universitário, no prazo de 05 (cinco) dias úteis, a contar da publicação prevista no item 6.9 deste edital.

8.1.1. O recurso deverá ser protocolado na Secretaria Geral da UNICAMP.

8.1.2. Não será aceito recurso via postal, via fac-símile ou correio eletrônico.

8.1.3. Recursos extemporâneos não serão recebidos.

8.2. O resultado do recurso será divulgado no sítio eletrônico da Secretaria Geral da UNICAMP (www.sg.unicamp.br)

9. DAS DISPOSIÇÕES FINAIS

9.1. A inscrição do candidato implicará o conhecimento e a tácita aceitação das



normas e condições estabelecidas neste Edital, em relação às quais o candidato não poderá alegar qualquer espécie de desconhecimento.

9.2. As convocações, avisos e resultados do concurso serão publicados no Diário Oficial do Estado e estarão disponíveis no sítio www.ic.unicamp.br/, sendo de responsabilidade exclusiva do candidato o seu acompanhamento.

9.3. Se os prazos de inscrição e/ou recurso terminarem em dia em que não há expediente na Universidade, no sábado, domingo ou feriado, estes ficarão automaticamente prorrogados até o primeiro dia útil subsequente.

9.4. O prazo de validade do concurso será de 1 (um) ano, a contar da data de publicação no Diário Oficial do Estado da homologação dos resultados pela CEPE, podendo ser prorrogado uma vez, por igual período.

9.4.1. Durante o prazo de validade do concurso poderão ser providos os cargos que vierem a vagar, para aproveitamento de candidatos aprovados na disciplina ou conjunto de disciplinas em concurso.

9.5. A critério da Unidade de Ensino e Pesquisa, ao candidato aprovado e admitido poderão ser atribuídas outras disciplinas além das referidas na área do concurso, desde que referentes à área do concurso ou de sua área de atuação.

9.6. O candidato aprovado e admitido somente será considerado estável após o cumprimento do estágio probatório, referente a um período de 03 (três) anos de efetivo exercício, durante o qual será submetido à avaliação especial de desempenho, conforme regulamentação prevista pela Universidade.

9.7. Até 60 (sessenta) dias após a publicação da homologação do concurso o candidato poderá solicitar a retirada dos memoriais (item 3.2. “c” e “d”) entregues no ato da inscrição e que não foram utilizados pela Comissão Julgadora, mediante requerimento protocolado na Secretaria do Instituto de Computação. Após este prazo, se não retirados, os memoriais serão descartados.

9.8. O presente concurso obedecerá às disposições contidas na Deliberação CONSU-A-30/2013, Deliberação CONSU-A-046/2019 e Deliberações da Congregação IC nº22/2014 e 178/2019, que dispõem sobre os critérios para realização de Concurso para Professor Doutor no Instituto de Computação.

9.8.1. Cópia das deliberações mencionadas podem ser obtidas nos sítios www.sg.unicamp.br e www.ic.unicamp.br ou junto à Secretaria do Instituto de Computação, que poderá prestar quaisquer outras informações relacionadas ao concurso público.

9.9. Os itens deste edital poderão sofrer eventuais alterações, atualizações ou acréscimos enquanto não consumada a providência ou evento que lhes disser respeito, até a data de convocação para a prova correspondente, circunstância que será mencionada em Edital ou Aviso a ser publicado.

9.10. Qualquer alteração nas regras de execução do concurso deverá ser objeto de



novo Edital.

Anexo I – Programas das Disciplinas

MC889 - Introdução à Criptografia

1. Criptografia clássica: algoritmos e criptanálise.
2. Teoria de Shannon: entropia e segredo perfeito.
3. Cifras de bloco: DES e AES.
4. Funções de resumo criptográfico e Códigos de Autenticação de Mensagem.
5. Criptografia baseada na fatoração de inteiros: RSA e Rabin.
6. Criptografia baseada no logaritmo discreto: Diffie-Hellman, ElGamal e ECC.
7. Esquemas de assinatura digital.
8. Geração de números aleatórios.

MC938 - Algoritmos Criptográficos

1. Breve introdução à Criptografia moderna.
2. Algoritmos básicos: aritmética básica de precisão arbitrária, aritmética modular, máximo divisor comum, resolução de congruências.
3. Algoritmos intermediários: testes de primalidade, fatoração, logaritmo discreto, aritmética de corpos finitos, aritmética em curvas elípticas.
4. Algoritmos avançados: emparelhamentos bilineares, teste de primalidade.

MO422 - Algoritmos Criptográficos

Aritmética modular, algoritmos para aritmética de números grandes, algoritmo de Montgomery algoritmo de MDC, algoritmo estendido de Euclides, implementação em software, corpos finitos, corpos primos, corpos binários, implementação em software, geração de números primos, testes de primalidade, geração de números aleatórios, algoritmos simétricos, cifradores de bloco (DES, AES, Camellia), modos de operação funções de resumo criptográfico (hash), MAC, H-MAC, implementação em software, algoritmos assimétricos: RSA (variantes), ECC, algoritmos para criptografia baseada em identidades, aspectos de implementação em software, tópicos especiais.

Anexo II - Bibliografia

MC889 - Introdução à Criptografia



- Graduação: STINSON, Douglas. Cryptography: Theory and Practice. 3rd edition, CRC Press, 2006.
- Graduação: PAAR, Christof; PELZL, Jan. Understanding Cryptography, Springer, 2014.
- Pos: KATZ, Johnathan; LINDELL, Yehuda. Introduction to Modern Cryptography, CRC Press, 2007.
- Auxiliar: MENEZES, Alfred. Handbook of Applied Cryptography. CRC Press, 2001.

MC938/MO422 - Algoritmos Criptográficos

Guide to Elliptic Curve Cryptography, Darrel Hankerson, Alfred Menezes e Scott Vanstone, Springer-Verlag, 2004. Handbook of Applied Cryptography, A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1997. Modern Cryptography theory and practice, Wenbo Mao, Pearson Education, 2004. Cryptography Theory and Practice, Douglas R. Stinson, Chapman & Hall/CRC, 2005. A Computational Introduction to Number Theory and Algebra, Victor Shoup, Cambridge University Press, 2005.

Documento assinado eletronicamente por **ANDERSON DE REZENDE ROCHA, DIRETOR DE UNIDADE UNIVERSITÁRIA**, em 12/04/2022, às 16:47 horas, conforme Art. 10 § 2º da MP 2.200/2001 e Art. 1º da Resolução GR 54/2017.



A autenticidade do documento pode ser conferida no site:
sigad.unicamp.br/verifica, informando o código verificador:
0CE08D2D 713E4E49 99A00E16 55C0FE0F

