INSTITUTO FEDERAL
Minas Gerais
Campus Bambuí

**INSTITUTO FEDERAL DE MINAS GERAIS**
***CAMPUS* BAMBUÍ**

---

**Código:** BiSuCOM.114

**Disciplina:** Criptografia

**Pré-requisito(s):** Segurança Computacional/Matemática Discreta

**Co-requisito(s):** -

---

**Carga Horária**

**Teórica:** 33.2 **Prática:** 33.2 **Total:** 66.4

---

**Ementa:**

Histórico da criptografia. Cifras Simétricas: Técnicas Clássicas de Criptografia; Cifras de bloco; DES, 3DES, AES; Cifras de fluxo; Distribuição de Chaves. Criptografia de Chave Pública e Funções de Hash: Teoremas de Fermat e Euler; Teorema Chinês do Resto; Criptossistemas de Chave Pública e RSA; Gerenciamento de Chaves; Autenticação de Mensagem e funções de hash e MAC; Assinaturas Digitais e protocolos de autenticação. Certificação Digital. Esteganografia. Criptoanálise. Criptografia de curva elíptica.

---

**Objetivo Geral:**

Compreender os processos criptográficos disponíveis atualmente, visando prover os conceitos necessários para sua utilização de acordo com as necessidades do usuário.

---

**Objetivo Específico:**

Compreender o histórico da criptografia na História da Humanidade. Correlacionar os conceitos de criptografia de bloco e de fluxo e suas aplicações. Distinguir as aplicações para cifras simétricas e assimétricas. Compreender a aplicação da criptografia na segurança de sistemas. Compreender as Infraestruturas de Chaves Públicas existentes.

---

**Bibliografia Básica:**

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008. 492 p. Disponível em:

<http://ifmg.bv3.digitalpages.com.br/users/publications/9788576051190>, Acesso em: 20 mai. 2018

SHOKRANIAN, SALAHODDIN. **Criptografia para Iniciantes.** 2. ed. Rio de Janeiro: Ciência Moderna, 2012. 92 p. Acervo: 005.82 S559c 2. ed.

**SEGURANÇA DE DADOS.** criptografia em redes de computador. 2. ed. São Paulo: Blucher, 2008. 305 p. Acervo: 005.82 T315s 2008

**Bibliografia Complementar:**

NAKAMURA, EMILIO TISSATO; GEUS, PAULO LÍCIO DE. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007. 483 p. Acervo: 005.8 N163s

MENEZES, PAULO BLAUTH . **Matemática discreta para computação e informática**. 4. ed. Porto Alegre: Bookman, 2013. 348 p. Acervo: 510 M543m

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, CERT.BR.. **Cartilha de Segurança para Internet:** versão 4.0. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 142 p. Disponível em: <http://cartilha.cert.br/livro/>, Acesso em: 20 mai. 2018

SILVA, LUIZ GUSTAVO CORDEIRO DA; SILVA; PAULO CAETANO DA; BATISTA, EDUARDO MAZZA; HOMOLIKA, HEBERT OTTO; AQUINO JÚNIOR, IVANILDO JOSÉ DE SOUSA; LIMA, MARCELO FERREIRA DE. **Certificação Digital:** Conceitos e Aplicações - Modelos Brasileiro e Australiano. Rio de Janeiro: Ciência Moderna, 2008. 201 p. Acervo: 005.8 C418 c2008

KUROSE, JAMES F.; ROSS, KEITH W.. **Redes de computadores e a internet:** uma abordagem tpo-down. 6. ed. São Paulo: Pearson Education, 2013. 634 p. Disponível em: <http://ifmg.bv3.digitalpages.com.br/users/publications/9788581436777>, Acesso em: 20 mai. 2018