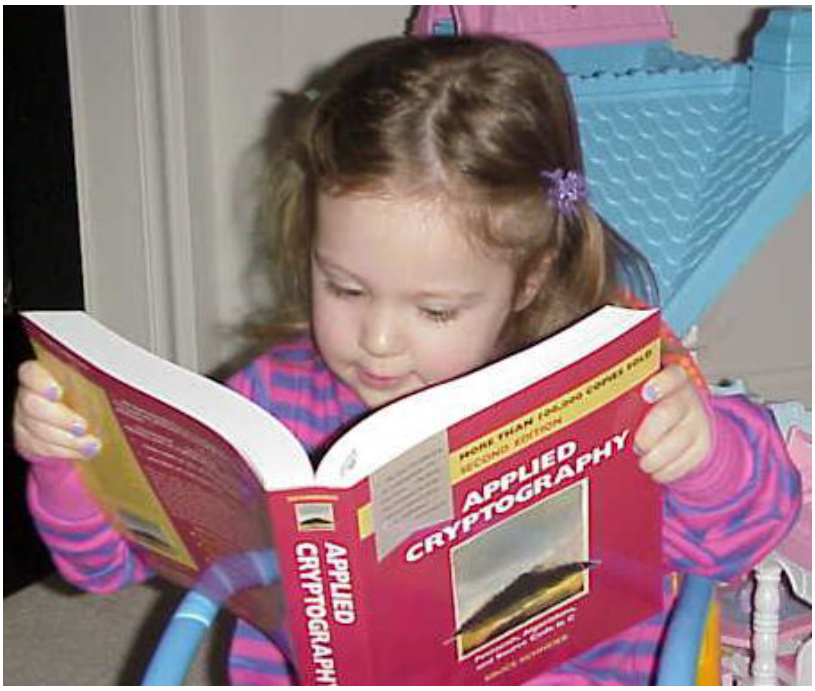
Computação segura (cod.10524)

Departamento de Informática
Universidade da Beira Interior

Ano lectivo 2012/2013



Esta página no formato pdf

1 Novidades

- Novo horário! consultar 7.
- Aviso para os alunos empenhados
- Como colocar uma dúvida ao regente da Unidade Curricular?
  1. Comparecer nas aulas e colocá-la directamente ao regente
  2. Comparecer no horário de atendimento do regente e colocá-la directamente
  3. Enviar um email ao regente (desousaUUU@UUUdi.ubi.pt, (retire os UUU)) com o assunto "CS: XXXX"em que XXX é o título da dúvida em questão. Qualquer outro formato no assunto arrisca condenar o email ao esquecimento.
- Inscrição em turmas práticas: via site dos serviços académicos.
- As aulas práticas começam na segunda semana de aulas.
- Os alunos com estatuto de *trabalhador estudante* são convidados a dirigir-se ao regente para discutir os critérios de avaliação.

Conteúdo

2 Docentes

- Simão Melo de Sousa (regente) - Gabinete 3.17 - Laboratório 6.10 - Bloco VI.

3 Objectivos

Este UC tem por objectivo uma introdução aos fundamentos e à prática da criptografia e das suas técnicas. Serão cobertos tópicos como a cifra (chave-privada, chave-pública, chaves simétricas), assinaturas digitais, autenticação segura, partilha de segredos, e protocolos criptográficos.

4 Programa

- Classical vs. modern cryptography; some historical ciphers; principles of modern cryptography; perfectly secret encryption.
- Computational security. Symmetric-key encryption.
- Message authentication and hash functions.
- Block cipher design.
- Theoretical constructions of pseudorandom generators/functions.

- Number theory; cryptographic hardness assumptions and their applications.
- The public-key revolution; Diffie-Hellman key exchange.
- Public-key encryption.
- Digital signatures.
- The random oracle model and efficient cryptographic schemes.

4.1 Competências da UC ou Resultados da Aprendizagem

O aluno deverá ser capaz de perceber os conceitos próprios a segurança da informação e das comunicações. Deverá perceber os detalhes e os fundamentos das primitivas criptográficas e os diversos protocolos criptográficos estabelecidos e emergentes.

Deverá ser capaz de perceber que propriedades de segurança são desejáveis nos diversos sistemas de informação e de comunicação que se querem seguros. Deverá saber adequadamente definir e comprovar tais propriedades.

Deverá igualmente saber como usar ou desenhar e implementar primitivas, protocolos criptográficos que respeitam comprovadamente tais propriedades.

5 Critérios de Avaliação

5.1 Actividades de Ensino-Aprendizagem e Metodologias Pedagógicas

Por fim a avaliar as competências adquiridas, as actividades de Ensino-Aprendizagem avaliarão tanto a compreensão dos conceitos teóricos expostos como a capacidade em por estes em prática.

Assim, a avaliação será constituída por duas componentes: a componente **prática** (exercícios práticos entregues à equipa docente) e a componente **teórica** (provas escritas).

5.2 Fraudes

A equipa docente realça que qualquer tipo de fraude em qualquer dos itens desta disciplina implica a reprovação automática do aluno faltoso, podendo ainda vir a ser este alvo de processo disciplinar.

Listamos a seguir as diferentes componentes da avaliação.

5.3 Componente Prática

- Esta avaliação mede em termos práticos a aquisição dos conceitos expostos. Como tal é baseada na avaliação da resolução de exercícios durante as práticas laboratoriais. Em particular o último exercício, com data de entrega definida para a última aula prática, dará lugar a uma defesa.

- A *Nota da Componente Prática* (NCP, 20 valores) é a soma dos valores atribuídos aos diferentes exercícios resolvidos.

5.4 Componente Teórica

A avaliação da componente teórica consiste na realização de uma frequência, (ver secção 6 para consultar a data da sua realização)

Desta prova resulta a *Nota da Componente Teórica* (NCT, 20 valores).

5.5 Avaliação Contínua

A nota da avaliação contínua é determinada da seguinte forma:

$$\frac{\text{componente prática (NCP)} + \text{componente teórica (NCT)}}{2}$$

5.6 Admissão e Avaliação por Exame

- Mínimos: São seguidas as disposições aprovadas pelo Conselho Científico da Universidade aplicadas individualmente a cada componente da avaliação. Assim, $NCP \geq 6 \wedge NCT \geq 6 \Longrightarrow$ *admissão ao exame.*

- A prova escrita do exame substituirá a Nota da Componente Teórica da avaliação contínua, dando uma nova NCT.

- Assim a nota final (NFin) após exame é calculada da seguinte forma:

$$NFin = if\ (NCP \geq 6 \wedge NCT \geq 6)\ then\ \ \frac{NCT + NCP}{2}\ else\ \ Reprovado$$

6 Datas Importantes

- Frequência: 24 de Maio de 2013.
- Defesa do ultimo exercício: última aula prática do semestre.
- Exame Época 1 : (conferir no site dos académicos)
- Exame Época 2 : (conferir no site dos académicos)
- Exame Época Especial : (conferir no site dos académicos)

7 Horário

O horário sofreu uma actualização. Novo horário:

Tipo de aula	**Horário**	**Sala**	**Docente**
Teórica	Segunda-Feira das 14h00 às 16h00	6.16	S. Melo de Sousa
Práticas Laboratoriais	Segunda-Feira das 16h00 às 18h00	6.16	S. Melo de Sousa

8 Atendimento

Horário	**Docente**
Sexta-Feira das 9h00 às 12h00	S. Melo de Sousa

9 Material Pedagógico e Funcionamento da Disciplina

Os Apontamentos serão atempadamente disponibilizados nas aulas e por meios electrónicos. É esperado e assumido que o aluno tenha lido os acetatos referentes ao capítulo em curso antes das aulas teóricas.

Teóricas

O material pedagógico apresentado nas aulas é entregue nas mesmas.

IMC = Introduction to Modern Cryptography (J. Katz and Y. Lindell)
CTP = Cryptography: Theory and Practice, Third Edition (D. R. Stinson)
HAC = Handbook of Applied Cryptography (A. J. Menezes, P. C. van Oorschot and S. A. Vanstone)

No geral, existe um paralelo forte com o excelente curso de Dan Boneh disponível no youtube e no coursera (vídeos, slides exercícios etc.).

9.1 Aula 1

Programa coberto: **Capítulo 1 do IMC** e Capítulo 1 do CTP.

Material alternativo:

Um artigo curto e simples sobre técnicas de leitura de material técnico ou científico (pdf).

Why Cryptosystems Fail , Ross Anderson

Criptografia Clássica:

- Documentário em Português.
- Uma intervenção pública relevante que resume o documentário *The Science of Secrecy* (adaptado do livro *The Code Book* de Simon Singh).
- Cifra de Vigenère em Brasileiro.
- Tabelas de Frequências na Língua Portuguesa

Aulas de Dan Boneh que cobram a matéria dada.
Introduction to Cryptography
What is Cryptography
History of Cryptography

9.2 Aula 2

Programa coberto: **Capítulo 2 de IMC** e capítulo 2 de CTP, Anexo A de IMC, capítulo 2 de HAC (2.1 e 2.2).

Material alternativo:

Discrete Probability for Cryptography - 1
Discrete Probability for Cryptography - 2
Information Theoretic security and the one time pad
Stream ciphers and pseudo random generators
Attacks on stream ciphers and the one time pad

9.3 Aula 3 e Aula 4

Programa coberto: **MIC capítulo 3** , CTP capítulo 8, HAC capítulo 2 (2.3), capítulos 5 e 6.

Material alternativo:

Analise de algoritmos, complexidade de algoritmos, classes de complexidade - Por Jorge Sousa Pinto (DIUM)

A Gentle Introduction to Algorithm Complexity Analysis
Real World Stream Ciphers
PRG Security Definition
Semantic Security
Stream Ciphers are semantically secure
What are block ciphers?
The Data Encryption Standard
Exhaustive search attacks
More attacks on block ciphers
The AES block cipher
Block ciphers from PRGs
Review: PRPs and PRFs
Mode of operation: one time key
Security for mani-time key
Modes of operation: many time key (CBC)
Modes of operation: many time key (CTR)

9.4 Aula 5

Programa coberto: **MIC capítulo 4** , CTP capítulo 4 , HAC capítulo 9.

Material alternativo:

Message Authentication Codes
MACs Based On PRFs
CBC-MAC and NMAC
MAC padding

PMAC and the Carter-Wegman MAC
Collision Resistance - Introduction
Generic Birthday attack
The Merkle-Damgard Paradigm
Constructing compression functions
HMAC
Timing attacks on MAC verification

Práticas

Exercícios da referência bibliográfica principal

Exercícios Práticos por entregar

- Selecção de exercícios da referência bibliográfica principal.
- Estudo (definição, conceito, propriedades – de segurança – e criptanalise) e implementação de um protocolo criptográfico escolhido em conjunto com a equipa docente.

10 Bibliografia Principal

A referências principal é:

- Introduction to Modern Cryptography, J. Katz and Y. Lindell. Chapman & Hall/CRC Press, 2007

Numa base frequente e regular utilizaremos as referências seguintes:

- Cryptography: Theory and Practice, (3nd Ed.) Douglas R. Stinson, CRC Press. 2005.
- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press.

Utilizaremos ocasionalmente as referências:

- A Classical Introduction to Cryptography Applications for Communications Security, Serge Vaudenay, Springer, pp. 370, 2005.

- A Classical Introduction to Cryptography Exercise Book, Thomas Baigneres, Pascal Junod, Yi Lu, Jean Monnerat, Serge Vaudenay, Springer, pp. 254, 2005.
- A Course in Number Theory and Cryptography (2nd Ed.), Neal Koblitz, Springer-Verlag, Graduate Texts in Mathematics, 1994.
- Applied Cryptography: Protocols, Algorithms and Source Code in C, Bruce Schneier, John Wiley & Sons.
- Lecture Notes on Cryptography, Shafi Goldwasser and Mihir Bellare (disponível online, via google)
- (advanced) The Foundations of Cryptography - Volume 1, Oded Goldreich, Cambridge University Press, 2001
- (advanced) The Foundations of Cryptography - Volume 2, Oded Goldreich, Cambridge University Press, 2004

Bibliografia complementar em Língua Portuguesa:

- Segurança no Software, Miguel Pupo Correia and Paulo Jorge Costa, FCA- Editora de Informática, 462, 2010.
- Segurança em Redes Informáticas. André Zúquete, FCA - Editora de Informática, 3ra Ed. (actualizada e aumentada), 2010.

Enviar comentários e dúvidas para (retire os UUU) : desousaUUU@UUUdi.ubi.pt