MC889/MO421 - Introdução a Criptografia
Prof. Diego Aranha
1º Semestre de 2017

1 Objetivos

A disciplina visa apresentar os conceitos essenciais sobre o projeto e implementação de primitivas criptográficas.

2 Programa

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

3 Avaliação

- 2 Avaliações Dissertativas P_1 e P_2, que contribuem com mesmo peso para a Média das Provas $P = (P_1+P_2)/2$. As avaliações serão realizadas nos dias 24/04 e 19/06;
- 3 Trabalhos Práticos T_1, T_2, T_3 individuais envolvendo a implementação de algoritmos e criptanálise. Para alunos de pós-graduação, T_3 será uma sequência de seminários sobre tópicos avançados. Os trabalhos contribuem com o mesmo peso para a Média dos Trabalhos $T = (T_1 + T_2 + T_3)/3$.

A Médial Parcial M será calculada pela expressão:

$$M = (T + P)/2.$$

Para MC889, a Média Final F será calculada pela expressão:

$$F = \begin{cases} M, & \text{se } M \geq 6 \\ (M + Exame)/2, & \text{se } M \geq 2,5 \\ M, \text{caso contrário.} \end{cases}$$

O Exame será realizado no dia 10 de Julho, no local e horário da aula. Só será permitida a realização do exame se a frequência for igual ou superior a 75%.

Para MO421, a Média Final F será calculada pela expressão:

$$F = \begin{cases} A, & \text{se } M \geq 8,5 \\ B, & \text{se } 7 \leq M < 8,5 \\ C, & \text{se } 5 \leq M < 7 \\ D, & \text{caso contrário.} \end{cases}$$

Qualquer tentativa de fraude ou plágio será resolvida com $F = 0$.

4 Bibliografia

- Undergrad: PAAR, Christof; PELZL, Jan. Understanding Cryptography, Springer, 2014.
- Undergrad: STINSON, Douglas. Cryptography: Theory and Practice. 3rd edition, CRC Press, 2006.
- Grad: KATZ, Johnathan; LINDELL, Yehuda. Introduction to Modern Cryptography, CRC Press, 2007.
- Auxiliary: MENEZES, Alfred. Handbook of Applied Cryptography. CRC Press, 2001. (`http://cacr.uwaterloo.ca/hac/`)

MC889/MO421 - Introduction to Cryptography
Prof. Diego F. Aranha
1st Term of 2017

1 Objectives

The course aims to familiarize the student with the design and implementation of cryptographic primitives.

2 Program

- Classical Cryptography: algorithms and cryptanalysis.
- Shannon Theory: entropy and perfect secrecy.
- Block ciphers: DES and AES.
- Cryptographic Hash Functions and Message Authentication Codes.
- RSA and Rabin cryptosystems.
- Discrete Log-based Asymmetric Encryption.
- Digital signature schemes.
- Random number generation.

3 Evaluation

- 2 Written Tests T_1 and T_2 which contribute with the same weight to $T = (T_1 + T_2)/2$. The dates for the written tests are April 24 and June 19.
- 3 Individual Projects P_1, P_2 and P_3 involving implementation of algorithms and cryptanalysis. For graduate students, P_3 will be a short sequence of seminars. They contribute with the same weight to $P = (P_1 + P_2 + P_3)/3$.

The final score M will be computed by the expression:

$$M = (T + P)/2.$$

For MC889, the final grade F will be computed by the expression:

$$F = \begin{cases} M, & \text{se } M \geq 6 \\ (M + Exam)/2, & \text{se } M \geq 2,5 \\ M, \text{otherwise.} \end{cases}$$

The undergraduate Exam is scheduled to April 10th at the same time and place for the classes. Students taking the $Exam$ must satisfy a 75% attendance rate.

For MO421, the final grade F will be computed by the expression:

$$F = \begin{cases} A, & \text{if } M \geq 8,5 \\ B, & \text{if } 7 \leq M < 8.5 \\ C, & \text{if } 5 \leq M < 7 \\ D, & \text{otherwise.} \end{cases}$$

Any attempt at fraud or plagiarism will be resolved with $F = 0$. Attendance in class will not be evaluated for graduate students.

4 Bibliografia

- Undergrad: PAAR, Christof; PELZL, Jan. Understanding Cryptography, Springer, 2014.
- Undergrad: STINSON, Douglas. Cryptography: Theory and Practice. 3rd edition, CRC Press, 2006.
- Grad: KATZ, Johnathan; LINDELL, Yehuda. Introduction to Modern Cryptography, CRC Press, 2007.
- Auxiliary: MENEZES, Alfred. Handbook of Applied Cryptography. CRC Press, 2001. (also available at `http://cacr.uwaterloo.ca/hac/`)