Criptografie și Securitate

- Prelegerea 0 -
Informații administrative

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

1. Cadre didactice
2. Reguli
3. Organizare și evaluare
4. Structura cursului
5. Referințe bibliografice

Cadre didactice

Adela Georgescu

adela@fmi.unibuc.ro

Ruxandra F. Olimid

ruxandra.olimid@fmi.unibuc.ro

www.ruxandraolimid.weebly.com

Reguli

1. Sunt prezent pentru că mă interesează!
2. Nu deranjez pentru că nu imi place să fiu deranjat!
3. Întreb pentru că vreau să știu!

Organizare și evaluare

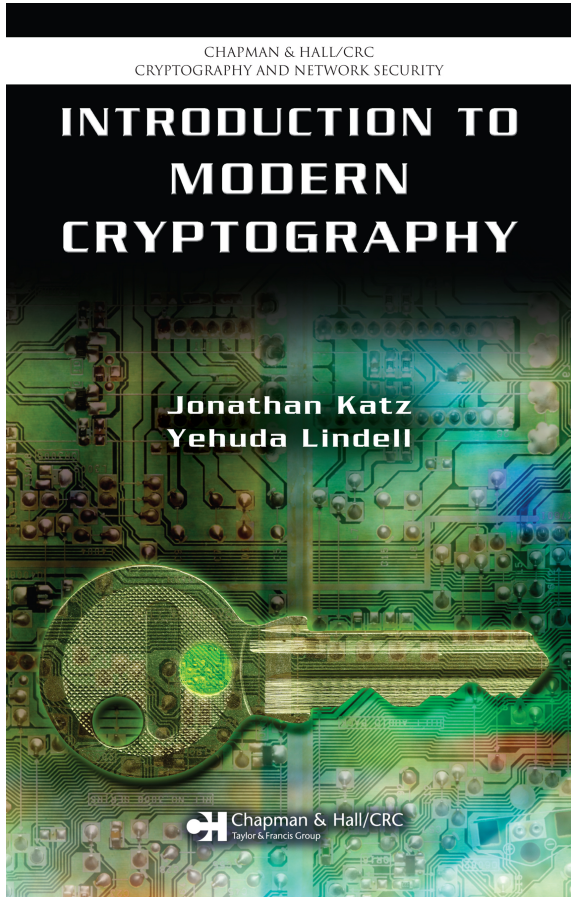
1. Organizare:
   - 2h curs / sapt
   - 2h seminar / 2 sapt
   - 2h laborator / 2 sapt
2. Evaluare:
   - 60 % examen (cu materiale)
   - 20 % seminar
   - 20 % laborator
3. Condiții de promovare:
   - $\geq$ 50 % din sem. + lab. (pentru participare la examen!)
   - $\geq$ 50 % din examen

`http://ruxandraolimid.weebly.com/cryptography.html`

Structura cursului

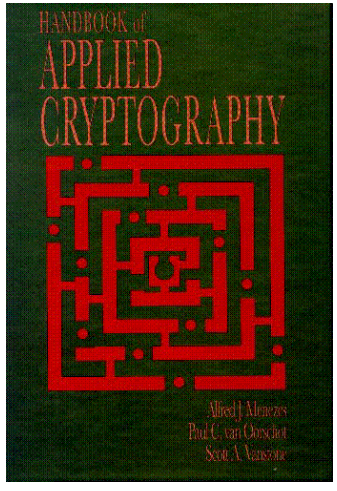
1. Introducere. Motivație. Principii.
2. Sisteme istorice de criptare
3. Securitate perfectă. One time pad.
4. Criptografia computațională. Pseudoaleatorismul.
5. Sisteme de criptare fluide.
6. Sisteme de criptare bloc.
7. Integritatea mesajelor (MAC). Funcții Hash.
8. Noțiuni de teoria numerelor. Probleme dificile în criptografie.
9. Criptografia cu cheie publică.
10. Criptografia pe curbe eliptice.

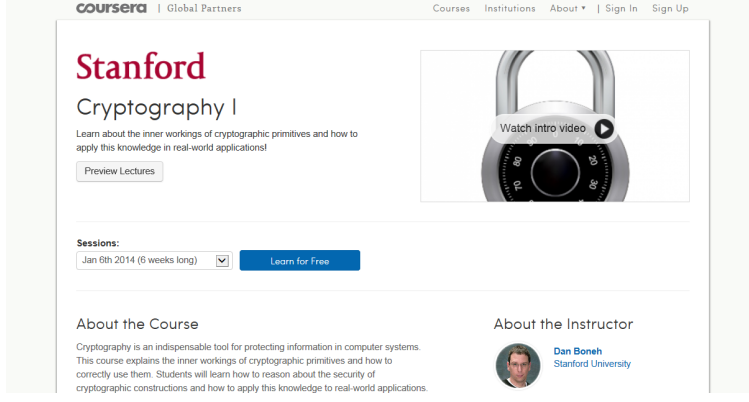
Referințe bibliografice



`http://www.cs.umd.edu/~jkatz/imc.html`

Referințe bibliografice





`http://cacr.uwaterloo.ca/hac/` https://www.coursera.org/course/crypto