Criptografie și Securitate

- Prelegerea 0 -
Informații administrative

Ruxandra F. Olimid

(multe slide-uri preluate din cursul comun realizat impreuna cu Adela Georgescu)

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Cadre didactice

Ruxandra F. Olimid

ruxandra.olimid@fmi.unibuc.ro

www.ruxandraolimid.weebly.com

UNIVERSITATEA DIN BUCUREȘTI
VIRTUTE ET SAPIENTIA

NTNU

Seminar, Laborator:

Diana Maimut, George Teseleanu
Cosmin Obretin, Ionut-Daniel Dobos

Ce aștept de la voi?

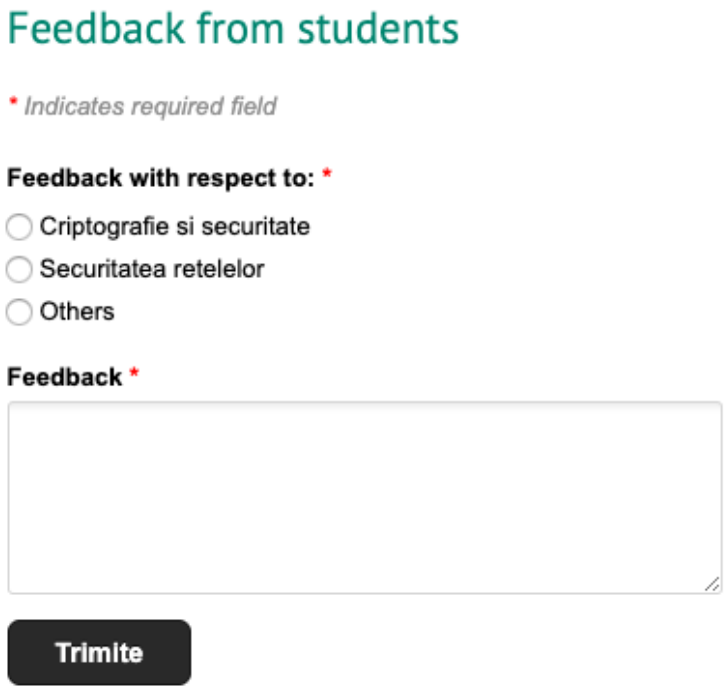
Sunt prezent pentru că mă interesează!

Studiez individual

Întreb pentru că vreau să știu!

Promovez (cu o notă bună)

Ce așteptați voi de la mine?



`http://ruxandraolimid.weebly.com/feedback-from-students.html`

Organizare și evaluare

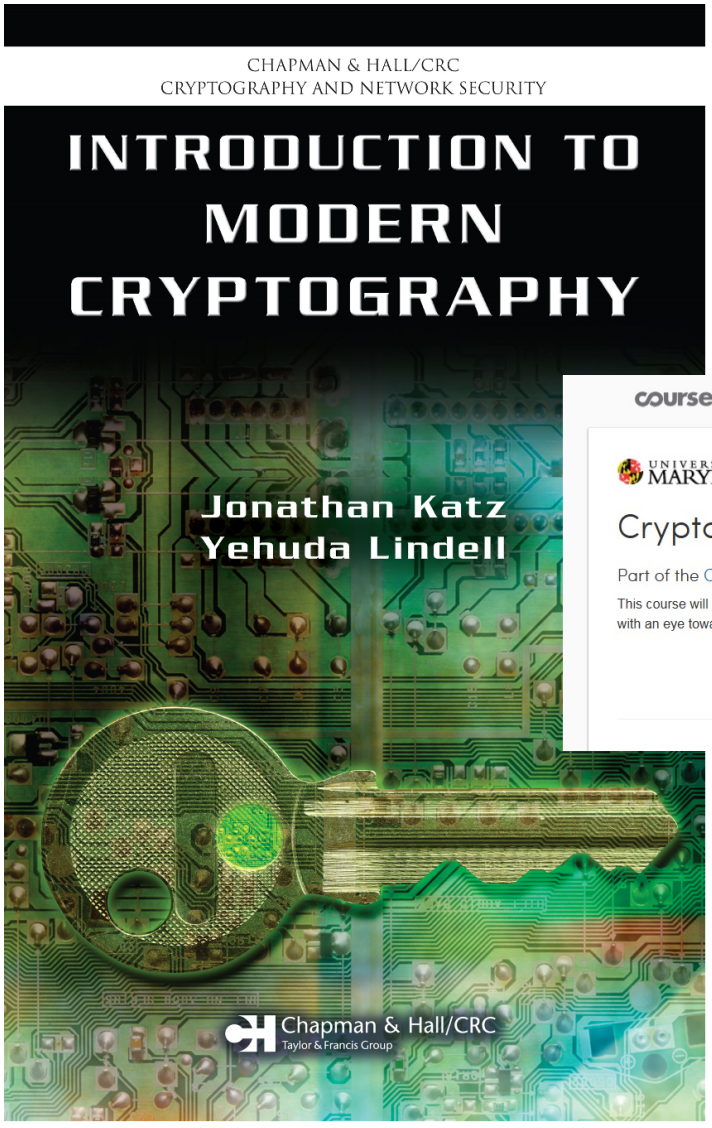
1. Organizare:
   - 2h curs / săpt
   - 2h seminar / 2 săpt
   - 2h laborator / 2 săpt
2. Evaluare:
   - 60 % examen (cu materiale)
   - 10 % seminar
   - 10 % laborator
   - 10 % proiect (deadlines!)
   - 10 % temă (deadlines!)
   - +10% bonus :)
3. Condiții de promovare:
   - $\geq$ 45 % din examen
   - $\geq$ 45 % din total

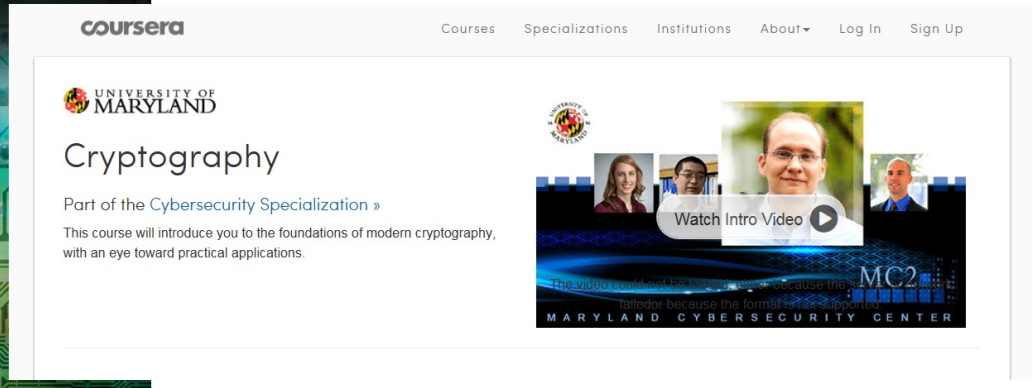
 Moodle: Crypto

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.
11. Alte topici de criptografie.

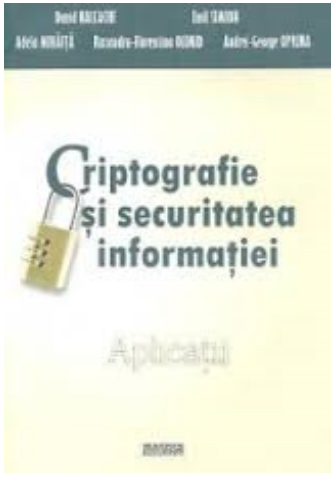
Referințe bibliografice

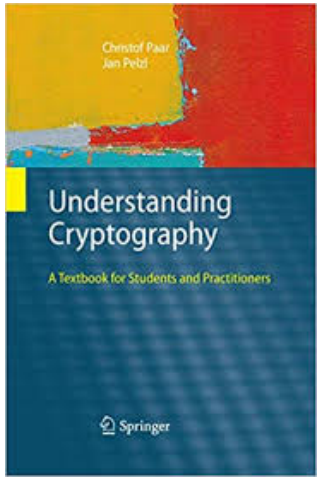


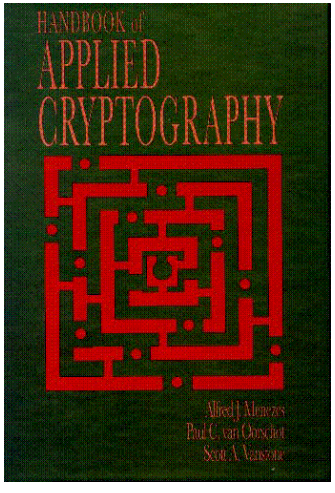


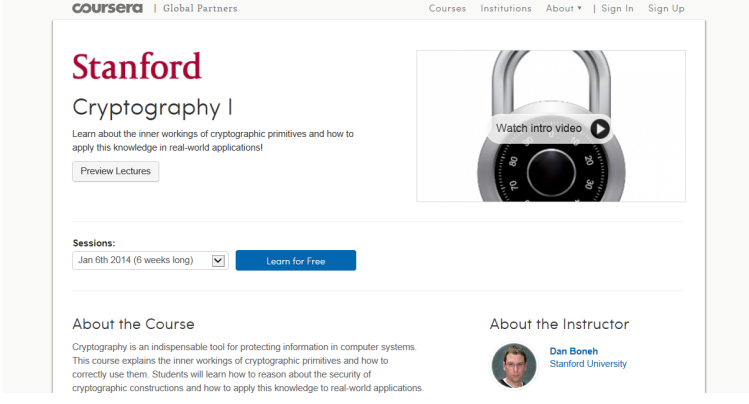
http://www.cs.umd.edu/~jkatz/imc.html

Referințe bibliografice









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