Coordonator: Conf. Mihai Prunescu

1. Ayushi: A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15. 2010. http://www.ijcaonline.org/journal/number15/pxc387502.pdf

2. Ian Goldberg, David Wagner: Randomness and the netscape Browser. How secure is the World Wide Webb. Dr. Dobb Journal, January 1996. https://people.eecs.berkeley.edu/~daw/papers/ddj-netscape.html

Observatie: Articolele 1 si 2 sunt foarte scurte asadar ar trebui pregatite de un singur student care face o prezentare combinata.

3. Daniel J. Bernstein: Protecting communications against forgery. Algorithmic Number Theory, Volume 44, 2008. 535 – 549 https://cr.yp.to/antiforgery/forgery-20080501.pdf

Observatie: Articolul 3 este consistent. A se lua de catre un student bun.

4. Jeffrey R. Yost: An Interview with MARTIN HELLMAN. Charles Babbage Institute, Center for the History of Information Technology, University of Minnesota, Minneapolis, 2004. (interviu de 59 de pagini) https://conservancy.umn.edu/bitstream/handle/11299/107353/oh375mh.pdf?sequence=1&isAllowed=y

Observatie: Fiind vorba despre un interviu foarte dens, dar fara nici o urma de matematica formala, ar fi prea greu pentru un student sa faca o prezentare de seminar. Il putem recomanda insa tuturor ca lectura interesanta.

##########

5. David Jao, Luca De Feo: Towards quantum-resistant cryptosystems from supersingular

elliptic curve isogenies. preprint.

https://web.archive.org/web/20120507222310/http://eprint.iacr.org/2011/506.pdf

Observatie: Este cel mai greu articol deoarece contine foarte multa geometrie algebrica. E nevoie de un student foarte bun, care nu se sperie usor.

##########

6. Certicom Research: Standards for Efficient Cryptography: Sec. 1, Elliptic Curves. 2009 https://web.archive.org/web/20141111191126/http://www.secg.org/sec1-v2.pdf

Observatie: Un student ne poate trece in revista tot ansamblul de standarde folosite in criptografia practica la nivelul anului 2009. Textul este atat matematic cat si tehnologic explicit. Studentul trebuie sa realizeze o vedere de ansamblu a situatiei.

##########

7. Dan Boneh: Twenty Years of Attacks on the RSA Cryptosystem. preprint. http://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf

Observatie: Foarte multa teoria numerelor. Sa faca cat poate. Se poate imparti eventual la doi studenti.

##########

8. M. Bellare, P. Rogaway *Optimal Asymmetric Encryption -- How to encrypt with RSA* extended abstract in Advances in Cryptology - Eurocrypt '94 Proceedings, Lecture Notes in Computer Science Vol. 950, A. De Santis ed, Springer-Verlag, 1995. http://cseweb.ucsd.edu/~mihir/papers/oae.pdf

Observatie: Articol tipic de criptografie. Cred ca poate fi facut de un student, macar asa, in principiu.

9. Laura Hitt: On the Minimal Embedding Field. preprint. https://eprint.iacr.org/2006/415.pdf

Observatie: Alt articol de geometrie algebrica, dar mai usor decat cel de la punctul 5. Poate de preferat aceluia.