Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Planilla a completar para presentación de Cursos de Posgrado

1.- DEPARTAMENTO de COMPUTACIÓN

2.- NOMBRE DEL CURSO: Criptografía Moderna

3.- DOCENTES:

RESPONSABLE/S: Juan A. Garay
COLABORADORES: Yuval Ishai, Hugo Krawczyk, Vassilis Zikas
AUXILIARES: .....

4.- CARRERA de DOCTORADO

5.- AÑO: 2018 CUATRIMESTRE/S: Invierno

6.- PUNTAJE PROPUESTO PARA CARRERA DE DOCTORADO: ½ punto

7.- DURACIÓN (anual, cuatrimestral, bimestral u otra): Única vez

8.- CARGA HORARIA SEMANAL:

Teóricas: .....
Problemas: .....
Laboratorio: .....
Seminarios: .....
Teórico – Práctico: 20 horas
Salida a Campo: .....

9.- CARGA HORARIA TOTAL: 20 horas

10.- FORMA DE EVALUACIÓN: Examen final

11.- PROGRAMA ANALÍTICO:
1. Introduction to Modern Cryptography.
2. Design and Analysis of Authenticated Key-Exchange Protocols.
3. Secure Multi-Party Computation.
4. Homomorphic Secret Sharing and Applications.

5. Foundations and Applications of Blockchain Protocols.

12.- BIBLIOGRAFÍA:

- M. Bellare and P. Rogaway, "Entity authentication and key distribution", Advances in Cryptology, CRYPTO'93, Lecture Notes in Computer Science Vol. 773, D. Stinson ed, Springer-Verlag, 1994, pp. 232-249. https://cseweb.ucsd.edu/~mihir/papers/eakd.pdf
- E. Boyle, G. Couteau, N. Gilboa, Y. Ishai and M Orru, ``Homomorphic Secret Sharing: Optimizations and Applications." ACM CCS 2017: 2105-2122
- E. Boyle, N. Gilboa and Y. Ishai, ``Function Secret Sharing: Improvements and Extensions." ACM CCS 2018: 1292-1303
- E. Boyle, N. Gilboa, Y. Ishai, H. Lin and S. Tessaro, ``Foundations of Homomorphic Secret Sharing." ITCS 2018: 21:1-21:21
- R. Canetti and H. Krawczyk, ``Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels", Advances in Cryptology -- EUROCRYPT 2001 Proceedings, Lecture Notes in Computer Science, Vol.~2045, Springer-Verlag, B. Pfitzmann, ed, 2001, pp. 453--474. http://eprint.iacr.org/2001/040
- J. Garay, Y. Ishai, R. Ostrovsky and V. Zikas, ``The Price of Low Communication in Secure Multi-party Computation." CRYPTO (1) 2017: 420-446. https://eprint.iacr.org/2017/520
- J. Garay, A. Kiayias and N. Leonardos, ``The Bitcoin Backbone Protocol: Analysis and Applications." EUROCRYPT (2) 2015: 281-310. https://eprint.iacr.org/2014/765
- J. Garay, A. Kiayias and N. Leonardos, ``The Bitcoin Backbone Protocol with Chains of Variable Difficulty." CRYPTO (1) 2017: 291-323. https://eprint.iacr.org/2016/1048
- J. Garay, A. Kiayias, N., Leonardos and G. Panagiotakos, ``Bootstrapping the Blockchain, with Applications to Consensus and Fast PKI Setup." Public Key Cryptography (2) 2018: 465-495. https://eprint.iacr.org/2016/991
- C. Hazay and Y. Lindell, **Efficient Secure Two-Party Protocols - Techniques and Constructions.** Information Security and Cryptography, Springer 2010, ISBN 978-3-642-14302-1, pp. 3-254
- O. Goldreich, **Foundations of Cryptography, Volume 2, Basic Applications, 1st Edition.** Cambridge University Press, ISBN-13: 978-0521119917

- O. Goldreich, S. Micali and A. Wigderson, ``How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. STOC 1987: 218-229
- J. Katz and Y. Lindell, **Introduction to Modern Cryptography, Second Edition.** CRC Press 2014, ISBN 9781466570269
- H. Krawczyk, `SIGMA: the `SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and its Use in the IKE Protocols", Advances in Cryptology -- CRYPTO 2003 Proceedings, Lecture Notes in Computer Science, Vol. 2729, Springer-Verlag, D. Boneh, ed, 2003, pp.~399--424. webee.technion.ac.il/~hugo/sigma-pdf.pdf
- D. Stinson, **Cryptography: Theory and Practice, Third Edition.** CRC Press 2005, ISBN 9781584885085