UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
BLOC-524DL	Cryptographic Systems Security	10
Prerequisites	**Department**	**Semester**
BLOC-511DL	Digital Innovation	Fall/Spring
Type of Course	**Field**	**Language of Instruction**
Elective	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
2nd Cycle	Dr. Theodosis Mourouzis	2nd
Mode of Delivery	**Work Placement**	**Corequisites**
Distance Learning	N/A	N/A

Course Objectives:

- Understanding of the basic security requirements such as confidentiality, integrity, authenticity, anonymity and how these requirements can be met.
- Detailed study of cryptographic primitives such as encryption/decryption, hash functions, digital signatures, message authentication codes.
- Detailed study of the security of the aforementioned cryptographic primitives and methods to attack them.
- Understanding the purpose that these cryptographic primitives serve to the design of Blockchain or Distributed Ledger Technologies (DLTs) related systems.
- Compare several Blockchain and DLT frameworks from crypto point of view.
- Understanding of several attacks on Blockchain or DLT schemes.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. Understand fundamental security requirements such as confidentiality, integrity, authenticity, and anonymity.
2. Understand the basic cryptographic primitives and how these are combined in order to design Blockchain or DLT related schemes.
3. Understand possible attacks on cryptographic primitives by understanding how to attack

the underlying computational hard problems on which the security of these primitives relies.
4. Understand possible attacks on different Blockchain or DLT schemes.
5. Conduct security evaluation of such systems from a crypto point of view.
6. Categorizing different Blockchain or DLT networks with respect to their crypto design.

Course Content:

1. Introduction to security requirements(confidentiality, integrity, authenticity, anonymity, non-repudiation) and computational hard problems (integer factoring, discrete logarithm problem etc)
2. Cryptographic design and crypto primitives: confusion, diffusion, avalanche effect, notion of randomness, encryption decryption (symmetric & asymmetric), hash functions, message authentication codes, digital signatures (multi-signature schemes, ring signatures), zero knowledge proofs, key exchange protocols
3. Cryptographic attacks: attacks on encryption protocols, hash function attacks
4. Cryptography for Blockchain or DLTs: blocks, Merkle Trees, hashchain, on the longest chain, soft/hard forks, challenges (scalability, anonymity, interoperability)
5. Cryptography for digital currencies/tokens: wallets (hot, cold, custodian), multi-signature wallets, hierarchical deterministic wallets
6. Attack Frameworks for Blockchain or DLTs: 50+1 attack, eclipse attack, selfish miner attack, attacks on wallets
7. Consensus Algorithms: proof of work, proof of stake, delegated proof of stake, proof of memory/space, proof of elapsed time, multisignature scheme, Byzantine fault, tolerance, federated Byzantine agreement
8. Study of different Blockchain/DLT frameworks from crypto perspective: Bitcoin, Ripple, Monero

Learning Activities and Teaching Methods:

Lectures, Live Discussions, Course Forum discussions, Case-study analyses

Assessment Methods:

Written and programming assignments, mid-term exam, final exam

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Applied Cryptography: Protocols, Algorithms and Source Code in C	Bruce Schneier	Wiley Publications	2015	
Security In Computing. 5th Edition	Charles P. Pfleeger And Shari Lawrence Pfleeger	Prentice Hall Publications	2018	
Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)	Alfred J. Menezes, Jonathan Katz, Paul C. van Oorschot, Scott A. Vanstone.	CRC Press Publications	1996	

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Short Intro to Crypto World. Optimizations in algebraic and differential cryptanalysis.	Theodosis Mourouzis	University College London, UK	2016	

Recommended Articles/ Reading List:

- Claude E. Shannon. *Communication theory of secrecy systems*. Bell System Technical Journal 28 (1949)
- Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system.*Available:

http://www.bitcoin.org/ bitcoin.pdf (2009)

- Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. *NISTIR 8202 Blockchain Technology Overview.* This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8202 (2018)

- Miers, C. Garman, M. Green, A. D. Rubin. *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, in 2013 IEEE Symposium on Security and Privacy, San Francisco, CA, pp 397-411 (2013)

- R.C. Merkle. *Protocols for public key cryptosystems*. In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980 (1980)