



Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-530	Cryptographic Systems Security	10
Prerequisites	Department	Semester
DFIN-511	Computer Science	Fall/Spring/Summer
Type of Course	Field	Language of Instruction
Elective	Computer Science	English
Level of Course	Lecturer(s)	Year of Study
2 nd Cycle	Dr. Theodosios Mourouzis	2nd
Mode of Delivery	Work Placement	Co-requisites
Distance Learning	N/A	N/A

Course Objectives:

The main objectives of the course are to:

- 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:

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

- Understand fundamental security requirements such as confidentiality, integrity, authenticity, and anonymity.
- Understand the basic cryptographic primitives and how these are combined in order to design Blockchain or DLT related schemes.
- Understand possible attacks on cryptographic primitives by understanding how to attack the underlying computational hard problems on which the security of these primitives relies.

- Understand possible attacks on different Blockchain or DLT schemes.
- Conduct security evaluation of such systems from a crypto point of view.
- Categorizing different Blockchain or DLT networks with respect to their crypto design.

Course Content:

- Introduction to security requirements(confidentiality, integrity, authenticity, anonymity, non-repudiation) and computational hard problems (integer factoring, discrete logarithm problem etc)
- 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
- Cryptographic attacks: attacks on encryption protocols, hash function attacks
- Cryptography for Blockchain or DLTs: blocks, Merkle Trees, hashchain, on the longest chain, soft/hard forks, challenges (scalability, anonymity, interoperability)
- Cryptography for digital currencies/tokens: wallets (hot, cold, custodian), multi-signature wallets, hierarchical deterministic wallets
- Attack Frameworks for Blockchain or DLTs: 50+1 attack, eclipse attack, selfish miner attack, attacks on wallets
- 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

Study of different Blockchain/DLT frameworks from crypto perspective: Bitcoin, Ripple

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	978-1-119-09672-6

Security In Computing, 5th Edition	Charles P. Pfleeger And Shari Lawrence Pfleeger	Prentice Hall Publications	2018	9780134085043
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	978-0849385230

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Optimizations in algebraic and differential cryptanalysis.	Theodosios Mourouzis	University College London, UK	2015	Online
Bitcoin: A peer-to-peer electronic cash system	Satoshi Nakamoto		2009	Online
NISTIR 8282,Blockchain Technology Overview	Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone		2018	Online
ZeroCoin: Anonymous Distributed E-Cash from Bitcoin, in 2013 IEEE Symposium on Security and Privacy, San Francisco, CA, pp 397- 411	Miers, C. Garman, M. Green, A. D. Rubin		2013	Online

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