Titolo del corso: A Pragmatic Introduction to Cryptography

Docente: Filippo Valsorda

Membro del collegio proponente: Giovanni Paolini
Ore frontali di lezione: 20h
Periodo di lezione: 30 marzo - 8 maggio (due lezioni di 2h a settimana, con una settimana di pausa)
Settore disciplinare del corso: INFO-01/A
Tipologia di corso: base
Modalità di verifica dell'apprendimento: presentazione di progetto

Abstract del corso:

An applied introduction to cryptography engineering, focusing on how cryptographic primitives work and how they are used to build real-world cryptosystems, presented from the perspective of a cryptography implementer and specification author. More applied than an Applied Cryptography course, we will avoid most formalisms and theoretical proofs, and explore how building blocks fit together to provide concrete security outcomes. The course assumes no pre-existing knowledge of cryptography, but can greatly benefit from some knowledge of any programming language.

Programma del corso:

1. Introduction: what cryptography does, the one security level, entropy and randomness
2. Symmetric encryption: stream and block ciphers, nonces, authenticated encryption
3. Hashes: hashes, PRFs, ciphers, MACs, and KDFs and how to turn each into each other
4. Asymmetric cryptography: quantum computers, legacy hard problems, and why no more RSA
5. Key exchange: Diffie-Hellman, prime order groups, KEMs, ML-KEM, and hybrid encryption
6. Signatures: ECDSA and its nonces, EdDSA and Schnorr and the Fiat–Shamir, ML-DSA, SLH-DSA
7. Protocols: TLS, X.509, SSH, Noise, age, and how everything is a protocol
8. Fancy crypto: Merkle trees, zero-knowledge proofs, threshold signatures, MPC, FHE
9. Realities: specifications, key management, libraries, testing, side-channels, and moral character
10. Recap and exam project preparation