

Crypto 2016-17

Ημ/νια	Τίτλος
04/10/16	Intro
07/10/16	Κλασσικά κρυπτοσυστήματα
11/10/16	Θεωρία αριθμών, ομάδων
14/10/16	Θεωρία αριθμών, ομάδων
18/10/16	Θεωρία αριθμών, ομάδων
21/10/16	Θεωρία αριθμών, ομάδων
25/10/16	Έλεγχος πρώτων, παραγοντοποίηση
01/11/16	Pseudorandom, stream ciphers
04/11/16	DES, AES
08/11/16	One-way, hash, Merkle trees
11/11/16	HMAC
18/11/16	Εφαρμογές hash
22/11/16	Παίγνια, Diffie-Hellman
25/11/16	RSA
29/11/16	Διακριτός λογάριθμος, ελλειπτικές καμπύλες
02/12/16	Ψηφιακές υπογραφές I
06/12/16	Ψηφιακές υπογραφές II
09/12/16	Zero knowledge proofs
13/12/16	Πρωτόκολλα
16/12/16	Εκλογές I
20/12/16	Εκλογές II
10/01/17	Επιθέσεις https
13/01/17	blockchain/bitcoin
17/01/17	projects
20/01/17	projects