13/12/2024					
19.45-20.15	Αθανάσιος	Τάχος	CSCYB24043	Deterministic Random Bit Generator Mechanisms (Hash_DRBG and HMAC_DRBG, CTR_DRBG)	
	ΚΩΝΣΤΑΝΤΙΝΑ	ΣΜΑΡΝΑΚΗ	CSCYB24032		NIST SP 800-90A
	ΣΤΑΥΡΟΥΛΑ	ΑΡΜΕΝΙΑΚΟΥ	CSCYB24004		https://doi.org/10.6028/NIST.SP.800-90Ar1
20.15-20.45	Θεόδωρος	Αλεξόπουλος	CSCYB24002	Recommendation for the Entropy Sources Used for Random Bit Generation	
	ΑΓΓΕΛΟΣ	ΔΡΥΛΕΡΑΚΗΣ	CSCYB24011		(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf)
	Ευστάθιος	Μίντζιας	CSCYB24024		
21.00-21.30	ΙΩΑΝΝΗΣ -	ΚΑΡΑΝΤΑΚΗΣ	CSCYB24015	Recommendation for Random Bit Generator (RBG) Constructions	
	ΒΑΣΙΛΕΙΟΣ	ΠΑΠΠΑΣ	CSCYB24029		(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.4pd.pdf)
	ΕΛΕΥΘΕΡΙΟΣ	ΧΑΡΑΛΑΜΠΙΔΗΣ	CSCYB24039		
21.30-22.00	ΑΛΕΞΑΝΔΡΟΣ	ΒΑΡΣΟΣ	CSCYB24050	AES-Keywrap	
	ΧΡΙΣΤΙΝΑ	ΜΕΜΑ	Cscyb22012		NIST SP800-38F (algorithms KW and KWP)
	Ελευθέριος	Ντόκος	CSCYB24055		
20/12/2024					
19.45-20.15	ΠΑΝΑΓΙΩΤΗΣ	ΚΑΤΕΡΙΝΟΠΟΥΛΟΣ	**CSCYB24016**	XTS and FF1 encryption mode	NIST SP 800-38E
	ΧΡΗΣΤΟΣ-ΣΤΕΦΑΝ	ΚΑΨΙΜΑΛΗΣ	**CSCYB24018**		NIST SP 800-38G
	Φωτιος	Χόχλακας	**CSCYB24040**		
20.15-20.45	ΜΗΝΑΣ	ΜΠΑΤΜΑΝΟΓΛΟΥ	**CSCYB24026**	Salsa, Chacha20, poly1305	
	ΔΗΜΗΤΡΙΟΣ	ΣΙΣΚΟΣ	**CSCYB24031**		RFC7539
	ΒΑΣΙΛΕΙΟΣ	ΣΤΑΜΟΣ	**CSCYB24033**		https://www.rfc-editor.org/rfc/pdfrfc/rfc7539.txt.pdf
21.00-21.30	Βασιλική	Παππά	**CSCYB24028**	Ascon-Based Lightweight Cryptography	
	ΚΩΝΣΤΑΝΤΙΝΟΣ	ΚΕΦΑΛΑΣ	**CSCYB24019**		https://csrc.nist.gov/pubs/sp/800/232/ipd
	ΣΕΡΑΦΕΙΜ	ΤΡΙΑΝΤΑΦΥΛΛΟΥ	**CSCYB24037**		
21.30-22.00	Λάμπρος	Γκαναβίας	**CSCYB24008**	EdDSA, Ed25519 and Ed448	
	Λάμπρος	Μανούσος	**CSCYB24023**		RFC8032
	ΑΝΤΩΝΙΟΣ	ΑΛΥΚΑΡΙΔΗΣ	**CSCYB24003**		https://datatracker.ietf.org/doc/html/rfc8032
10/1/2025					
19.45-20.15	ΚΩΝΣΤΑΝΤΙΝΟΣ	ΚΑΡΑΓΙΑΝΝΗΣ	**CSCYB24014**	Blinded Signatures	
	ΜΑΡΙΑ	ΛΑΜΠΡΟΥ	**CSCYB24021**		https://asecuritysite.com/blind/
	Χρήστος	Αρχοντάκης	**CSCYB24005**		
20.15-20.45	Ευαγγελία	Φενέκου	**CSCYB24056**	Bleichenbacher Attack on RSA PKCS #1 v1.5 For Encryption Robot attack	
	Απόστολος	Καψάλης	**CSCYB24052**		(Check the web for references)
	ΒΑΣΙΛΕΙΟΣ	ΧΑΤΖΗΠΑΝΑΓΙΩΤΗΣ	**CSCYB24058**		
20.45-21.15	Δημήτριος	Δημοβασίλης	**CSCYB24009**	Διαχείριση κλειδιών στο σύστημα Signal	https://signal.org/
	Βάιος	Ευθυμιόπουλος	**CSCYB24012**		
	Εμμανουήλ	Τσινιδέλος	**CSCYB24038**		
21.15-21.45	ΝΙΚΟΛΑΟΣ	ΓΚΙΝΗΣ	cscyb23047	Oblivious transfer and TinyOT	
	Ραφαήλ	ΔΟΥΛΦΗΣ	**CSCYB24010**		https://eprint.iacr.org/2020/300.pdf
	Ηλίας	Τζανετουλάκος	**CSCYB24035**		
17/1/2024					
19.45-20.15	ΧΑΡΙΛΑΟΣ	ΒΙΤΩΡΑΚΗΣ	**CSCYB24006**	Argon2 και Bcrypt	https://www.cryptolux.org/images/0/0d/Argon2.pdf
	ΒΑΣΙΛΙΚΗ - ΜΑΡΙΑ	ΚΑΤΣΟΥΛΗ	**CSCYB24017**		RFC 7914

	ΝΙΚΟΛΑΟΣ	ΜΟΥΤΑΒΕΛΗΣ	**CSCYB24025**		https://datatracker.ietf.org/doc/html/rfc7914
20.15-20.45	ΚΩΝΣΤΑΝΤΙΝΟΣ	ΑΛΕΞΙΟΥ	**CSCYB24001**	PBKDF and HKDF	RFC2898
	ΝΙΚΟΛΑΟΣ	ΓΚΟΡΓΚΟΛΗΣ	**CSCYB23011**		https://www.ietf.org/rfc/rfc2898.txt
	Γεράσιμος	Τζάκης	**CSCYB24034**		RFC 5869
21.00-21.30	Χαράλαμπος	Ευμορφίδης	**CSCYB24051**	Salted hashes and HashWires	
	Ηλίας	Μπέλλος	**CSCYB24053**		https://eprint.iacr.org/2021/297
	Νικόλαος	Νανης	**CSCYB24054**		
21.30-22.00	Αθανάσιος	Γεωργίου	**CSCYB24007**	Oblivious RAM	Path ORAM
	Γεώργιος-Ραφαήλ	Κιουρτάκης	**CSCYB24020**		Circuit ORAM
	Ιωάννης	Μπρώνης	**CSCYB24027**		
22.00-22.15	ΓΕΩΡΓΙΟΣ	ΜΕΛΕΤΙΟΥ	cscyb21017	Επίθεση POODLE	(Check the web for references)