TEK4500 - Schedule 2022

Note: this is a *preliminary* schedule for the semester. Changes will most likely happen.

Lecture	Date	Topic	Recommended reading
1	24.08	Introduction to cryptography, historical ciphers, perfect privacy, one-time pad	Chapter 1+2 in [BR]
2	31.08	Block ciphers, PRF/PRPs, AES, DES	Chapter 3 + 4 in [BR] (4.8–4.10 can be skipped)
3	07.09	Symmetric encryption, IND-CPA, CTR/CBC-mode	Chapter 5 in [BR] (5.6+5.8 can be skipped)
4	14.09	MACs, UF-CMA, CBC-MAC, CMAC	Chapter 7 in [BR] (7.8 can be skipped)
5	21.09	Authenticated encryption, IND-CCA, AE, GCM-mode	Note
6	28.09	Hash functions, SHA1/SHA2, HMAC	Chapter 6 + Appendix A (birthday problem) in [BR], Chapter 11 [PP]
7	05.10	Randomness and entropy, random number generators, PRNGs, stream ciphers	TBD
8	12.10	Group theory, Diffie-Hellman key exchange, the discrete logarithm problem	Chapter 9 + 10.1–10.2 in [BR] (9.4 can be skipped)
9	19.10	Diffie-Hellman II, elliptic curves, backdoors	
10	26.10	Diffie-Hellman III, computational aspects	Chapter 8 + 9 in [PP] (8.5 can be skipped)
11	02.11	Public-key encryption, IND-CPA, ElGamal, RSA, the factoring problem	Chapter 11 + Chapter 10.3 in [BR]
12	09.11	Digital signatures, UF-CMA, Schnorr, RSA, Public-key infrastructure (PKI)	Chapter 12 in [BR] (12.3.6 can be skipped), Chapter 10 in [PP] (10.3 can be skipped)
13	16.11	Quantum computers, Shor's algorithm, post-quantum cryptography	TBD

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[PP] Christof Paar and Jan Pelzl. *Understanding Cryptography - A Textbook for Students and Practitioners*. Springer, 2010.

[Ros] Mike Rosulek. *The Joy of Cryptography*, (draft Feb 6, 2020). https://web.engr.oregonstate.edu/~rosulekm/crypto/crypto.pdf.