Checklist “Do I meet the prerequisites?”

NOTE: You should also do the attached “Homework I: Cryptographic Background” to recall the most important concepts in this checklist!

For this course, you are expected to have a working knowledge of the following concepts
For each concept, a reference to “Homework I” or to the specific section explaining the concept in Nigel Smart’s textbook [Sma] is given. You may use these references to rehearse the concept at hand.

☐	Basic Maths: Modular Arithmetic, Groups, Finite Fields, and Probability	[Sma, Ch. 1]
☐	Cryptographic Hash Functions and Message Authentication Codes	[Sma, Ch. 10]
☐	Secret-Key Cryptography (Stream and Block Ciphers)	[Sma, Ch. 7-8]
☐	Public-Key Cryptography (Encryption, Signatures, Key Exchange)	[Sma, Ch. 11+14]
☐	Negligibility (as in “negligible probability”)	[Sma, Ch. 20]
☐	Discrete Logarithm Based Problems: DLP, DHP, DDH	Homework I
☐	Game-Based Security Definitions and Security Proofs	Homework I
☐	ElGamal Encryption and its CPA-Security	Homework I

References

[Sma] Nigel Smart. *Cryptography: An Introduction*. Third Edition, 2013. Available at https://www.cs.bris.ac.uk/~nigel/Crypto_Book/.

Homework I: Cryptographic Background

Privacy Enhancing Technologies (201500042)

1. **DLP, DHP, DDH** Recall the Discrete Logarithm Problem (DLP), the Diffie–Hellman Problem (DHP), the Decisional Diffie–Hellman problem (DDH), and the relations among them. A good reference is:

   [Sma]: **pp. 169** (last paragraph, first bullet) – **pp. 171** (until Lemma 11.3, excl.)

2. **ElGamal Encryption and Security Proofs** Recall the ElGamal Encryption Scheme and what a security proof is (aka "reduction proof"):

   [Sma]: **Section 11.4, pp. 178–179**

   Most importantly, read and understand the proof of Lemma 11.8. It is a security proof showing a reduction from the DHP to the security of ElGamal, meaning that if you can break ElGamal, you can solve DHP (which is assumed to be a hard problem).

3. **Security Definitions** Read and understand the concept of Security Definitions:

   [Sma]: **Sections 18.1, pp. 289–292** (until 1.3 "Other Security Concepts", excl.)

   Understand the three security notions: perfect, semantic, and polynomial security (aka "indistinguishable encryptions") and the three attack notions on encryption schemes: CPA, CCA1, and CCA2.

4. **CPA-Security of ElGamal** Understand why the ElGamal encryption scheme is CPA-secure under DDH:

   [Sma]: **Sections 18.2.2, pp. 294–296**

   In particular, understand the proof of Lemma 18.8.

References

[Sma] Nigel Smart. *Cryptography: An Introduction*. Third Edition, 2013. Available at https://www.cs.bris.ac.uk/~nigel/Crypto_Book/.