Security and Cryptography IN4191

Checklist "Do I meet the prerequisites?"

This course is an introductory course for security and cryptography. Despite that, it requires 5ECTS (140 hours) of intensive work. Students are expected to have a strong mathematical background, particularly in integer arithmetic and good understanding in probability. It is also essential to know at least one of the programming languages like C, C++, C#, Java, Python since in one of the assignments, it might be the case that an implementation of a cryptographic algorithm or a protocol would be necessary.

For this course, you are expected to have a working knowledge of the following concepts

☐	Modular Arithmetic	[Sma, Ch. 1]
☐	Groups and Finite Fields	[Sma, Ch. 1]
☐	Probability (Conditional probability)	[Sma, Ch. 1]
☐	Programming skills (C, C++, C#, Java, Python etc)	Programming courses
☐	Logic gates, flip-flops and registers	Any logic Design courses

For example, can you compute or describe the followings?

- 17 mod 7
- 21 mod 4
- Z_8^* and Z_8

References

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