

Only the german version of the module description as part of the study regulations is legally binding.

Module name	Cryptography and cryptanalysis
Module number	INF-25-Ba-W-Kryp
Responsible lecturer	Dr. Elke Franz elke.franz@tu-dresden.de
Qualification objectives	Students are familiar with the basic types of cryptographic systems and know which security objectives can be implemented with them. They are familiar with historical methods and modern symmetric and asymmetric methods and are able to assess the security of these methods based on known attacks. Students will be able to use these systems to securely implement the various security objectives in line with the current state of the art and will be familiar with various attack techniques and possible countermeasures.
Content	The module covers the basics of cryptography and cryptanalysis, in particular different system types, types of attack and security concepts, historical procedures with their weaknesses, modern renewed symmetric and asymmetric procedures as well as known attacks for security evaluation.
Teaching and learning methods	The module comprises lectures of 2 SWS, exercises of 2 SWS and the self-study. The language of instruction for the lectures and exercises is German.
Prerequisites for participation	The Bachelor's degree program in Computer Science requires the skills acquired in the modules INF-25-Ba-Si Security and INF-25-Ba-Ma3 Algebra.
Applicability	In the Bachelor's degree program in Computer Science, the module is a compulsory elective module of the subject specialization, which must be selected in accordance with the annex to the examination regulations. The module creates the prerequisites for the modules listed under prerequisites for participation.
Requirements for earning credit points	The credit points are earned if the module examination is passed. The module examination consists of a non-public oral examination as an individual examination lasting 25 minutes. The examination language is German.
Credit points and grades	6 credit points can be earned through the module. The module grade corresponds to the grade of the examination.
Module frequency	The module is offered every summer semester.
Workload	The total workload is 180 hours.
Module duration	The module comprises one semester.