انجمن رمز ایران
Iranian Society of Cryptology

اصول طراحی امضاهای دیجیتال

امضاهای دیجیتال و گونه‌های مختلف آنها با کاربری‌های خاص،اجزای اصلی تعاملات و تجارت الکترونیکی هستند. در این کارگاه،اصول طراحی گونه‌هایی از امضای دیجیتال نظیر امضای معمولی، امضای کور، امضای ارزیاب معین و امضا با بازیابی پیام و سپس اصول طراحی گونه شناسه‌مبنای آنها را آموزش می‌دهیم. لازم به ذکر است که اکثر استانداردها و توصیه‌نامه‌ها برای امضاهای مورد نظر بر اساس این اصول و روشها تدوین شده‌اند.

Design principals of digital signatures

Digital signatures and their different types with special applications are the main components of electronic interactions and business. In this workshop, we teach design principals of some kinds of digital signatures such as ordinary signatures, blind signatures, designated verifier signatures, signatures with message recovery and their identity-based variants. It should be highlighted that most existing standard documents and recommendations for these signatures are based on these principals and methods.