Cryptographic systems

A system is a collection of entities that work together to get something done. For the rest of the semester we will look at a few systems that combine things we have learned about separately into something new.

Time permitting, we'll look at some of the following: tweakable block cipher (universal hashing and a block cipher), certificates (public and private keys), key-negotiation (Diffie-Hellman and certificates), random generation (hash function and block cipher).

Learning objectives

By the end of this module you should be able to...

- Name several instances in which multiple cryptographic primitives are assembled into a system; and
- Program or simulate some simple systems.