Modern Cryptography: From Turing to Present Day

Steven Myers
School of Informatics and Computing
Indiana University Bloomington

We will review the development of modern cryptography, which started just prior to World War II, and its (public) development to modern day. While Turing is famous at least in part for his role as the head cryptographer in Britain's Bletchley Park during World War II, and wrote papers on cryptanalysis (some of which have only been declassified in the last few months), it is his larger ideas related to Turing Machines and Computability, which led to Complexity Theory, and which, along with Shannon's information theory, jointly provided the foundations necessary for modern cryptography. We will look at how key ideas from these fields allowed for formal definitions of security, and brought provable security in to the field, thus making it more of a science than art. This formalization has given rise to a number of modern cryptographic primitives that were mostly inconceivable at the time of Turing, including public-key encryption, digital signatures, zero-knowledge proofs, secure multi-party computation, and fully homomorphic encryption. We will introduce and discuss the development of these primitives.