CPSC 467b: Cryptography and Computer Security

Lecture 12

Michael J. Fischer

Department of Computer Science
Yale University

February 17, 2010

More number theory with cryptographic applications

We turn next to other number-theoretic techniques with important cryptographic applications.

We begin by looking in greater detail at the structure of $\mathbf{Z}_n^*$, the set of integers in $\mathbf{Z}_n$ that are relatively prime to n.