

CPSC 467b: Cryptography and Computer Security

Michael J. Fischer

Lecture 2

January 11, 2012

Security of Symmetric Cryptography

Complexity

Confidentiality

Attacks

Randomness

Probability Theory

Perfect Secrecy

Security of Symmetric Cryptography