ASSUMPTIONS

RSA Assumption

Factoring Assumption

DCRA Assumption

DDH Assumption

Discrete Log Assumption

Collision-resistant Hashing

SHA-1

One-way Functions

P ≠ NP

Block Ciphers

PRIMITIVES

Trapdoor Permutations

Oblivious Transfer

Public-key Encryption

Digital Signatures

Constraint Solving

MACs

Pseudorandom Functions

Private-key Encryption

PROTOCOLS

Secure 2-party / Multi-party Computation

Privacy-preserving Data mining

Secure Auctions

E-voting

E-cash

SSL

Constructions in CS 120

Fall 2006

implies

proven in class

implies known but not proven in class

implies immediate implication