

The Weak Factoring Experiment. (302)
Theorem 8.32.
Theorem 8.33.
Algorithm 8.31/8.34.
Proposition 8.36.
Lemma 8.37.
The Factoring Experiment. (311)
Definition 8.45.
The RSA Experiment.
Definition 8.46.
The RSA Assumption.
GenRSA.
Theorem 8.50.
Definition 8.51.
Proposition 8.52.
Proposition 8.53.
Definition Cyclic Group.
Definition Generator.
Proposition 8.54.
Corollary 8.55.
Theorem 8.56.
The Discrete-logarithm Experiment. (And definitions.)
Definition 8.62.
Definition 8.63.
Theorem 8.64.
Group Generation Algorithm.
Construction 8.78. (335)
Theorem 8.79.
Theorem 8.80.
The Key-Exchange Experiment. (365)
Definition 10.1.
Construction 10.2. (Diffie-Hellman)
Theorem 10.3. Real Life weaknesses.
Definition: Public Key Crypto.
Definition: Signatures.
Definition: Non-repudiation.
Definition 11.1: Public Key Encryption Scheme.
The Eavesdropping Indistinguishability Experiment.
Definition 11.2.
Proposition 11.3.
Theorem 11.4.
The LR-oracle Experiment.
Definition 11.5.

Theorem 11.6.
Claim 11.7.
The CCA Indistinguishability Experiment.
Definition 11.8.
Definition 11.9: Key Encapsulation Mechanism.
Construction 11.10.
The CPA Indistinguishability Experiment.
Definition 11.11.
Theorem 11.12.
The CCA Indistinguishability Experiment.
Definition 11.13.
Theorem 11.14.
Lemma 11.15.
Construction 11.16: El Gamal.
Theorem 11.18.
Construction 11.19: El Gamal-like KEM.
Theorem 11.20.
Theorem 11.21.
Theorem 11.22.
Construction 11.23.
Corollary 11.24.
Algorithm 11.25.
Construction 11.26: Textbook RSA.
Algorithm 11.28: An attack on plain RSA.
Theorem 11.29.
Construction 11.30: Padded RSA.
The RSA hard-core predicate experiment.
Theorem 11.31.
Construction 11.32.
Theorem 11.33.
Construction 11.34.
Theorem 11.35.
Construction 11.36.
Construction 11.37.
Theorem 11.38.
Claim 11.39.
Definition 12.1. (442)
Definition 12.2.
Construction 12.3.
Theorem 12.4.
Construction 12.5: Plain RSA signatures.
Construction 12.6.
Theorem 12.7.