**Glossary of Crypto Definition Acronyms**

**PRG**: Pseudorandom Generator $G : X \to Y$

**PRF**: Pseudorandom Function $F : K \times X \to Y$

**PRP**: Pseudorandom Permutation $F : K \times X \to X$

**Ciphers**

(Enc, Dec), $\mathsf{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, $\mathsf{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ (sometimes also includes nonces)

Security definitions for ciphers:

Semantic Security
CPA Security: Chosen Plaintext Attack
Ciphertext Integrity
AE: Authenticated Encryption (CPA Security + Ciphertext Integrity)
CCA Security: Chosen Ciphertext Attack

**MACs**: Message Authentication Codes (security notion is Existential Unforgeability)

(Sign, Verify), $\mathsf{Sign} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$, $\mathsf{Verify} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \to \{0,1\}$

**CRHF**: Collision Resistant Hash Function

**DDH**: Decisional Diffie-Hellman ($\{g, g^x, g^y, g^{xy}\} \approx_c \{g, g^x, g^y, g^z\}$)

**CDH**: Computational Diffie-Hellman (Given $g, g^x, g^y$, compute $g^{xy}$)

**TDP**: Trapdoor Permutation

**OWF**: One-way Function

**ROM**: Random Oracle Model

**LWE**: Learning with Errors

**IP**: Interactive Proofs

**ZK**: Zero Knowledge

**HVZK**: Honest Verifier Zero Knowledge

**ZKPoK**: Zero Knowledge Proof of Knowledge

**NIZK**: Non-Interactive Zero Knowledge

**2PC**: Two Party Computation

**MPC**: Multiparty Computation