University of Maryland
CMSC858K — Cryptography
Professor Jonathan Katz

Problem Set 3

Due at *beginning* of class on Mar. 18

1. **Basing identification on private-key encryption.** Let $(\mathcal{E}, \mathcal{D})$ be a private-key encryption scheme for k-bit messages, and consider the following identification protocols in the shared-key setting (the prover $\mathcal{P}$ and verifier $\mathcal{V}$ begin by sharing a random key $s \in \{0,1\}^k$):

   Protocol 1. $\mathcal{V}$ chooses $r \in \{0,1\}^k$ at random and sends r to $\mathcal{P}$. The prover computes $C \leftarrow \mathcal{E}_s(r)$ and sends C. The verifier accepts iff $\mathcal{D}_s(C) \stackrel{?}{=} r$.

   Protocol 2. $\mathcal{V}$ chooses $r \in \{0,1\}^k$ at random, computes $C \leftarrow \mathcal{E}_s(r)$, and sends C to the prover. $\mathcal{P}$ computes $r' = \mathcal{D}_s(C)$ and sends r'. The verifier accepts iff $r \stackrel{?}{=} r'$.

   For each of the following statements, give either a proof of security or a counterexample showing that the statement is, in general, not true. (If you give a counterexample, you need not be completely formal if your counterexample is "obviously" true.)

   - If $(\mathcal{E}, \mathcal{D})$ is secure against ciphertext-only attacks, then Protocol 1 is necessarily secure against weak attacks.
   - If $(\mathcal{E}, \mathcal{D})$ is secure against chosen-plaintext attacks, then Protocol 1 is necessarily secure against passive attacks.
   - If $(\mathcal{E}, \mathcal{D})$ is secure against chosen-plaintext attacks, then Protocol 2 is necessarily secure against passive attacks.
   - If $(\mathcal{E}, \mathcal{D})$ is secure against chosen-plaintext attacks, then Protocol 2 is necessarily secure against active attacks.