A Definition of Security for Symmetric Encryption

This handout gives a sketch of a widely accepted formal definition of security of a symmetric encryption scheme against a chosen plaintext attack. The definition is formulated in terms of a “game” played between an adversary and his environment. The game runs as follows:

1. A random key $K$ for the encryption is chosen (but not shown to the adversary).

2. A random bit $b \in \{0, 1\}$ is chosen (but not shown to the adversary).

3. The adversary poses a series of questions to an encryption oracle. Each question is of the form $(m_0, m_1)$, where $m_0$ and $m_1$ are messages (i.e., plaintexts) of the same length (we assume messages are byte strings). Given $(m_0, m_1)$, the encryption oracle encrypts message $m_b$ using the encryption algorithm and the key $K$, and gives the resulting ciphertext to the adversary.

   Note that the adversary may choose his queries to the encryption oracle however he wants (subject to the constraint that both messages in the query are the same length). In particular, his queries to the oracle may depend on previous outputs from the oracle.

4. At the end of the game, the adversary outputs a bit $\hat{b} \in \{0, 1\}$.

   We define an adversary’s advantage to be $|p - 1/2|$, where $p$ is the probability that $\hat{b} = b$ in the above game.

   We say that a given encryption scheme is secure against chosen ciphertext attack if no efficient adversary has a non-negligible advantage. Equivalently, a scheme is insecure according to this definition if there exists an efficient adversary that has a non-negligible advantage.