1. The ACME Crypto Company sells cheap licenses for a block cipher. The ACME block cipher has the following structure. The cipher has a block size of 128 bits and a key size of 128 bits. A given key $K$ is expanded into 32 128-bit subkeys $K_1, \ldots, K_{32}$ (the details of the key expansion are not so important here). The cipher proceeds in rounds. There are 32 rounds. For $i = 1, \ldots, 32$, the input to round $i$ is a 128-bit string $X_{i-1}$, and the output is a 128-bit string $X_i$. In round $i$, $X_i$ is computed as

\[ X_i = P(X_{i-1} \oplus K_i), \]

where $P$ is a function that maps a 128-bit string $y_1y_2\cdots y_{128}$ to the 128-bit string $y_{\pi(1)}y_{\pi(2)}\cdots y_{\pi(128)}$, for some permutation $\pi$ on $\{1, \ldots, 128\}$. The exact permutation $\pi$ is not important — but it is fixed and publicly known and the same for every round.

The plaintext is $X_0$ and the ciphertext is $X_{32}$.

Comment on the security of the ACME cipher.

2. Give a convincing and detailed argument that ECB mode is insecure according to the definition of security in Handout 1.

3. Consider the following variation of CBC mode (this is actually a real-world example). For a given key $K$, a random initial vector is used to encrypt the first message. However, the initial vector used to encrypt the second message is the final block of the first ciphertext. In general, the initial vector used to encrypt the $(i+1)$st message is the final block of the $i$th ciphertext.

Give a convincing and detailed argument that this variant of CBC mode is insecure according to the definition of security in Handout 1.