ECS 227 — Modern Cryptography — Winter 00
Problem Set 3

Phillip Rogaway

Out: 1 February 2000. Due: 15 February 2000.

1. **An attack.** Consider the following "output feedback mode" (OFB) of encryption. Let $E : \text{Keys} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $Z(K)$ be the infinite string $Z_1 Z_2 Z_3 \cdots$ defined by $Z_0 = 0^n$ and, for $i \geq 1$, $Z_i = E_K(Z_{i-1})$. OFB mode is stateful, having a counter *ctr*, which is initialized to 1. The encryption of a message M is $(ctr, M \oplus Z[ctr..ctr + |M| - 1]$. After encrypting a message M, increment *ctr* by $|M|$.

   Find an attack on OFB, in the sense of violating the real-or-random definition of security. Your attack should do a good job if you get a single ciphertext, C, of length about $n2^{n/2}$ bits. Analyze your attack, identifying any "heuristic" aspect of the analysis.

2. **An alternative formulation of real-or-random security suggested by Rivest.** Consider the following alternative version of rr-security. Let $\Pi = (\mathcal{K}, \mathcal{E}, D)$ be an encryption scheme. Let A be an adversary. Then

   $$\mathrm{Adv}_A^{\mathrm{rr2}} \;=\; \Pr[K \leftarrow \mathcal{K}\;;\; A^{\mathcal{E}_K(\cdot),\, \mathcal{E}_K(\cdot)} = 1] - \Pr[K \leftarrow \mathcal{K}\;;\; A^{\mathcal{E}_K(\cdot),\, \mathcal{E}_K(\$^{|\cdot|})} = 1]\,.$$

   Part A. Explain the intuition of this definition, and why it might be stronger (=stricter, more restrictive) than our rr-definition.

   Part B. Nonetheless, state and prove a theorem which shows that if an encryption scheme is secure in the rr-sense, then it is secure in the rr2-sense as well.

3. **Whichkey-concealing encryption.** Call an encryption scheme "whichkey-revealing" if an adversary can tell if two ciphertexts were encrypted under the same key. (For example, maybe an adversary who sees $C_1 \xleftarrow{R} \mathcal{E}_a(M_1)$ and $C_2 \xleftarrow{R} \mathcal{E}_a(M_2)$ and $C_3 \xleftarrow{R} \mathcal{E}_b(M_3)$, for random keys a and b, can tell that C_1 and C_2 were encrypted under the same key, and C_3 was encrypted under a different key.) Call an encryption scheme whichkey-concealing if an adversary can't make such a determination .

   Part A. Show that our rr-definition of an encryption scheme does not guarantee that the scheme is whichkey-concealing. To do this, start from a secure encryption scheme (in the rr-sense) and construct an equally-secure one (in the rr-sense) which is whichkey-revealing.

   Part B. Modify the rr-definition of security so that it implies that the scheme is whichkey-concealing.

   Part C. State and prove a theorem showing that counter-mode encryption with a PRF meets your definition from Part B.