ECS 227 — Modern Cryptography — Winter 2009

Phillip Rogaway

Out: Wednesday, 25 February 2009.
Due: Monday, 9 March 2009.

7. *(A wrong way to extend the CBC MAC.)* Consider the following variant of the CBC MAC, intended to allow one to MAC messages of arbitrary length. The construction uses a blockcipher $E\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, which you should assume to be secure in the sense of a PRP. The domain for the MAC is $(\{0,1\}^n)^+$. To MAC a message M under key $K1 \parallel K2$, $|K1| = |K2| = n$, first compute the "ordinary" CBC MAC of M, keyed by $K1$, and then xor into the result the key $K2$. Show that this MAC is completely insecure: break it (getting advantage of about 1) by a simple adversary that asks a constant number of queries.

8. *(Nonce-based encryption)* A *nonce-based symmetric encryption scheme* is a three-tuple of algorithms $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ that is like the encryption schemes we have defined before except that $\mathcal{E}$ is now deterministic and stateless (as is $\mathcal{D}$), and $\mathcal{E}$ and $\mathcal{D}$ now take in an additional argument $N \in \mathcal{N} \subseteq \{0,1\}^*$, the *nonce*. When encrypting, a party is required to select a new nonce N to go with each message that is encrypted. As long as he does this, privacy should be assured. The nonce could be a counter, for example, or a long enough random string.

(a) Carefully formalize a notion of real-or-random security for a nonce-based symmetric encryption scheme.

(b) Describe a blockcipher-based scheme Π that achieves your notion of security from (a), assuming that the blockcipher $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ from which Π is defined is secure as a PRP.

(c) Do you see any advantages of the nonce-based notion? Any disadvantages? Briefly discuss.