Problem Set 6 – Due Monday, May 23, 2011

Problem 21. Fix a blockcipher $E : K \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ and let CBC$_K(M)$ be the CBC MAC, using $E_K$, of a message $M$ that is a positive multiple of $n$ bits. We have seen that this construction is not secure as a (variable-input-length) MAC: even if $E$ is an ideal cipher there is an efficient algorithm to forge under CBC. (Recall what this forging algorithm is?) So consider instead the proposal $\text{CBC2}_K(M) = \text{CBC}_K(M) \oplus K'$ where $K' \in \{0, 1\}^n$. Show that this is a bad MAC, too: you can easily forge against CBC2.

Problem 22. Formalize and prove the following statement:

If $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ is a collision-resistant hash function and $E : K \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ is a PRF-secure blockcipher then $F_K(X) = E_K(H(X))$ is a good PRF.

Problem 23. Consider the following “Propagating Cipher Block Chaining” (PCBC) mode: a plaintext $P = P_1 \cdots P_m$, where $|P_i| = n$, is encrypted as PCBC$_K(P_1 \cdots P_m) = C_0 C_1 \cdots C_m$ where $\text{IV} = P_0 \oplus C_0$ is a random $n$-bit string and $C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1})$.

Part A. In what ways is PCBC less efficient than CBC?

Part B. Show that if two ciphertext blocks are exchanged, this does not effect the decryption of subsequent plaintext blocks.

Part C. Consider the authenticated-encryption mode where one takes a plaintext $P$, assumed to be a multiple of $n$ bits, appends a block $\oplus P_i$, then PCBC-encrypts the resulting string $P'$. (Decryption does the natural thing, returning $\perp$ if a recovered plaintext has the wrong final block.) Argue that this AE mode does not work: it doesn’t achieve the authenticity requirement.

Problem 24. Say that a symmetric encryption scheme is chosen-ciphertext-attack (CCA) secure if the indistinguishability condition holds even in the presence of a decryption oracle: $\text{Adv}_{\text{CCA}}^E(A) = \Pr[A^{E_K(\cdot), D_K(\cdot)} \Rightarrow 1] - \Pr[A^{E_K(\emptyset^1), D_K(\cdot)} \Rightarrow 1]$ is small for any efficient $A$.

Part A. What restriction on the queries of $A$ must we make for the above definition to be achievable?

Part B. Show that CBC$ is not CCA-secure. (Nor are CTR, CFB, OFB, PCBC, etc.)

Part C. Argue that any authenticated-encryption scheme (an AE-method secure in the sense described in class) is CCA-secure.