Problem Set 5 – Due Monday, May 16, 2011

Problem 17. Problem 5.7 of your text. Assume a random IV and describe any attacks in terms of breaking the ind or ind$ security of the proposed scheme.

Problem 18. Problem 5.11 of your text.

Problem 19. Fix a blockcipher $E$ with an 8-byte (64-bit) blocksize. Given a byte string $M$, let $\text{pad}(M)$ be $M$ followed by enough bytes to take you to the next multiple eight bytes: append either the byte 01, or two bytes of 02 (that is, 02 02) or three bytes of 03 (that is, 03 03 03), and so on, up to appending eight bytes of 08 (all of these constants written in hexadecimal). Let $\text{CBC}^*$ be the variant of CBC$ encryption that encrypts $M$ by applying CBC, over $E$, with a random IV, to $\text{pad}(M)$. The method is specified in Internet Standard RFC 2040. Note that a $\text{CBC}^*$ ciphertext for $M$ will have the form $C = \text{IV} \parallel C'$ where $|\text{IV}| = 64$ and $|C'|$ is the least multiple of 64 exceeding $|M|$.

Part A. Do you believe that $\text{CBC}^*$ achieves good ind$-security when $E$ is a good PRP? Why or why not?

Part B. Write a careful fragment of pseudocode for an algorithm $\text{Decrypt}$ to decrypt a byte string $C$ under $\text{CBC}^*$. Let $\text{Decrypt}_K(C)$ return the distinguished symbol $\perp$ if it is provided an invalid ciphertext; otherwise, it returns a byte string $M$.

Part C. Suppose an adversary is given an oracle, $\text{Valid}$, that, given a ciphertext $C$, returns a single bit: the bit “1” if $C$ is valid—meaning $\text{Decrypt}_K(C) \in \{0, 1\}^*$—and the bit “0” if it is not—meaning $\text{Decrypt}_K(C) = \perp$. Show how to use the oracle to decrypt a block $Y = E_K(X)$ for an arbitrary 8-byte $X$. Hint: all your queries to the $\text{Valid}$ oracle will be 16 bytes. I don’t mind if you make several hundred of them.

Part D. Show how to decrypt any ciphertext $C = \text{CBC}^*_K(M)$ given a $\text{Valid}$ oracle.

Part E. What advice would you give to security practitioners who were considering the use of $\text{CBC}^*$ in their networking protocol?

Problem 20. Consider using the “CBC MAC” as a cryptographic hash function: the blockcipher is $E_K$ for some fixed (and public) key $K$, and one hashes a message $M$ by appending $10^*$ padding, then CBC encrypting with a zero IV, and then using the final $n$-bit block as the hash of $M$. Is this method collision resistant?

NB: So sorry—there are no animal pictures on this problem set.