ECS 227 — Modern Cryptography — Winter 00
Problem Set 4

Phillip Rogaway
Out: 17 February 2000. Due: 2 March 2000.

1. Let $p = 2^{32} - 5$. This is a prime number. Consider the ϵ-AU hash-function family H whose domain is $(\{0,1\}^{32})^{n+1}$, for some fixed, small n, where a key k is a random number $k \in [0..p-1]$, and where we hash the sequence of words $M = m_n m_{n-1} m_1 m_0$ under k to $(m_n k^n + m_{n-1} k^{n-1} + \cdots m_1 k + m_0) \bmod p$.

(A) Describe how to compute H on a 32-bit computer. Assume you can cheaply multiply two 32-bit numbers to generate a 64-bit result.

(B) Can you think of a modification to the key set of H that will make the computation of H even faster?

(C) The hash function H is not ϵ-AU (for a desirable value of ϵ). Explain.

(D) Modify the hash function H to make a hash function H' that is ϵ-AU, for a small value of ϵ. Prove your bound on the collision probability of H'. Try to retain as much efficiency as possible. In particular, computation of $H_k(M)$ should be only a few percent slower than computation of H. To achieve this, avoid expensive "bit twiddling." It is OK if your value of ϵ goes up some. You may assume that the inputs M that you will hash are random.

2. Consider the following two variants of the CBC MAC, intended to allow one to MAC messages of arbitrary length. Both MACs use a block cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, which you should assume to be secure. The domain for the MAC is $(\{0,1\}^n)^+$.

(A) To MAC M under key K compute $\mathrm{CBC}_K(M \parallel |M|)$, where $|M|$ is the length of M, written in n bits. Of course K has k bits. Show that this MAC is insecure.

(B) To MAC M under key $K \parallel K'$, compute $\mathrm{CBC}_K(M) \oplus K'$. Of course K has k bits and K' has n bits. Show that this MAC is insecure.

3. Let $\mathrm{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme and let $\mathrm{MA} = (\mathcal{K}', \mathrm{MACG}, \mathrm{MACV})$ be a message authentication code. Alice (A) and Bob (B) share a secret key $K = (K1, K2)$ where $K1 \leftarrow \mathcal{K}$ and $K2 \leftarrow \mathcal{K}'$. Alice wants to send messages to Bob in a private and authenticated way. Consider her sending each of the following as a means to this end. For each, say whether it is a secure way or not, and briefly justify your answer. (In the cases where the method is good, you don't have to give a proof, just the intuition.)

(a) $M, \mathrm{MACG}_{K2}(\mathcal{E}_{K1}(M))$

(b) $\mathcal{E}_{K1}(M, \mathrm{MACG}_{K2}(M))$

(c) $\mathrm{MACG}_{K2}(\mathcal{E}_{K1}(M))$

(d) $\mathcal{E}_{K1}(M), \mathrm{MACG}_{K2}(M)$

(e) $\mathcal{E}_{K1}(M), \mathcal{E}_{K1}(\mathrm{MACG}_{K2}(M))$

(f) $C, \mathrm{MACG}_{K2}(C)$ where $C = \mathcal{E}_{K1}(M)$

(g) $\mathcal{E}_{K1}(M, A)$ where A encodes the identity of Alice; B decrypts the received ciphertext C and checks that the second half of the plaintext is "A".

In analyzing these schemes, you should assume that the primitives have the properties guaranteed by their definitions, but no more; for an option to be good it must work for *any* choice of a secure encryption scheme and a secure message authentication scheme.

Now, out of all the ways you deemed secure, suppose you had to choose one to implement for a network security application. Taking performance issues into account, do all the schemes look pretty much the same, or is there one you would prefer?