Problem Set 5—Due Wednesday, October 29

Problem 20 *In this problem you need the following fact about numbers: "the numbers modulo a prime form a field." Thus when* p *is a prime, all the numbers* $1, 2, \ldots, p-1$ *have an inverse modulo* p*. For example, among the numbers modulo* 5*, the inverse of* 1 *is* 1 *(since* $1 \cdot 1 = 1 \bmod 5$*), the inverse of* 2 *is* 3 *(since* $2 \cdot 3 = 1 \bmod 5$*), the inverse of* 3 *is* 2 *(since* $3 \cdot 2 = 1 \bmod 5$*), and the inverse of* 4 *is* 4 *(since* $4 \cdot 4 = 1 \bmod 5$*).*

Reminder: $\mathcal{H} = \{h : U \to [0..M-1]\}$ *is* ***universal-2*** *if for all distinct* $x, x' \in U$, $\Pr_h[h(x) = h(x')] = 1/M$. $\mathcal{H} = \{h : U \to [0..M-1]\}$ *is* ϵ-***universal-2*** *if for all distinct* $x, x' \in U$, $\Pr_h[h(x) = h(x')] \leq \epsilon$.

Let W denote the space of 28-bit strings, interpreted as numbers between 0 and $2^{28} - 1$.

(A) For each $a \in [0..130]$, let $h_a : W \to [0..130]$ be defined by $h_a(x) = a + x \bmod 131$. Is $\mathcal{H} = \{h_a\}$ universal-2? Prove or disprove.

(B) For each $a \in [0..130]$, let $h_a : W \to [0..130]$ be defined by $h_a(x) = ax \bmod 131$. Is $\mathcal{H} = \{h_a\}$ universal-2? Prove or disprove.

(C) For each $a = a_1a_2a_3a_4$, where $a_1, a_2, a_3, a_4 \in [0..130]$, and for each $x = x_1x_2x_3x_4 \in W$, where each $0 \leq x_1, x_2, x_3, x_4 \leq 127$ is a byte, let $h_a(x) = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \bmod 131$. Is $\mathcal{H} = \{h_a\}$ universal-2? Prove or disprove.

(D) Describe an ϵ-universal-2 family of hash functions $\mathcal{H} = \{h : W \to [0..127]\}$, for some $\epsilon \approx 1/128$. Calculate ϵ. *Hint: First use the hash family of (C), but then do something reasonable when the hash value comes out* 128, 129, *or* 130.

Problem 21 Alice and Bob share a random function $f : W \to W$, where W is the space of 32-bit strings. To authenticate a message $x = x_1$, where $x_1 \in W$, Alice sends Bob $(x, f(x))$. To authenticate a message $x = x_1x_2$, where $x_1, x_2 \in W$, Alice sends Bob $(x, f(f(x_1) \oplus x_2))$. To authenticate a message $x = x_1x_2x_3$, where $x_1, x_2, x_3 \in W$, Alice sends Bob $(x, f(f(f(x_1) \oplus x_2) \oplus x_3)$. And so forth. Show how to break this MAC. *Hint. If you ask the right two questions, you can forge a third message.*