MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #8

Problems for all

Problem 1. Let $k \geq 2$, let $A = (\mathbb{Z}/2\mathbb{Z})^k$, and define the maps

$$\begin{aligned} s, g &: A \times A \to A \times A \\ s(x, y) &= (y, x) \\ g(x, y) &= \begin{cases} (x, y), & y \neq (0, 0, \dots, 0); \\ (x + \underbrace{(1, 1, ..., 1)}_{k}, (0, 0, \dots, 0)), & y = (0, 0, \dots, 0). \end{cases} \end{aligned}$$

(a) Prove that s^2 and g^2 are the identity on $A \times A$.
(b) Prove that $(sg)^4 = sgsgsgsg$ moves only 3 elements of $A \times A$, i.e.

$$\#\{(x, y) \in A \times A : (sg)^4(x, y) \neq (x, y)\} = 3.$$

(c) Prove that $(sg)^{12}$ is the identity.

Problem 2. Encrypt the message 001100001010 using SDES and key 111000101. *[Hint: After one round, the output is* 001010010011*.]*

Problem 3. Suppose the key for round 0 in AES consists of 128 bits, each of which is 0. Show that the key for the first round is

$$\begin{pmatrix} 01100010 & 01100010 & 01100010 & 01100010 \\ 01100011 & 01100011 & 01100011 & 01100011 \\ 01100011 & 01100011 & 01100011 & 01100011 \\ 01100011 & 01100011 & 01100011 & 01100011 \end{pmatrix}.$$

Problem 4. In the Rijndael field $F = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)$, where bytes are associated to polynomials modulo $X^8 + X^4 + X^3 + X + 1$, compute the product $01010010 \cdot 10010010 \in F$.

Problem 5.

(a) Find all monic irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$.
(b) Verify that the Rijndael polynomial

$$f(X) = X^8 + X^4 + X^3 + X + 1$$

is irreducible in $\mathbb{F}_2[X]$. *[Hint: If it has a factor, it must have degree at most* 4*.]*

Problem 6. Put $f(X) = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$, and let

$$a = 00001100 = X^3 + X^2 \in F = \mathbb{F}_2[X]/(f).$$

(a) Compute a^5.
(b) Find the inverse $f^{-1} \in F$ of $f = X^2 = 00000100$.
(c) Multiply $f^{-1}a$ and verify that $f^{-1}a = X + 1$ in F.

Date: Due Friday, October 22, 2010.

Additional problems for 395A

Problem 7. For a bit string x, let $\overline{x}$ denote the complementary string obtained by interchanging 0s to 1s, e.g., $\overline{101100} = 010011$; equivalently, $\overline{x} = x + 1111\ldots$. Show that if (S)DES encrypts $E_K(x) = y$, then $E_{\overline{K}}(\overline{x}) = \overline{y}$.

Problem 8. Let p be prime and define

$$a_n(p) = \#\{f \in \mathbb{F}_p[X] : \deg f = n,\ f \text{ monic irreducible}\}.$$

(a) Show that $a_2(p) = (p^2 - p)/2$ and $a_3(p) = (p^3 - p)/3$.

(b) Use the equality

$$\sum_{d|n} d a_d(p) = p^n \tag{$*$}$$

(which you may assume) to compute $a_2(n)$ for $n = 1, \ldots, 10$.

(c) Use $(*)$ to prove that

$$\frac{p^n - 2p^{n/2}}{n} < a_n(p) \leq \frac{p^n}{n}.$$

Conclude that the probability that a random monic polynomial of degree n over $\mathbb{F}_p$ is irreducible is roughly $1/n$.

Computational challenge

Problem C. Write a computer program that performs one round of AES with a key size of 128 bits.