MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #7

Problems for all

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

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

(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.
(a) From a cryptanalytic point of view, how important is the initial permutation in DES?
(b) Describe *Triple DES* as an encryption function mathematically: what are the plaintext space $\mathcal{P}$, the ciphertext space $\mathcal{C}$, and the key space $\mathcal{K}$? *[Hint: Read* §4.6.*]*

Problem 4. 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

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

Additional problems for 395A

Problem 5. 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 DES encrypts $E_K(x) = y$, then $E_{\overline{K}}(\overline{x}) = \overline{y}$.

Date: Due Wednesday, 22 October 2008.