MATH 75: Cryptography	Spring 2022

PSET 5 — May 6, 2022

Prof. Asher Auel | ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***Cryptography*** by **Simon Rubinsen-Salzedo**

Problems

1. Let $k \geq 2$ and $A = (\mathbb{Z}/2\mathbb{Z})^k$. Let $\vec{0}, \vec{1} \in A$ be the vectors of all zeros and all ones, respectively. Define the map $g : A \to A$ by

$$g(y) = \begin{cases} \vec{0} & y \neq \vec{0} \\ \vec{1} & y = \vec{0} \end{cases}$$

Then define

$$s, G : A \times A \to A \times A$$
$$s(x, y) = (y, x)$$
$$G(x, y) = (x + g(y), y)$$

(a) Prove that s^2 and G^2 are the identity on $A \times A$. *[We actually proved this in lecture, so just make sure you understand it here.]*

By definition:

(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.

2. Encrypt the message 001100001010 using two rounds of SDES and (9 bit) key 111000101, as explained in lecture. Show all your steps! *[Hint: After one round, the output is* 001010010011.*]*

3. 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 $01010010 \cdot 10010010 \in F$.

4. Here you will prove something that was claimed in lecture!

(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: Any factor must have degree at most* 4*.]*

5. 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 $b^{-1} \in F$ of $b = X^2 = 00000100$.

(c) Compute the product $b^{-1}a$ and verify that $b^{-1}a = X + 1$ in F.