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

$$\begin{aligned} s, G &: A \times A \to A \times A \\ s(x, y) &= (y, x) \\ G(x, y) &= (x + g(y), y) \end{aligned}$$

(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:

$$\begin{aligned} s(x, y) &= (y, x) \\ s^2(x, y) = s(s(x, y)) &= s(y, x) \\ &= (x, y) \end{aligned}$$

Likewise:

$$\begin{aligned} G(x, y) &= (x + g(y), y) \\ G^2(x, y) = G(x + g(y), y) &= (x + 2g(y), y) \\ &\equiv (x + 0, y) \pmod 2 \\ &\equiv (x, y) \end{aligned}$$

(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.

We know that:

$$G(x,y) = (x + g(y), y)$$
$$s(x,y) = (y,x)$$
$$\therefore sG(x,y) = (y, x + g(y))$$

For the case of simplicity, let's substitute 0 and 1 for x, y where necessary and retain x, y where the values of x and y are not $\vec{0}$ or $\vec{1}$.

Then, each vriable can assume any of three general values: $\vec{0}$, $\vec{1}$, or an intermediate value (such as the vector $\langle 1,0,0,1 \rangle$), which will be represented as just x or y.

id	sG	$(sG)^2$	$(sG)^3$	$(sG)^4$	$(sG)^8$	$(sG)^{12}$
(0,0)	(0,1)	(1,0)	(0,0)	(0,1)	(1,0)	(0,0)
(0,y)	(y,0)	(0,ŷ)	(ŷ,0)	(0,y)	(0,y)	(0,y)
(0,1)	(1,0)	(0,0)	(0,1)	(1,0)	(0,0)	(0,1)
(x,0)	(0,x̂)	(x̂,0)	(0,x)	(x,0)	(x,0)	(x,0)
(x,y)	(y,x)	(x,y)	(y,x)	(x,y)	(x,y)	(x,y)
(x,1)	(1,x)	(x,1)	(1,x)	(x,1)	(x,1)	(x,1)
(1,0)	(0,0)	(0,1)	(1,0)	(0,0)	(0,1)	(1,0)
(1,y)	(y,1)	(1,y)	(y,1)	(1,y)	(1,y)	(1,y)
(1,1)	(1,1)	(1,1)	(1,1)	(1,1)	(1,1)	(1,1)

From the table, we can infer that:

(a) $sG(x)$ is the identity for $x \in \{(1,1)\}$.
(b) $sG(x)$ repeats values with a period of 2 for $x \in \{(x,1),(1,y),(x,y)\}$.
(c) $sG(x)$ repeats values with a period of 3 for $x \in \{(0,0),(0,1)(1,0)\}$.
(d) $sG(x)$ repeats values with a period of 4 for $x \in \{(x,0),(0,y)\}$.

Thus, sG^4 will be the identity for all values where the sequence has a period that is a divisor of 4. These are all values **except** $\{(0,0),(0,1),(1,0)\}$, which have a period of 3 and $3 \nmid 4$. Indeed, as we can see from the table, $(sG)^4$ is fixed for all except these.

On the other hand, $(1 \mid 12) \wedge (2 \mid 12) \wedge (3 \mid 12) \wedge (4 \mid 12)$. Therefore, $(sG)^{12}(x,y)$ will be the identity for all (x,y).

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.*]*

First, let's define our permutation function:
permute (123456) = 12434356

And tables:

s_1	1	2	s_2	1	2
000	101	001		100	101
001	010	100		000	011
010	001	110		110	000
011	110	010		101	111
100	011	000		111	110
101	100	111		001	010
110	111	101		011	001
111	000	011		010	100

ROUND 1

$$L_0 = 001100$$
$$R_0 = 001010$$
$$K_0 = 11100010$$
$$\textbf{permute}\ (R_0) = 00010110$$
$$00010110\ \textbf{xor}\ K_0 = 11110100$$
$$S_1(1111) = 011$$
$$S_2(0100) = 111$$
$$011111\ \textbf{xor}\ L_0 = 010011$$

$$L_1 \leftarrow R_0$$
$$R_1 \leftarrow 010011$$

Excryption after 1 round: 001010010011

ROUND 2

$$L_1 = 001010$$
$$R_1 = 010011$$
$$K_1 = 11000101$$
$$\textbf{permute}\ (R_1) = 01000011$$
$$01000011\ \textbf{xor}\ K_1 = 10000110$$
$$S_1(1000) = 001$$
$$S_2(0110) = 011$$
$$001011\ \textbf{xor}\ L_1 = 000001$$

$$L_2 \leftarrow R_1$$
$$R_2 \leftarrow 000001$$

Excryption after 2 rounds: 010011000001

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 $01010010 \cdot 10010010 \in F$.

We can represent polynomials in F as binary numbers, where the state of each bit (whether 0 or 1) represents whether the corresponding power in the polynomial has a factor of 0 or 1.
Then:

$$X^8 + X^4 + X^3 + X + 1 = 100011011$$

Then, we can perform the multiplication modulo 2:

$$\begin{array}{r}
1\,0\,0\,1\,0\,0\,1\,0 \\
\times \quad 1\,0\,1\,0\,0\,1\,0 \\
\hline
1\,0\,0\,1\,0\,0\,1\,0\,\cdot \\
1\,0\,0\,1\,0\,0\,1\,0\,\cdot\,\cdot\,\cdot\,\cdot \\
1\,0\,0\,1\,0\,0\,1\,0\,\cdot\,\cdot\,\cdot\,\cdot\,\cdot\,\cdot \\
\hline
1\,0\,1\,1\,0\,2\,1\,0\,2\,0\,0\,1\,0\,0
\end{array}$$

Shifting back to base 2, we get: 10110010000100
We then need to find this number $\mod 100011011$

$$\mod 10110010000100, 100011011$$

$$\begin{array}{r|r}
100011011 & 10110010000100 \\
100000 & 100011011\,.\,.\,.\,.\,. \\
 & 111111100\,.\,.\,. \\
1000 & 100011011\,.\,.\,. \\
 & 111001111\,.\,. \\
100 & 100011011\,.\,. \\
 & 110101000\,. \\
10 & 100011011\,. \\
 & 101100110 \\
1 & 100011011 \\
\hline
101111 & 1111101
\end{array}$$

Thus, the product in F is 1111101

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

(a) Find all monic irreducible polynomials of degree ≤ 4 in $\mathbb{F}_2[X]$.

There are 2^5 possible polynomials of degree ≤ 4 in $\mathbb{F}$.
We can eliminate half of these polynomials without a constant factor, since they will have 0 as a root.

f	$f(0)$	$f(1)$
1	1	1
$x+1$	1	0
x^2+1	1	0
x^2+x+1	1	1
x^3+1	1	0
x^3+x+1	1	1
x^3+x^2+1	1	0
x^3+x^2+x+1	1	0
x^4+1	1	0
x^4+x+1	1	1
x^4+x^2+1	1	1
x^4+x^2+x+1	1	0
x^4+x^3+1	1	1
x^4+x^3+x+1	1	0
$x^4+x^3+x^2+1$	1	0
$x^4+x^3+x^2+x+1$	1	1

We also need to remove sieve out polynomials that have quadratic factors. Since any factor of a polynomial of degree n must have a degree of *at most* $\frac{n}{2}$, any polynomials with a quadratic factor must have a degree of at least 4.
We also know that both factors must have a degree of 2 The only such irreducible polynomial is x^2+x+1.
We have only identified 4 such polynomials that don't have factors. Of the four:

x^4+x+1 – not divisible by x^2+x+1

$x^4+x^2+1 - = (x^2+x+1)^2 \pmod 2$

x^4+x^3+1 – not divisible by x^2+x+1

$x^4+x^3+x^2+x+1$ – not divisible by x^2+x+1

Since 1 is the identity, the monic irreducible polynomials are
$\{x^2+x+1, x^3+x+1, x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1\}$

(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.]*

Any factor must be a monic polynomial in $\mathbb{F}_2[X]$
Therefore, we can compute the remainders when $f(X) = X^8 + X^4 + X^3 + X + 1$ is divided by the monic polynomials. If any remainder is nonzero, then $f(X)$ is reducible.

Division by $x^4+x^3+x^2+x+1$.

$$\begin{array}{r|r}
11111 & 100011011 \\ \hline
10000 & 11111.... \\
 & 11101... \\
1000 & 11111... \\
 & 10001 \\ \hline
11000 & 10001
\end{array}$$

Division by x^4+x+1.

$$\begin{array}{r|r}
10011 & 100011011 \\ \hline
10000 & 10011.... \\
 & 10101. \\
10 & 10011. \\
 & 1101 \\ \hline
10010 & 1101
\end{array}$$

Division by x^2+x+1.

$$\begin{array}{r|r}
111 & 100011011 \\ \hline
1000000 & 111...... \\
 & 110..... \\
100000 & 111..... \\
 & 111... \\
1000 & 111... \\ \hline
1101000 & 011
\end{array}$$

Division by x^4+x^3+1.

$$\begin{array}{r|r}
11001 & 100011011 \\ \hline
10000 & 11001.... \\
 & 10001... \\
1000 & 11001... \\
 & 10000.. \\
100 & 11001.. \\
 & 10011. \\
10 & 11001. \\
 & 10101 \\
1 & 11001 \\ \hline
11111 & 1100
\end{array}$$

Division by x^3+x+1.

$$\begin{array}{r|r}
1011 & 100011011 \\ \hline
100000 & 1011..... \\
 & 1111... \\
1000 & 1011... \\
 & 1000.. \\
100 & 1011.. \\
 & 1111 \\
1 & 1011 \\ \hline
101101 & 100
\end{array}$$

Since all the remainders are non-zero, none of the irreducible monic polynomials of degree ≤ 4 divide $f(X)$. It therefore must be irreducible in $\mathbb{F}_2[X]$.

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.

Let's begin by computing a^2:

$$\begin{array}{r}
1\ 1\ 0\ 0 \\
\times\ 1\ 1\ 0\ 0 \\
\hline
1\ 1\ 0\ 0\ \cdot\ \cdot \\
1\ 1\ 0\ 0\ \cdot\ \cdot\ \cdot \\
\hline
1\ 2\ 1\ 0\ 0\ 0\ 0
\end{array} \equiv 1010000$$

We can then compute $a^4 = (a^2)^2$:

$$\begin{array}{r}
1\ 0\ 1\ 0\ 0\ 0\ 0 \\
\times\ 1\ 0\ 1\ 0\ 0\ 0\ 0 \\
\hline
1\ 0\ 1\ 0\ 0\ 0\ 0\ \cdot\ \cdot\ \cdot\ \cdot \\
1\ 0\ 1\ 0\ 0\ 0\ 0\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
\hline
1\ 0\ 2\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0
\end{array} \equiv 1000100000000$$

And, finally, $a^5 = a \cdot a^4$

$$\begin{array}{r}
1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\
\times\ \qquad\qquad 1\ 1\ 0\ 0 \\
\hline
1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \cdot\ \cdot \\
1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \cdot\ \cdot\ \cdot \\
\hline
1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0
\end{array}$$

We then need to find the equivalent of 1100110000000000 in the Rijndael field F by finding its modulus with $X^8 + X^4 + X^3 + X + 1$.

Division by $x^8 + x^4 + x^3 + x + 1 \equiv 100011011$.

$$\begin{array}{r|r}
100011011 & 1100110000000000 \\
\hline
1000000 & 100011011....... \\
 & 100000110...... \\
100000 & 100011011...... \\
 & 111010000.. \\
100 & 100011011.. \\
 & 110010110. \\
10 & 100011011. \\
 & 100011010 \\
1 & 100011011 \\
\hline
1100111 & 1
\end{array}$$

Thus, $a^5 \equiv 1 \in F$.

(b) Find the inverse $b^{-1} \in F$ of $b = X^2 = 00000100$.

Using the extended Euclidean Algorithm:
$f(X) = X^8 + X^4 + X^3 + X + 1 = 100011011$

$$\begin{aligned} 100011011 &\equiv 100 \cdot 1000110 + 11 \\ 100 &\equiv 11 \cdot 11 + 1 \end{aligned}$$

$$\begin{aligned} 1 &\equiv 100 - 11 \cdot 11 \\ 1 &\equiv 100 - 11 \cdot (100011011 - 1000110 \cdot 100) \\ 1 &\equiv 100 - 11(100011011) + 11 \cdot 1000110 \cdot 100 \\ 1 &\equiv 100 + 11 \cdot 1000110 \cdot 100 \\ 1 &\equiv 100 + (100011011 - 1000110 \cdot 100) \cdot 1000110 \cdot 100 \\ 1 &\equiv 100 + 100011011 \cdot 1000110 \cdot 100 - (1000110 \cdot 100)^2 \\ 1 &\equiv 100 - (1000110 \cdot 100)^2 \\ 1 &\equiv 100 - 1000110 \cdot 100 \cdot 1000110 \cdot 100 \\ 1 &\equiv 100 \cdot (1 - 100000001010000) \\ 1 &\equiv 100 \cdot 100000001010001 \\ 1 &\equiv 100 \cdot 11001011 \text{ (see below for reduction)} \\ \therefore b^{-1} &\equiv 11001011 \end{aligned}$$

Division by $x^8 + x^4 + x^3 + x + 1 \equiv 100011011$.

$$\begin{array}{r|r} 100011011 & 100000001010001 \\ \hline 1000000 & 100011011...... \\ & 110100100.. \\ 100 & 100011011.. \\ & 101111110. \\ 10 & 100011011. \\ \hline 1000110 & 11001011 \end{array}$$

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

First, we need to find the product $b^{-1}a$:

$$
\begin{array}{r}
1\,1\,0\,0\,1\,0\,1\,1 \\
\times \qquad\quad 1\,1\,0\,0 \\
\hline
1\,1\,0\,0\,1\,0\,1\,1\,\cdot\,\cdot \\
1\,1\,0\,0\,1\,0\,1\,1\,\cdot\,\cdot\,\cdot \\
\hline
1\,2\,1\,0\,1\,1\,1\,2\,1\,0\,0
\end{array}
\equiv 10101110100
$$

We then find the equivalent of this product in F by finding its modulus with
$f(X) = X^8 + X^4 + X^3 + X + 1$

$$
\begin{array}{r|r}
100011011 & 10101110100 \\
\hline
100 & 100011011\,.\,. \\
 & 100011000 \\
10 & 100011011 \\
\hline
110 & 11
\end{array}
$$

The modulus is 11, equivalent to $X + 1$.