CSCI-4116
Assignment 3

Anas Alhadi

B00895875

January 31, 2025

Question 1

The process described in the question can be represented as the composition of the encryption functions of the 2 affine ciphers, so:

Let:

$$F_1 : \mathbb{Z}_m \to \mathbb{Z}_m$$
$$s.t \quad x \mapsto ax + b(\text{mod } m), \qquad x, a, b \in \mathbb{Z}_m$$

And:

$$F_2 : \mathbb{Z}_m \to \mathbb{Z}_m$$
$$s.t \quad x \mapsto cx + d(\text{mod } m), \qquad x, c, d \in \mathbb{Z}_m$$

It follows then that the composition of both encryptions:

$$F_2 \circ F_1 : \mathbb{Z}_m \to \mathbb{Z}_m$$
$$s.t \quad x \mapsto c(a(x) + b) + d(\text{mod } m), \qquad x, a, b, c, d \in \mathbb{Z}_m$$

Which by proposition 2.1 (in the lecture notes) can be written as:

$$F_2 \circ F_1 : \mathbb{Z}_m \to \mathbb{Z}_m$$
$$s.t \quad x \mapsto kx + h(\text{mod } m), \quad k = ca,\ h = cb + d \text{ and } x, k, h \in \mathbb{Z}_m$$

Assuming that k and m are relativley prime (so $F_2 \circ F_1$ is a valid encryption function and the composition is a cryptosystem) then observe that the cryptoanalysis techniques we used in [sec 2.3.2] of the notes still holds. That is the number of possible key combinations for F_1, F_2 and $F_2 \circ F_1$ is the same since they all have the same restrictions on that values of a, c, k and b, d, h in modulo m. Further the plaintext and ciphertext space is the same for the 3 ciphers. So security is not increased.

Question 2

Aside:

Given an integer x we can represent it as a sequence of decimal values:

$$(x_n, \dots, x_0), \quad n = \lceil log_{10} x \rceil$$

So x can be written as the sum:

$$x = \sum_{i=0}^{n} x_i \times 10^i$$

Part a)

Given that $10 \equiv 1 (\bmod 9)$ then by proposition 2.1 (in the lecture notes).

We have it that:

$$10x \equiv x (\bmod 9)$$

Further, observe that (again by prop 2.1):

$$10^n \equiv 1 (\bmod 9), \quad \forall n \in \mathbb{Z}, n \geq 0$$

It follows then that:

$$x = \sum_{i=0}^{n} x_i \times 10^i \equiv \sum_{i=0}^{n} x_i (\bmod 9)$$

That is x is congruent to the sum of all its digits, mod 9. So 9 divides x iff the sum is equal to $0 (\bmod 9)$.

Part b)

Given that $10 \equiv -1 (\bmod 11)$

We make the observation that the congruence can be written in 2 different ways depending on the parity of the power of 10. That is:

$$\begin{aligned} 10^i \quad &\equiv -1 (\bmod 11) \quad & i = 2m+1, m \in \mathbb{Z} \\ &\equiv 1 (\bmod 11) & \text{Otherwise} \end{aligned}$$

So for an integer x (similar to part a. but now divide the sum based on the parity of x_i):

$$x = \sum_{i=0}^{n} x_i \times 10^i$$

$$= \sum_{i=0}^{\frac{n}{2}} x_{2i} \times 10^{2i} \; + \; \sum_{i=0}^{\frac{n}{2}} x_{2i+1} \times 10^{2i+1}$$

Now applying the congrunce relation on the sum:

$$\equiv \sum_{i=0}^{\frac{n}{2}} x_{2i} (\text{mod } 11) + \sum_{i=0}^{\frac{n}{2}} -x_{2i+1} (\text{mod } 11)$$

$$\equiv \sum_{i=0}^{\frac{n}{2}} x_{2i} + \sum_{i=0}^{\frac{n}{2}} -x_{2i+1} \pmod{11}$$

That is, x is congruent to the alternating sum $x_0 - x_1 + x_2 - x_3$ ... modulo 11. Thus 11 divies x iff the alternating sum is equal to $0 (\text{mod } 11)$.

Question 3

Recall that a monoid, is a semi-group that has a neutral element. The concatination of strings is by definition assosiative. So $(\Sigma^*, \circ)$ is a semi-group which contains $\epsilon =$ the empty set, that satisfies the properity:

$$\epsilon \circ a = a \circ \epsilon = a, \qquad \forall a \in \Sigma^*$$

So ϵ is a neutral element and $(\Sigma^*, \circ)$ is a monoid.

On the other hand, for a monoid to be a group, it must satisfy the properity that every element in it is invertibe, however ϵ is the only invertible element in $(\Sigma^*, \circ)$ with $\epsilon^{-1} = \epsilon$. Thus it is not a group.

Question 4

Let a and b be permutations in S_5 such that:

$$a = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{Bmatrix}$$

$$b = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{Bmatrix}$$

Now observe that the composition of the 2 permutations:

$$a \circ b = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{Bmatrix}$$

$$b \circ a = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{Bmatrix}$$

Thus permuting a sequence using b then a may return different values compared to when applying a then b. So the group S_5 is not commutative.

Question 5

Part a)

$n!$ since we are simply permuting on the indicies of the bits, so the permutations are strictly in S_n

Part b)

n We can shift by values 0 ... $n-1$ before we start looping back.

Part c)

The bitwise negation function is an example of such permutation.

That is, let a function

$$f : \{0,1\}^n \to \{0,1\}^n$$

$$\text{s.t} \quad \begin{aligned} f\ x_i = &\quad 1 \quad \text{when } x_i = 0 \\ f\ x_i = &\quad 0 \quad \text{Otherwise} \end{aligned}$$

Observe that for any sequence $x \in \{0,1\}^n$, flippling the bits will result in a unique sequence $y \in \{0,1\}^n$. Further, every element y in the codomain is mapped to by exactly one element x in the domain (where x is just $y's$ negation). That is to say f is a bijective function that maps $\{0,1\}^n \to \{0,1\}^n$. Thus f is a permutation.

However, since f $1000 \mapsto 0111$ this means f is not a valid bit permutation.

> **Aside:**
>
> Bit permutations only permute/"shuffle" the indicies of symbols in a sequence. Permutations are less restrictive as they allow the subsitution of symbols (which as seen above is not always interchangable).