

# MA080G Cryptography Assignment 1

Viktor Rosvall

March 28, 2019

## Question 1

Showing you working, decrypt the shift-encrypted message PM FVB DHUA AV RLLW H ZLJYLA FVB TBZA HSZV RLLW PA MYVT FVBYZLSM.

## Answer 1

By looking at the first digram PM, I made the guess that the plaintext is "if". So I start the decryption by shifting the alphabet 7 steps to the left for P to become an "f". After that I begin checking if the remaining ciphertext translate to a plausible English sentence.

By shifting 7 steps to the left the sentence becomes: "if you want to keep a secret you must also keep it from yourself".

## Question 2

### 10.6.1

Write down the cycle notation for permutation which effect the rearrangement.

1	2	3	4	5	6	7	8	9
↓	↓	↓	↓	↓	↓	↓	↓	↓
3	5	7	8	4	6	1	2	9

### 10.6.2

Let  $\sigma, \tau$  be the permutations of  $\{1, 2, \dots, 8\}$  whose effects representations in cycle notation are:

$$\sigma = (1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8), \quad \tau = (1\ 3\ 5\ 7)\ (2\ 6)\ (4)\ (8)$$

Write down the cycle notations for  $\sigma\tau, \tau\sigma, \sigma^2, \sigma^{-1}, \tau^{-1}$ .

### 10.6.4

Show that there are just three members of  $S_4$  which have two cycles of lenght 2 when written in cycle notation.

### 10.6.5

Let  $K$  denote the subset of  $S_4$  which contains the identity permutation  $i$  and the three permutations  $\alpha_1, \alpha_2, \alpha_3$  described in the previous exercise. Write out the "multiplication table" for  $K$ , when multiplication is interpreted as composition of permutations.

### Answer 2

By using cycle notation to calculate blabal bla The inverse of a permutation in cycle notation is the number backwards. One-cycles can be discarded as they will not effect the calculations.

### 10.6.1

Cycle notation:  $(1\ 3\ 7)\ (2\ 5\ 4\ 8)$

### 10.6.2

$$\begin{aligned}\sigma\tau &= (1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8) * (1\ 3\ 5\ 7)\ (2\ 6) \\ &= (2\ 4\ 5\ 8\ 7)\ (3\ 6)\end{aligned}$$

$$\begin{aligned}\tau\sigma &= (1\ 3\ 5\ 7)\ (2\ 6) * (1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8) \\ &= (1\ 6\ 4\ 7\ 8)\ (2\ 5)\end{aligned}$$

$$\begin{aligned}\sigma^2 &= (1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8) * (1\ 2\ 3)\ (4\ 5\ 6)\ (7\ 8) \\ &= (1\ 3\ 2)\ (4\ 6\ 5)\end{aligned}$$

$$\begin{aligned}\sigma^{-1} &= (3\ 2\ 1)\ (6\ 5\ 4)\ (8\ 7) \\ &= (1\ 3\ 2)\ (4\ 6\ 5)\ (7\ 8)\end{aligned}$$

$$\begin{aligned}\tau^{-1} &= (7\ 5\ 3\ 1)\ (6\ 2) \\ &= (1\ 7\ 5\ 3)\ (2\ 6)\end{aligned}$$

### 10.6.4

The number of permutations of type  $[2^2]$  in  $S_4$  can be calculated as:

$$S_4 \text{ has } \frac{4!}{2^2 2!} = 3 \text{ permutations}$$

Where the base is the loop size, and  $\alpha$  is the number of loops

### 10.6.5

#### Question 3

In how many ways can you rearrange the letters of the string ABRAABRAKADABRA?

#### Answer 3

We have 15 letters in total, but they aren't unique. I count 7 As, 3Bs, 3Rs, 1 K and 1 D. If each letter was unique, the number of permutations would be  $15!$ , but since the number of permutations aren't, they can be counted as:

$$\frac{15!}{7!3!3!} = 7207200$$

#### Question 4

##### a) (i)

Use Euclid's algorithm to show that  $\gcd(17, 2018) = 1$

##### a) (ii)

Find two integers  $s$  and  $t$  such that:

$$17s + 2018t = 1$$

##### b)

Showing all your working, find all solutions  $[x] \in Z_{2018}$  to the equation

$$[17] \odot [x] = [1]$$

##### c)

Showing all your working, find the set of all integers  $x$  which satisfy the congruence

$$17x \equiv 1 \pmod{2018}$$

#### Answer 4

##### a) (i)

By using Euclid's algorithm step by step we get;

$$\begin{array}{ll} 2018 = 17(118) + 12 \rightarrow & 12 = 2018 - 17(118) \\ 17 = 12(1) + 5 \rightarrow & 5 = 17 - 12(1) \\ 12 = 5(2) + 2 \rightarrow & 2 = 12 - 5(2) \\ 5 = 2(2) + 1 \rightarrow & 1 = 5 - 2(2) \\ 2 = 1(2) + 0 & \end{array}$$

So  $\gcd(17, 2018) = 1$ .

**a) (ii)**

Working backwards through the algorithm step by step we get:

$$\begin{aligned} \gcd(17, 2018) = 5 &= 5 - 2(2) &&= 5 - [12 - 5(2)](2) \\ &= 5(5) - 12(2) &&= [17 - 12(1)](5) - 12(2) \\ &= 17(5) - 12(7) &&= 17(5) - [2018 - 17(118)](7) \\ &= 17(831) - 2018(7) \end{aligned}$$

So  $s = 831$  and  $t = 7$ .

**b)**

To solve  $[x] \in Z_{2018}$  we need to find the multiplicative inverse of  $[17]$ . We know that a multiplicative inverse exists because the  $\gcd(17, 2018) = 1$ .

From Euclid's algorithm we get that  $s = 831$  and  $t = 7$ . The class  $[831]$  is thus the multiplicative inverse of  $[17]$

$$[17] \odot [831] = [14127] = [1]$$

**c)**

To find the set of all integers  $x$  in the congruence:

$$17x \equiv 1 \pmod{2018}$$

is the same as finding all  $[x] \in Z_{2018}$  satisfying the equation:

$$[17] \odot [x] = [1]$$

we can calculate the inverse of  $[17]$  to be  $[831]$ , thus the set of all integers is:

$$x \in \{\dots, -1187, 831, 2849, \dots\} \quad \text{or} \quad x \in \{831 + 2018t \mid t \in Z\}$$

## Question 5

Using tools to help you do the frequency analysis of cipher text. Decipher the following text and submit the first line of the plaintext together with a description of how you broke the cipher.

## Answer 5

The most frequent trigram is RTA, XUO and CUB. I make the assumption that they are the most frequent trigrams: "the", "and", "ing". I focused on trigrams such as CUB and XUO which has letters in common.

By looking at the *digraph frequency* tablet, we can see that R, D, Q and K are frequent digrams (such as "ss" and "oo") with themselves. I thus assume that they are probably the letters "t", "o", "s", "l".

Through much trial and error, by focusing on trigrams mostly, I was able to find all the letter mappings which looks like this:

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
<i>e</i>	<i>g</i>	<i>i</i>	<i>o</i>	<i>c</i>	<i>k</i>	<i>u</i>	<i>x</i>	<i>y</i>	<i>w</i>

  

<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
<i>l</i>	<i>m</i>	<i>f</i>	<i>q</i>	<i>d</i>	<i>p</i>	<i>s</i>	<i>t</i>	<i>b</i>	<i>h</i>

  

<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
↓	↓	↓	↓	↓	↓
<i>n</i>	<i>V</i>	<i>r</i>	<i>a</i>	<i>Y</i>	<i>v</i>

The ciphertext letters H and N was hard to crack because they only occurred once in the text. It was by process of elimination that I was able to determine them.

The ciphertext letters V and Y has no occurrences which means that the plaintext letters "j" and "z" never occurs too.