MA080G Cryptography Assignment 1

Viktor Rosvall

Mars 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.

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9 \end{array}$$

10.6.2

Let σ, τ be the permutations of {1, 2,...,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 $[2^2]$ on S_4 can be calculated as:

$$\frac{4!}{2^2 2!} = 3$$

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:

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