M360 Mathematics of Information Security

exercise sheet # 3

Exercise # 1 (1 points)

Decipher the substitution cipher "task 2" on the web (in the web, go to: M360 class homepage → interactive cryptanalysis → substitution cipher). Hint for task 2: h is an f.

Exercise # 2 (2 points)

When picking 2 successive cards from a standard 52-card deck, what is the probability of:

a) The first card is an Ace and the second card is not a Queen?

b) The first card is Spade and the second card is not a Queen?

Exercise # 3 (1 points)

There are 50 cards numbered from 1 to 50. Two different cards are chosen at random. What is the probability that one number is twice the other number?

Exercise # 4 (3 points)

a) Compute the gcd of 122 and 48 and write it in the form $s \cdot 122 + t \cdot 48$ with $s, t \in \mathbb{Z}$.

b) Solve the equation $10x + 15y + 12z = 1$ with integers x, y, z.

c) Show that the equation $12x + 15y + 21z = 1$ does not have a solution with integers x, y, z.

Bonus: For a, b, c and d integers, under which conditions does the equation $ax + by + cz = d$ has integer solutions in x, y, z.

Exercise # 5 (3=1+1+1 points)

The German Enigma used during WWII had three wheels (or rotors) which were serving as permutations $\sigma_1, \sigma_2, \sigma_3$. The wheels formed a sequence such that the permutations were applied one after another as $\sigma_3(\sigma_2(\sigma_1(x)))$, where x is the plaintext symbol. After that, a fixed permutation ρ was applied on the "Umkehrwalze" (return roll). Finally, the inverses of the three permutations were applied in reversed order, and a ciphertext symbol y was output.

In addition, once a letter was enciphered, the first permutation wheel was rotated by one step. If it happened to rotate from 25 to 0, then the second

permutation wheel was rotated once. If the second permutation wheel would rotate from 25 to 0, the third permutation wheel would rotate once (just as we know it from car odometers).

Also, a fixed initial rotation s_1, s_2, and s_3 of the three wheels was chosen at the beginning (the key).

Build your own Enigma from the two attached sheets (just cut out the three wheels from the second sheet and put them centered on top of the wheels on the first sheet; cut along the inner circle!). The shift is the rotation to bring a particular integer of the wheel under the 'A' position on the sheet. Note that the permutations $\sigma_1, \sigma_2, \sigma_3$ (the wheels) are read from "outer to inner" on the way down, and from "inner to outer" on the way back. The permutation ρ is listed at the bottom, in the usual list notation, i.e. it is read from the top row down to the bottom row. Rotate the wheels counterclockwise!

a) Use rotor settings $s_1 = 25$, $s_2 = 13$, and $s_3 = 7$. Encrypt the message

HI

b) The rotor settings $s_1 = 24$, $s_2 = 25$, and $s_3 = 19$ were used to produce the ciphertext

QAV

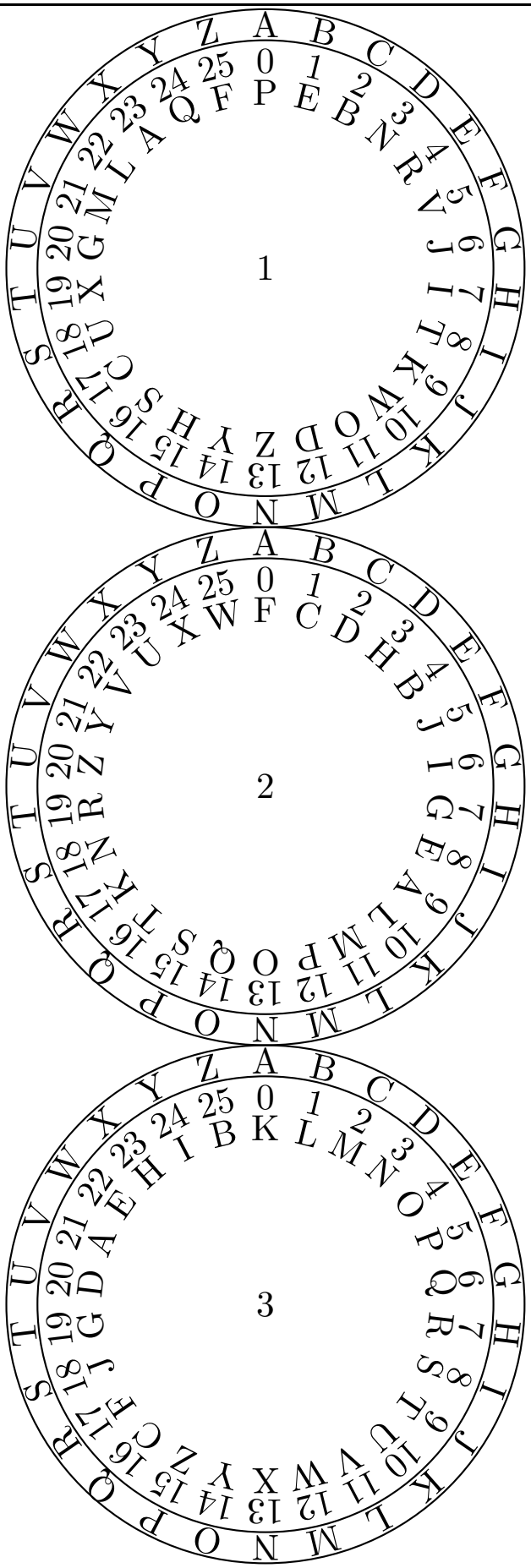
Decrypt the message

c) Rotors 1 and 3 were interchanged with rotor settings $s_1 = 23$ (the shift for the top wheel), $s_2 = 3$, and $s_3 = 7$ to produce the ciphertext

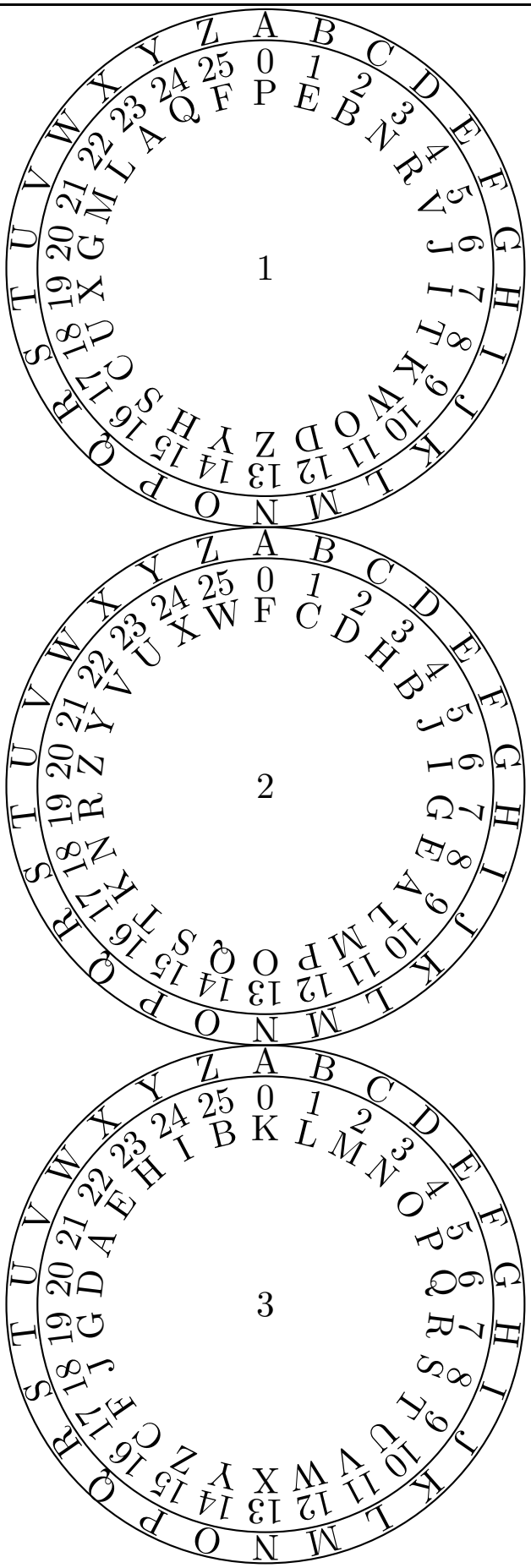
SKNSL BOWU

Decrypt the message.

due to Friday, 9/16/05.



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
M J D C Y S X I H B Z N A L V R T P F Q W O U G E K



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
M J D C Y S X I H B Z N A L V R T P F Q W O U G E K