

# M360 Mathematics of Information Security

## homework sheet # 2

### Problem # 1

Ernie, Bert and the Cookie Monster want to measure the length of Sesame Street. Each of them does it his own way. Ernie relates: “I made a chalk mark at the beginning of the street and then again every 7 feet. There were 2 feet between the last mark and the end of the street” Bert tells you: “Every 11 feet there are lamp posts in the street. The first is 5 foot from the beginning and the last one exactly at the end of the street” Finally Cookie Monster says: “starting at the beginning of Sesame Street, I put down a cookie every 13 feet. I ran out of cookies 22 feet from the end.” All three agree that the length does not exceed 1000 feet. How many feet is Sesame Street long?

### Problem # 2

- a) Let  $p$  be prime. Suppose  $a$  and  $b$  are integers such that  $ab \equiv 0 \pmod{p}$ . Show that either  $a \equiv 0$  or  $b \equiv 0 \pmod{p}$ .
- b) Show that if  $a, b, n$  are integers with  $n \mid ab$  and  $\gcd(a, n) = 1$ , then  $n \mid b$ .

### Problem # 3

Let  $p \geq 3$  be prime. Show that the only solution to  $x^2 \equiv 1 \pmod{p}$  are  $x \equiv \pm 1 \pmod{p}$ . *Hint:* Apply part a) of the previous exercise to  $(x + 1)(x - 1)$ .

### Problem # 4

Suppose  $x \equiv 3 \pmod{7}$  and  $x \equiv 3 \pmod{10}$ . What is  $x$  congruent to mod 70?

### Problem # 5

You are trying to cryptanalyze an affine enciphering transformation of single-letter message units in a 37-letter alphabet. This alphabet includes the numerals 0-9, which are labeled by themselves (i.e., by the integers 0-9). The letters A-Z have numerical equivalents 10-35, respectively, and blank=36. You intercept the ciphertext “OH7F86BB46R3627O266BB9” (here the O’s are the letter “oh”, not the numeral zero). You know the plaintext ends with the signature “007” (zero zero seven). What is the message?

### Problem # 6

You intercept the ciphertext “OFJDFOHFXOL”, which was enciphered using an affine transformation of single-letter plaintext units in the 27-letter alphabet (with blank=26). You know that the first word is “I” (“I” followed by blank). Determine the enciphering key, and read the message.

### Problem # 7

Suppose you have a language with only 3 letters  $a, b, c$ , and they occur with frequencies  $.7, .2, .1$ , respectively. The following ciphertext was encrypted by the Vigenère method (shifts are mod 3 instead of mod 26, of course):

CAAABBCACBCABACAABCCCACA.

Show that it is likely that the key length is 2, and determine the most probable key.

**Problem # 8**

- a) Convert 966 into binary, convert  $(110101011)_2$  into decimal.
- b) Convert  $(54265)_7$  into base 13.

**Problem # 9**

Divide  $2^{10203}$  by 101. What is the remainder?

**Problem # 10**

Find the last 2 digits of  $123^{562}$ .

**Problem # 11**

- (a) Solve  $7d \equiv 1 \pmod{30}$
- (b) Suppose you write a message as a number  $m \pmod{31}$ . Encrypt  $m$  as  $m^7 \pmod{31}$ . How would you decrypt? *Hint:* Decryption is done by raising the ciphertext to a power mod 31. Fermat's theorem will be useful.

**Problem # 12**

- a) Evaluate  $7^7 \pmod{4}$ .
- b) Use part a) to find the last digit of  $7^{7^7}$ . Note  $a^{b^c}$  means  $a^{(b^c)}$  since the other possible interpretation would be  $(a^b)^c = a^{bc}$ , which is written more easily without a second exponentiation. *Hint:* the last digit is computing mod 10. Then use Chinese Remainder Theorem.

**Problem # 13**

Let  $U_n = \{i \in \mathbb{Z} \mid 1 \leq i \leq n, \gcd(i, n) = 1\}$ . Let  $\phi(n) = |U_n|$  be the Euler-function. Show that for a prime  $p$  and a positive integer  $a$  we have  $\phi(p^a) = p^a - p^{a-1}$ .

**Problem # 14**

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  $\rho$  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  $\rho$  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

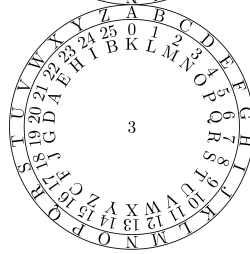
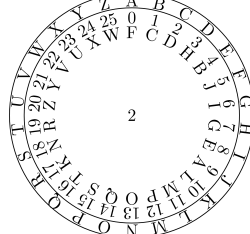
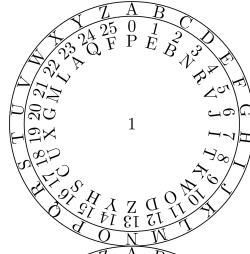
- c) Rotors 1 and 3 were interchanged with rotor settings  $s_1 = 23$  (the shift for the top wheel),  $s_2 = 3,$  and  $s_3 = 7$  to produce the ciphertext

SKNSL BOWU

Decrypt the message.

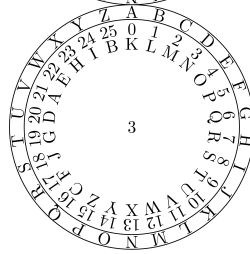
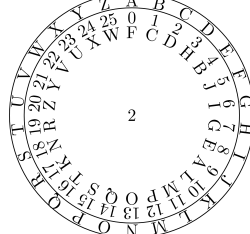
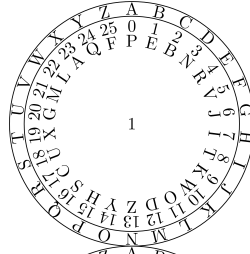
not collected.





ABCDEFGHI JKLMNOPQRSTUVWXYZ  
 MJD CYSX IH BZNLVRTPFQWOUGEK





ABCDEFGHI JKLMNOPQRSTUVWXYZ  
 MJD CYSX IH BZNLV R T P F Q W O U G E K