IDATT2503 - Cryptography - Fall 2024

Crypto Assignment 1

Problem 1

b) Calculate $-99 \bmod 1001$

c) Calculate $232 + 22 \cdot 77 - 18^3 \bmod 8$

d) Determine if $55 \equiv 77 \pmod{12}$

Problem 2

A number $a \in \mathbb{Z}_n$, i.e. an integer modulo n, has a *multiplicative inverse* if there exists $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \pmod{n}$.

a) Write the multiplication table of the elements of $\mathbb{Z}_{12}$, excluding the 0 element.

b) Which integers have a multiplicative inverse modulo 12?

c) Do the same for $\mathbb{Z}_{11}$. Which numbers have mult.inverse mod 11?

d) Find the multiplicative inverse to 11 modulo 29, by trial and error, ie. just try different values.

e) Formulate a condition for a to have a multiplicative inverse modulo n.

Hint: It involves the factorisations of a and n.

Problem 3 - Affine ciphers

We use small letters a-z for plain text, and cipher texts with capital letters, to distinguish the plain texts from cipherstext, but they represent the same alphabet, i.e. there are 26 letters.
We enocde the letters with numbers from 0 to 25, consideres as elements in $\mathbb{Z}_{26}$, the integers modulo 26.
The function $e_k : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ is given by the formula

$$e_k(x) = (3 \cdot x + 11) \mod 26$$

. The key is the pair $k = (3, 11)$

a) Write e_k as a permutation, i.e. the sequence of letters we get when encrypting a, b, c etc.

b) Use e_k to encrypt the message $m =$ 'alice'

c) Find the inverse of e_k as a

- permutation as in part a)
- as a formula $d_k(y) = ay + b \pmod{26}$ (the decryption) where you have to determine a and b.

  Hint: Invert the formula for e_k, where you need to use a multiplicative inverse.

d) Use the inverse d to decrypt $c = \text{RBKKXRQ}$

e) How secure is this cipher, compared to a rotation cipher? Consider both brute force and known plaintext attacks.

f) How many legal keys does are there for this choice of formula and alphabet?

Problem 4

You (an eavesdropper) see the following message from Alice to Bob (Only letters are included, and then grouped into fives):

RGMRQ ERQMZ MZXMD ENNZU QFD

You know they use a affine cipher. Use brute force to find plain text and key

Problem 5

The following ciphertext has been encrypted from English with a simple substitution cipher using the alphabet a - z and the space character, so that there are 27 letters. This is to make it easier to recognize words. So the space will be replaced by some other letter, and some other letter is replaced with a space. Otherwise there all other punctuations and line breaks are removed from the text.
Use statistical analysis to find the decrypted message. A tool that you can use is `https://www.dcode.fr/frequency-analysis` Here you can see the statistics of each letter but also for two or more letter combinations (digrams, trigrams etc). The first step is perhaps to get the spaces in the right place!
NB! There is a space at the end of each line in the ciphertext. So in your processing you need to keep a single space between the lines. There are also places where there are two successive spaces, you need to keep these. Technically, you should simply remove the newlines.
UPDATE: Below is a version of the text where spaces are shown as dots. There are no newlines so they need to be ignored. The text is also provided as a text-file in Blackboard.

```
UCBCKOPTKMI QEDVSMV Q S
QCBDEKBDQBDAIBIWKODIKVQOYDMIDMWCFIBDSVQBADHWIXSIBEYDKBKOYVQVD
TQVDCBOYDRCWFVDRIOODQHD TIDPOKQB IG DQVDOCBADIBCSATDKBJDQVDBC D
CCDJQHHIWIB DHWCUDBCWUKOD IG DCBIDVTCSOJDKOVCDFBCRDRTK DOKBASKAID TIDPOKQB
IG DQVDRWQ  IBDQBDKVD TIDHWIXSIBEQIVDCHDOI  IWVDLKWYDHWCUDOKBASKAID
CDOKBASKAIDVCUID IG VDKWIDTKWJIWD CDMWIKFD TKBDC TIWVDKBDIGKUPOIDQVD
TIDVIB IBEID TIDXSQEFDMWCRBDHCGDNSUPVDCLIWD TIDOKZYDJCAD TQVDVIB
IBEIDECB KQBVDILIWYDOI  IWDCHD TIDKOPTKMI DBC DTIOPQBAD TIDEWYP
KBKOYV DACCJDOSEF

UCBCKOPTKMI.QEDVSMV.Q.S.
QCBDEKBDQBDAIBIWKODIKVQOYDMIDMWCFIBDSVQBADHWIXSIBEYDKBKOYVQVD.
TQVDCBOYDRCWFVDRIOODQHD.TIDPOKQB.IG.DQVDOCBADIBCSATDKBJDQVDBC.D.
CCDJQHHIWIB.DHWCUDBCWUKOD.IG.DCBIDVTCSOJDKOVCDFBCRDRTK.DOKBASKAID.
TIDPOKQB.IG.DQVDRWQ..IBDQBDKVD.TIDHWIXSIBEQIVDCHDOI..IWVDLKWYDHWCUDOKBASKAID.
CDOKBASKAIDVCUID.IG.VDKWIDTKWJIWD.CDMWIKFD.TKBDC.TIWVDKBDIGKUPOIDQVD.
TIDVIB.IBEID.TIDXSQEFDMWCRBDHCGDNSUPVDCLIWD.TIDOKZYDJCAD.TQVDVIB.
IBEIDECB.KQBVDILIWYDOI..IWDCHD.TIDKOPTKMI.DBC.DTIOPQBAD.TIDEWYP.
KBKOYV.DACCJDOSEF
```