FRANCESCA GRIMALDI

# IDATT2503 - Kryptografi - Høst 2022

## Cryptography assignment 1

### Task 1

a) Show that $a\%n = b\%n$ (which we can also write as $a \mod n = b \mod n$) if and only if $a \equiv b \pmod n$

b) Calculate $-99 \mod 1001$

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

d) Decide whether $55 \equiv 77 \pmod{12}$

a) To show that $a\%n = b\%n \iff a \equiv b \pmod n$, we have to prove the implication in both directions.

FIRST DIRECTION $a\%n = b\%n \Rightarrow a \equiv b \pmod n$

For the definition of modulus we can write

$a = k_1 \cdot n + r_1$

$b = k_2 \cdot n + r_2$

Given $a\%n = b\%n$, we know that the remainders are the same, so $r_1 = r_2 = r$.

Subtracting the two equations,

$a - b = k_1 \cdot n + r - k_2 \cdot n + r$

$a - b = (k_1 - k_2)\, n$

This means that $(a-b)$ is a multiple of $n$.

$a \equiv b \pmod n$ means that $a$ and $b$ leave the same remainder when divided by $n$, and that $n$ divides $(a-b)$ which is written as $n \mid (a-b)$. From the latter, $(a-b)$ is a multiple of $n$.

Therefore, $a\%n = b\%n \Rightarrow a \equiv b \pmod n$

SECOND DIRECTION $a \equiv b \pmod n \Rightarrow a\%n = b\%n$

The statement $a \equiv b \pmod n$ means that $(a-b)$ is a multiple $n$, so we can write $(a-b) = k \cdot n$, with $k$ integer value.

Applying the modulus operator to both sides of the equation,

$(a-b)\%n = (k \cdot n)\%n$

this equals to zero, because we are dividing a multiple of n by n itself

$(a-b)\%n = 0$, which means that $a\%n = b\%n$, as we wanted to show.

As we have showed both directions, $a\%n = b\%n \iff a \equiv b \pmod n$ is proved as well.

b) $-99 = -1 \cdot 1001 + 902$
$\Rightarrow -99 \bmod 1001 = 902$

c) $(232 + 22 \cdot 77 - 18^3) \bmod 8 =$
$= -3906 \bmod 8$
$-3906 = -489 \cdot 8 + 6 \Rightarrow -3906 \bmod 8 = 6$

d) $55 \,\%\, 12 = 7$ because $55 = 12 \cdot 4 + 7$
$77 \,\%\, 12 = 5$ because $77 = 12 \cdot 6 + 5$
The two numbers do not leave the same remainder when divided by 12, so they are <u>not</u> congruent modulo 12.

**Task 2**

A number $a \in Z_n$, i.e. a number modulo $n$, is said to have a multiplicative inverse if there exists $b \in Z_n$ so that $ab \equiv 1 \pmod{n}$.

a) Write the multiplication table in $Z_{12}$, (without including the row or column for the 0 time).

b) Which numbers have multiplicative inverses modulo 12?

c) Do the same for $Z_{11}$. What numbers have a multiplicative inverse mod 11?

d) Find a multiplicative inverse to 11 modulo 29, with "brute force"

e) Formulate a connection between the fact that $a$ has a multiplicative inverse modulo $n$, and whether the number has common factors with $n$.

a) Multiplication table in $\mathbb{Z}_{12}$

| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 2 | 2 | 4 | 6 | 8 | 10 | 0 | 2 | 4 | 6 | 8 | 10 |
| 3 | 3 | 6 | 9 | 0 | 3 | 6 | 9 | 0 | 3 | 6 | 9 |
| 4 | 4 | 8 | 0 | 4 | 8 | 0 | 4 | 8 | 0 | 4 | 8 |
| 5 | 5 | 10 | 3 | 8 | 1 | 6 | 11 | 4 | 9 | 2 | 7 |
| 6 | 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 | 0 | 6 |
| 7 | 7 | 2 | 9 | 4 | 11 | 6 | 1 | 8 | 3 | 10 | 5 |
| 8 | 8 | 4 | 0 | 8 | 4 | 0 | 8 | 4 | 0 | 8 | 4 |
| 9 | 9 | 6 | 3 | 0 | 9 | 6 | 3 | 0 | 9 | 6 | 3 |
| 10 | 10 | 8 | 6 | 4 | 2 | 0 | 10 | 8 | 6 | 4 | 2 |
| 11 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

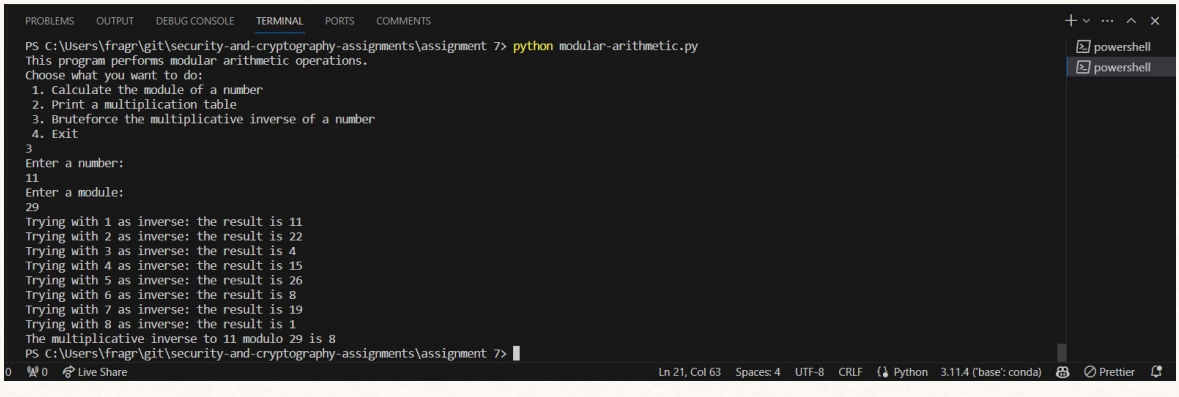
b) The numbers that have multiplicative inverses modulo 12 are 1, 5, 7 and 11.

c) Multiplication table in $\mathbb{Z}_{11}$

| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2 | 2 | 4 | 6 | 8 | 10 | 1 | 3 | 5 | 7 | 9 |
| 3 | 3 | 6 | 9 | 1 | 4 | 7 | 10 | 2 | 5 | 8 |
| 4 | 4 | 8 | 1 | 5 | 9 | 2 | 6 | 10 | 3 | 7 |
| 5 | 5 | 10 | 4 | 9 | 3 | 8 | 2 | 7 | 1 | 6 |
| 6 | 6 | 1 | 7 | 2 | 8 | 3 | 9 | 4 | 10 | 5 |
| 7 | 7 | 3 | 10 | 6 | 2 | 9 | 5 | 1 | 8 | 4 |
| 8 | 8 | 5 | 2 | 10 | 7 | 4 | 1 | 9 | 6 | 3 |
| 9 | 9 | 7 | 5 | 3 | 1 | 10 | 8 | 6 | 4 | 2 |
| 10 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

All numbers 1-10 have a multiplicative inverse modulo 11.

d) To find a multiplicative inverse to 11 modulo 29, one has to find the number m such that
$(11 \cdot m) \% 29 = 1$
This can be done bruteforcing each number from 1 to m and checking the result.
For this, I used the `find_inverse` function that can be found in the `modular_arithmetic.py` file, and found that 8 is multiplicative inverse to 11 modulo 29.
In fact, $(11 \cdot 8) \% 29 = 88 \% 29 = 1$
↳ $88 = 29 \cdot 3 + 1$




e) From the two examples above, it is possible to notice that if the number a has common factors with n (not considering the number 1), then a does not have multiplicative inverse modulo n. Each number in $\mathbb{Z}_{11}$ table has a multiplicative inverse, and 11 has no common factors (other than 1) with the others. In $\mathbb{Z}_{12}$ table, the only numbers with multiplicative inverse are 1, 5, 7, 11: all numbers that have no common factors

with 12 ($12 = 2^2 \cdot 3$).
The presence of a multiplicative inverse modulo n is a sign of the fact that a and n are coprime.

**Task 3**

We will use the alphabet a-å (small letteres only) for plain text, and write cipher text in capital letters. We also identify the letters with the numbers from 0 to 28, considered as numbers in $Z_{29}$, i.e. the integers modulo 29.
We have a function $f : Z_{29} \to Z_{29}$ given by the formula

$$f(x) = (11 \cdot x - 5) \mod 29$$

a) Write down the values of $f$ as a sequence $f(0), f(1), \ldots, f(28)$. Convert the numbers to letters. (You can easily create code that calculates this, but it is also a good idea to calculate some of the numbers by hand as well.)

b) Explain that $f$ is a *permutation* of $Z_{29}$.

c) Find the inverse permutation $f^{-1}$ to $f$, both

- as a sequence of values $f^{-1}(0), f^{-1}(1), \ldots$
- as a formula of the form $f^{-1}(y) = ay + b \pmod{29}$, i.e. determine $a$ and $b$.

d) Use $f$ as the key in a simple substituion cipher to enrcrypt the message m = 'alice'

e) Use $f$ as the key and *dekrypt* c = SIØPBE

a) $f(0) = (11 \cdot 0 - 5) \mod 29 = -5 \mod 29 = 24$ → letter Y
(0 = letter a; $-5 = -1 \cdot 29 + 24$)
$f(1) = (11 \cdot 1 - 5) \mod 29 = 6 \mod 29 = 6$ → letter G
$f(2) = (11 \cdot 2 - 5) \mod 29 = 17 \mod 29 = 17$ → letter R
$f(3) = (11 \cdot 3 - 5) \mod 29 = 28 \mod 29 = 28$ → letter Å
$f(4) = (11 \cdot 4 - 5) \mod 29 = 39 \mod 29 = 10$ → letter K
⋮
$f(28) = (11 \cdot 28 - 5) \mod 29 = 303 \mod 29 = 13$ → letter N
(28 = letter å; $303 = 10 \cdot 29 + 13$)

```
f( 0 a ) = 24 which corresponds to letter y
f( 1 b ) = 6 which corresponds to letter g
f( 2 c ) = 17 which corresponds to letter r
f( 3 d ) = 28 which corresponds to letter å
f( 4 e ) = 10 which corresponds to letter k
f( 5 f ) = 21 which corresponds to letter v
f( 6 g ) = 3 which corresponds to letter d
f( 7 h ) = 14 which corresponds to letter o
f( 8 i ) = 25 which corresponds to letter z
f( 9 j ) = 7 which corresponds to letter h
f( 10 k ) = 18 which corresponds to letter s
f( 11 l ) = 0 which corresponds to letter a
f( 12 m ) = 11 which corresponds to letter l
f( 13 n ) = 22 which corresponds to letter w
f( 14 o ) = 4 which corresponds to letter e
f( 15 p ) = 15 which corresponds to letter p
f( 16 q ) = 26 which corresponds to letter æ
f( 17 r ) = 8 which corresponds to letter i
f( 18 s ) = 19 which corresponds to letter t
f( 19 t ) = 1 which corresponds to letter b
f( 20 u ) = 12 which corresponds to letter m
f( 21 v ) = 23 which corresponds to letter x
f( 22 w ) = 5 which corresponds to letter f
f( 23 x ) = 16 which corresponds to letter q
f( 24 y ) = 27 which corresponds to letter ø
f( 25 z ) = 9 which corresponds to letter j
f( 26 æ ) = 20 which corresponds to letter u
f( 27 ø ) = 2 which corresponds to letter c
f( 28 å ) = 13 which corresponds to letter n
```

← Full sequence of characters, generated using function print_sequence in Python file task3.py

b) $f$ is a permutation of $\mathbb{Z}_{29}$ because its codomain consists of all the values of $\mathbb{Z}_{29}$ (numbers from 0 to 28), but in a shuffled order.

c) $f(x) = (11x - 5) \bmod 29 = y$

To find $f^{-1}(y) = x$, we need to solve $11x - 5 \equiv y \pmod{29}$

to eliminate 11, we multiply by its multiplicative inverse as found in TASK 2b ↓

$11x \equiv (y+5) \pmod{29}$

$x \equiv 8(y+5) \pmod{29}$

so the general formula is $f^{-1}(y) = (\underbrace{8}_{a}y + \underbrace{40}_{b}) \pmod{29}$

```
f^-1( 0 a ) = 11 which corresponds to letter l
f^-1( 1 b ) = 19 which corresponds to letter t
f^-1( 2 c ) = 27 which corresponds to letter ø
f^-1( 3 d ) = 6 which corresponds to letter g
f^-1( 4 e ) = 14 which corresponds to letter o
f^-1( 5 f ) = 22 which corresponds to letter w
f^-1( 6 g ) = 1 which corresponds to letter b
f^-1( 7 h ) = 9 which corresponds to letter j
f^-1( 8 i ) = 17 which corresponds to letter r
f^-1( 9 j ) = 25 which corresponds to letter z
f^-1( 10 k ) = 4 which corresponds to letter e
f^-1( 11 l ) = 12 which corresponds to letter m
f^-1( 12 m ) = 20 which corresponds to letter u
f^-1( 13 n ) = 28 which corresponds to letter å
f^-1( 14 o ) = 7 which corresponds to letter h
f^-1( 15 p ) = 15 which corresponds to letter p
f^-1( 16 q ) = 23 which corresponds to letter x
f^-1( 17 r ) = 2 which corresponds to letter c
f^-1( 18 s ) = 10 which corresponds to letter k
f^-1( 19 t ) = 18 which corresponds to letter s
f^-1( 20 u ) = 26 which corresponds to letter æ
f^-1( 21 v ) = 5 which corresponds to letter f
f^-1( 22 w ) = 13 which corresponds to letter n
f^-1( 23 x ) = 21 which corresponds to letter v
f^-1( 24 y ) = 0 which corresponds to letter a
f^-1( 25 z ) = 8 which corresponds to letter i
f^-1( 26 æ ) = 16 which corresponds to letter q
f^-1( 27 ø ) = 24 which corresponds to letter y
f^-1( 28 å ) = 3 which corresponds to letter d
```

← Full sequence of values of the inverse permutation, generated using function `print_inverse_sequence` in Python file `task3.py`

d) $m =$ "alice"

Knowing that $f(a) = y$, $f(l) = a$, $f(i) = z$, $f(c) = r$ and $f(e) = k$

$C = f(a)f(l)f(i)f(c)f(e) =$ YAZRK

The same result is obtained using function `encrypt` in Python file `task3.py`

e) $c =$ SIØPBE

Knowing that $f^{-1}(s) = k$, $f^{-1}(i) = r$, $f^{-1}(ø) = y$, $f^{-1}(p) = p$, $f^{-1}(b) = t$ and $f^{-1}(e) = o$

$m = f^{-1}(s)f^{-1}(i)f^{-1}(ø)f^{-1}(p)f^{-1}(b)f^{-1}(e) =$ krypto

The same result is obtained using function `decrypt` in Python file `task3.py`

**Task 4**

You have intercepted the following message between Alice and Bob: (Here, spaces from the plaintext have been removed, and the ciphertext is grouped by 5 characters.)

YÆVFB VBVFR ÅVBV

You know that Alice and Bob use a k-skift-cipher. Use brute-force to find the encryption key and plaintext.
Feel free to write a program to help you.

Knowing that Alice and Bob used a k-shift-cipher, it is possible to make different attempts in decrypting the message trying all values between 1 and 29 for the shift. Then, each output is checked to see if there is a complete sentence.
For this, I created a program (shift-cipher.py) through which I found that the used shift was 17, and the sentence "hjernen er alene".
(All the outputs are included in the bruteforce.txt file).

**Task 5**

In this exercise you will use the Vigènere cipher. (It was not Vigènere who invented the cipher, but it was first described by Giovan Battista Bellaso in 1553.) It is a type of polyalphabetic substitution cipher, i.e. the encryption of a character is not the same for each occurrence. It also depends on where the character is in the plain text.
Give a keyword, e.g. 'lat', and a text "fisk", then a message is encrypted in the following way:

- the first character in the plaintext 'f' value 5, is encrypted with the shift-cipher with the letter 'l' (value 11) as key, which gives 5 + 11 = 16, i.e. 'Q'
- the second character 'i' is encrypted with the key 'a', which gives 'I'
- the third character 's' is encrypted with the key 't' which gives 'I'
- the fourth character 'k' is encrypted with 'l' (starting from the beginning of the keyword), which gives 'V'
- the fifth character would be encrypted with 'a' again, etc

So 'fisk' encrypted with 'lat' becomes QIIV.

a) Encrypt the text "Snart helg" with the keyword "torsk".

b) Decrypt QZQOBVCAFFKSDC with the keyword "brus".

c) If the keyword has length 15, how many keys are there? Would you consider this secured in terms of a brute-force attack?

It was long thought that Vigenere cipher was 'unbreakable'. It is not, as was shown in 1863.

a) m = "Snart helg", K = "torsk"
To encrypt the first character using Vigènere cipher, one has to sum the value of S with that of t: 18 + 19 = 37, and then calculate this result modulo 29 → 37 % 29 = 8 which corresponds to letter I.
(29: letters in Norwegian alphabet)

The procedure is the same for each character, and when the end of the keyword is reached, we go back to its beginning.
Using the encrypt function in vigenere.py, the encrypted text is
c = IØRGA ÆSÅY

b) Similarly, using the decrypt function in vigenere.py, the plaintext is m = pizza eller taco.

c) If the keyword has 15 letters, there are $29^{15}$ possible keys because each position has 29 possible characters.
Being a big number, this could be secure against brute force only ciphertext attacks.