## 9.1 The Caesar Cipher

One assigns a number from the residue class ring ℤ/26ℤ to each letter from a to z, as The Caesar cipher , also called the shift cipher, works as follows: shown in the table.

Table 5: Assignment of letters to numbers from ℤ/26ℤ

3 8 4 18 8 18 19 4 8 13 4 6 4 7 4 8 12 4 13 0 2 7 17 8 2 7 19

Source: Brückmann, 2013.

The word “hello” could therefore be represented by the sequence of numbers 7 4 11 11 14, for example: the letter h corresponds to the number 7, the letter e is assigned the number 4, l is replaced by 11 and o by the number 14.

Special characters, punctuation marks and blanks are initially ignored.

The idea of the Caesar cipher is to first convert the given plaintext into its corresponding

fixed value (please note that of course you have to calculate in ℤ/26ℤ!). The sequence of sequence of numbers and then to add a previously defined value to each number. This previously agreed value is called the key of the cryptosystem. All numbers are shifted by a

numbers transformed in this way is then transferred back into a text of letters using the above table. This is how the ciphertext is created.

Example: Encryption and decryption in the Caesar cipher We choose the value 17 as the key and use it to encrypt the message:

This is a secret message.

To do this, we first convert the text into the corresponding numerical sequence using the table above. We receive:

3 8 4 18 8 18 19 4 8 13 4 6 4 7 4 8 12 4 13 0 2 7 17 8 2 7 19 residue class ring ℤ/26ℤ. It follows that: Now we must add the key 17 to each number. Please note that we have to calculate in the 38418++++ 17

This results in the sequence of numbers:8413464719818++++++++++++++17171717171717171717171717171717171717171717171717===========================212125211721252120192425242321251924252934363030363535 ======== 3449810910

2074817134122 +++++++++17 7819

20 25 21 9 25 9 10 21 25 4 21 23 21 24 21 25 3 21 4 17 19 24 8 25 19 24 10

To obtain the ciphertext, we translate this sequence of numbers back into a sequence of letters using the table above. The ciphertext therefore reads:

u z v j z j k v z e v x v y v z d v e r t y i z t y k

The decryption of a ciphertext works completely analogously. We also need the previously chosen key for this. The only difference is that this time we do not add the value of the key but subtract it from the numbers. In this way we calculate back the numerical values and get the original plain text. The recipient of the secret message

u z v j z j k v z e v x v y v z d v e r t y i z t y k

would therefore first translate this into the corresponding numerical sequence and gets

20 25 21 9 25 9 10 21 25 4 21 23 21 24 21 25 3 21 4 17 19 24 8 25 19 24 10

Now he would subtract the chosen key, in this case 17, from each individual numerical252192591020++++++++++−−−−−−−−−−−171717171717ℤ/26ℤ=

2125423

21242121++ 4171932521+++++

The result of this calculation is therefore the sequence of numbers:value (again, of course, as a calculation in 10241982524+−−−++++−+−−−−−−−−−17171717−−−1711717171717171717177171717171717==========================28−7−−−−−−07486444448278−873981811):3374========1918171812131319

3 8 4 18 8 18 19 4 8 13 4 6 4 7 4 8 12 4 13 0 2 7 17 8 2 7 19

This can now be translated back into a sequence of letters using our table to preserve the original plain text. It results in:

this is a secret message

(Please note that as this book has been translated from German, this exercise reveals a German message: dies ist eine geheime Nachricht, which translates to “this is a secret message.”)

characters from above. Instead of expecting 26 letters in ℤ/26ℤ, we could extend the char-k ∈ ℕ You have noticed that special characters, punctuation marks, and spaces are initially

acter set and perform all operations in ℤ/kℤ if the new table then has entries. ignored in this procedure. However the table could easily be extended with additional