I Replaced:

```
a = z
b = y
c = x
d = w
e = m
f = u
g = t
h = s
i = r
j = q
k = p
l = o
m = e
n = v
o = l
p = k
q = j
r = i
s = h
t = g
u = f
v = n
w = d
x = c
y = n
z = a
```

I started with the links because its easy to predict.

The main assignment of today can be found on https://www.os3.nl/_media/2017-2018/courses/ssn/ssn_lab1.pdf and the template for your answeres can be found on https://www.os3.nl/2017-2018/courses/ssn/lab1_template Please note that these templates will not be created in the future, so please make sure you know how to use dokuwiki. with kind regards,

QUESTION 1:

(A) What is Affine? The Affine cipher is a monoalphabetic substitution cipher. It used mathematical formulas for encryption and decryption. In affine cipher we can add or multiply or we can do both together. However, we cannot multiply by any number. The numbers must not have a common factor with m(length of alphabet). Ex: we can multiply by 3, but not 8. Because 8 and 26 can be both divided by 2. If we have number bigger than 25 we need to use modular arithmetic.

```
Encryption:
C = (ax +b) mod m.  m = alphabet letters length, x = Plain letter, a and b = key.
So in Affine cipher key should be 2 integers.
Ex: encrypt ¨GO¨ using affine cipher key(7:a,2:b):
(C(G) = (7*6+2) mod 26) = 18 which is letter ¨s¨
```

```
(C(O) = (7*14+2) mod 26) = 22 which is letter ¨w¨
¨GO¨" --> ¨SW¨
```

```
Decryption:
D = a^-1 (c - b). where D is the letter that we need to decrypt.
Ex: decrypt ¨SW¨ using affine cipher key(7:a,2:b):
D(S) = 15(16) = 240 mod 26 = 6 which is letter ¨s¨
D(W) = 15(20) = 300 mod 26 = 14 which is letter ¨o¨

¨SW¨-->¨GO¨"
```

Resource: https://www.youtube.com/watch?v=bnsGxuoAOZs

(B) What is Atbash? The Atabash is a monoalphabetic substitution cipher originally used for the Hebrew. It's very simple to use but its simplicity is it's biggest fall. Because it used a straightforward way of encryption which is the first letter of the alphabet is encrypted to the last letter of the alphabet, the second letter to the penultimate letter and so on.

```

Encryption:
        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
        z y x w v u t s r q p o n m l k j i h g f e d c b a
```

Decryption:

```
      To encipher a message, find the letter you wish to encipher in the top
row, then replace it with the letter in the bottom row we encipher the
message 'ATTACK AT DAWN'. The first letter we wish to encipher is 'A', which
is above 'Z', so the first ciphertext letter is 'Z'. The next letter is 'T',
which is above 'G', so that comes next. The whole message is enciphered:
```

```
ATTACK AT DAWN
ZGGZXP ZG WZDM
```

(C) What is ADFGVX? The ADFGVX cipher was used by the German army in World War I. It is an extension of an earlier version called ADFGX. The cipher is named after the six possible letters used in the ciphertext: A, D, F, G, V and X. The letters were chosen to reduce the probability of operator error (sound very different in Morse code). It is a fractionation transposition cipher. It has 6×6 squares which is 36 boxes (a-z and 0-9). So how it works ? first we should specify a keyword. this keyword will be filled in the 6×6 boxes if its less we fill the not repeated alphabet sequence in the remaining boxes. so at the end of the day we should have in the 6×6 squares table the 26 letters and the numbers 0-9.

How ADFGVX working in depth?

```
I- ADFGVX key is a key square ex:
p h 0 q g 6
4 m e a 1 y
l 2 n o f d
x k r 3 c v
s 5 z w 7 b
```

```
j 9 u t i 8

II- The key square is 6x6 square containing all letters and numbers 0-9. and
its keyword is any number.

III- Steps:

a- Build a table with the key square.
    A D F G V X
A | p h 0 q g 6
D | 4 m e a 1 y
F | l 2 n o f d
G | x k r 3 c v
V | s 5 z w 7 b
X | j 9 u t i 8
```

b- Encode the text using this matrix. For example, if we want to decrypt the letter 'a', we take its (x, y) location on the matrix. So X and Y axes for this letter is the encryption pair for that letter. e.g: 'attack' 'a' = DG, 't' = XG, 't' = XG, 'a' = DG, 'c' = GV, 'k' = GD.

Encryption: To encrypt a message a mixed polybius square is drawn up with the cipher name letter as heading. The keyword is written in the squares, if it contains redundant letters we remove them and the remaining squares will be filled with the remaining letters that are not exist in the KEYWORD and we must fill them alphabetically. The new text is then written out in rows beneath the second keyword and columnar transposition is performed, rearranging the columns so the letters of the keyword are in alphabetical order.

Example: Encrypt a text “attack at 1200am” using keyworks 147 regiment and privacy:

```

 A D F G V X
A | 1 4 7 r e g
D | i m n t a b
F | c d f h j k
G | l o p q s u
V | v w x y z 0
X | 2 3 5 6 8 9

The coordinates of each letter:
a = DV, t = DG, t = DG, a = DV, c = FA, k = FX, a = DV, t = DG, 1 = AA, 2 =
XA, 0 = VX, 0 = VX, a = DV, m = DD .
```

Now we take this generated text, and write it our in rows beneath the keyword privacy. We also number the letters of the keyword in alphabetical order.

The ciphertext is then read off down the columns, in the order of the numbers (alphabetical order of the keyword. We get “DXXV GDAD DAAX DVDX VFGV GFAD DVVD”.

Decryption: We must first undo the Columnar Transposition by writing the ciphertext in the grid in the right way. Then we read off the rows (with the keyword correctly ordered) and finally convert the pairs of letters back to plaintext using the Mixed Square.

Ex: Decrypt the cipher text “ADDDF DDAXF XAGGF DXXAX FGXFG G” using the keywork monkeys and zebras.

The ciphertext filled into the Columnar Transposition grid. By reading off each row we get the intermediate text “GXFGAX XFDFDA FXDDDX GAAXDF GG”.

Now we need to generate the Mixed Square using keyword monkeys.

The Mixed Square with keyword monkeys.

Now, as I mentioned above. we take (x, y) to get the plain text letter. In our case GX is the location of the first letter which is 't' and so on. The plain text is “the way is clear”.

Sources: 1- https://www.youtube.com/watch?v=-j4JlGBXfFM 2- http://practicalcryptography.com/ciphers/adfgvx-cipher/ 3- http://crypto.interactive-maths.com/adfgvx-cipher.html

(D) What is Playfair?

The Playfair cipher is a digraph substitution cipher. It employs a table where letter J of the alphabet is omitted and I takes its place, and the letters are arranged in a 5×5 grid. To encode a message, one breaks it into two-letter chunks. Repeated letters in the same chunk are usually separated by an X. Example: The message, “HELLO ONE AND ALL” would become “HE LX LO ON EA ND AL LX”.

(E) What is Pigpen? The Pigpen cipher is substation cipher, it replaces letters by symbols. Its encryption process is straightforward, just replace each occurrence of a letter with the specific symbols. The decryption process is just the reverse of the encryption process. The symbols is assigned to the letter using the key “image below”, where the letter shown is replaced by the part of the image in which it is located.

Letters are represented by the part of the grid they are in.

Example: Letter 'A' = Letter 'W' = Letter 'M' =

Decryption: The decryption process is just the reverse of the encryption process, Using the same key we locate the image depicted in the cipher text, and replace it with the letter given by that part of the grid.

Source:

1- https://lobestir.files.wordpress.com/2014/05/cypher-pig-pen-lower.png

2- http://crypto.interactive-maths.com/pigpen-cipher.html

Notice that the majority of this information is from the Code book.

QUESTION 2:

Encrypt an English text of at least 80 words using the Vigenere cipher and exchange it with one of your fellow students.

Student Name: Kees deJong This is my Vigenere cipher text Keyword(pixel):

```
wmipz bg kext qp oziiffl.
x ij jcdu pccxi. f kcplreetl tmew i yenwmisc smdvpt qk myuwoqliqlr lcl
zsxbckmnpbfsy imzlydtlkj. x pxzp iel motip gzckbvyxvd xst apr qxvxp
agwgini, al mq nwr hzcb eegt xxvecmo cpi eb glc bbex jx qsrtbeic pva jtcl
qltgl michwk my dzaic iw amdrcpw pkmocewqkk lqwrx ewm pwy uqkew ezlnprb.
fr ndvzpfhqlr, t likx ed beeyz gly qdz vsfg pbpa xv pwy aiy 1 eys q oilatv
eaezbgtpbb me.
qmpx ctoxvoh,
glyc rtxwd biqi li abee 15
```

Plain Text:

```
hello my name is kotaiba.
i am from syria. i graduated with a bachelor degree in information and
communication technology. i have two ideas concerning the ssn final
project, so if you dont have partner yet we can team up together and find
third person in order to discuss everything about the ssn final project.
in conclusion, i want to thank you for your help in ssn lab 1 and i really
appreciate it.
best regards,
your class mate at seat 15
```

QUESTION 3:

Crack the encrypted text of your fellow student using the Vigenere cipher tool.

CIPHER TEXT (Vigenere):

```
npeij gcu ss zmel nvqr ka’j qarhpxidif her yekukourgk gfatgycm. xyerzzk ag
dzzx pghib flgzv htmpnj of xjl lbuzgyjwfc cuu cr gqbigq hwyzbs swy fkz
gcyvsd. m csdcex jhms qmiokm istkj, w psp’a vjqr ilk wf ajf ns zigk jc
yepf ncdhu. wicnedsp ha fwpcr gt uvds bevavfzw hvi hti fltfktvpfb fsqsj.
ozcyhp, zax’u vw kavfz ysdi cuu amcdl zh imns ss qrqbxv ur c mvk eievere.
m ypcz vyua bsqt qu kmbmpn rbp xtf ecf xq orjq wrlczuri lifavu ivqmyul
kvmx yvlzp wwjb tav vov rqgtfghusp afcxw.
```

DECIPHER TEXT: this is the plain text for your Kees cipher text using key “chrome”:

```
linux can be nice when it’s configured and maintained properly. luckily we
will learn these things at the university and of course during our own
career. i almost have eighty words, i don’t even get it why we need so
many words. probably to build up some patterns for the decryption tools.
anyway, lot’s of words here and maybe it will be enough in a few seconds.
i will just keep on typing and try not to have spelling errors because
that would suck for the decryption tools.
```

QUESTION 4: Go through the previous two steps again, this time using a cipher of your own choosing. Do not tell your fellow student what cipher you used!

Kees send me me this cipher text: And this is my 'secret' cipher:

```
Yvahk pna or avpr jura vg’f pbasvtherq naq znvagnvarq cebcreyl. Yhpxvyl jr
jvyy yrnea gurfr guvatf ng gur havirefvgl naq bs pbhefr qhevat bhe bja
pnerre. V nyzbfg unir rvtugl jbeqf, V qba’g rira trg vg jul jr arrq fb
znal jbeqf. Cebonoyl gb ohvyq hc fbzr cnggreaf sbe gur qrpelcgvba gbbyf.
Naljnl, ybg’f bs jbeqf urer naq znlor vg jvyy or rabhtu va n srj frpbaqf.
V jvyy whfg xrrc ba glcvat naq gel abg gb unir fcryyvat reebef orpnhfr
gung jbhyq fhpx sbe gur qrpelcgvba gbbyf.
```

We had a deal to not use an IMPOSSIBLE encryption algorithm for example RSA. We made a deal to use one of the ciphers that we took in class.

So, it was **ROT13**. But how I knew that? to be honest, we made a deal to give each other a vague hint. so it was not hard to detect.

So the DECIPHER TEXT is:

```
Linux can be nice when it’s configured and maintained properly. Luckily we
will learn these things at the university and of course during our own
career. I almost have eighty words, I don’t even get it why we need so many
words. Probably to build up some patterns for the decryption tools. Anyway,
lot’s of words here and maybe it will be enough in a few seconds. I will
just keep on typing and try not to have spelling errors because that would
suck for the decryption tools.
```

Now, its my turn: I will use Atbash cipher:

Plain Text:

```
In this Program we focus on Open Standards, Open Software and Open Security,
hence the name OS3.
```

Cipher Text:

```
Rm gsrh Kiltizn dv ulxfh lm Lkvm Hgzmwziwh, Lkvm Hlugdziv zmw Lkvm Hvxfirgb,
svmxv gsv mznv LH3.
```