Technical University of Denmark

01410 Cryptology 1

Homework 1

Authors:

Andreas Hallberg Kjeldsen
s092638@student.dtu.dk

Morten Chabert Eskesen
s133304@student.dtu.dk

March 10, 2014

Exercise 1.1

1.1.1

We are considering the Hill cipher. We have plaintext $\mathcal{P}$, **crypto**, which map to values **[2,17,24,15,19,14]**. We also have ciphertext $\mathcal{C}$, **LSDKDH**, which map to values **[11,18,3,10,3,7]**. We have that $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$.

We wish to find the 2 × 2 key matrix K used in the encryption. To do this we first split the plaintext and ciphertext into pairs of two, this gives that **cr** is encrypted to **LS**, **yp** to **DK** and **to** to **DH**. Now we must find two pairs we can use to figure out the key. We start off with **cr** and **yp**.

First we wish to check if the plaintext message m is invertible.

$$m = \begin{bmatrix} c & r \\ y & p \end{bmatrix} (\texttt{mod}\ 26) = \begin{bmatrix} 2 & 17 \\ 24 & 15 \end{bmatrix} (\texttt{mod}\ 26)$$

$$m^{-1} = ?$$

The plaintext message m is not invertible. We skip the plaintext **cr** and use the next pair from the plaintext. Now we have **yp** and **to**.

$$m = \begin{bmatrix} y & p \\ t & o \end{bmatrix} (\texttt{mod}\ 26) = \begin{bmatrix} 24 & 15 \\ 19 & 14 \end{bmatrix} (\texttt{mod}\ 26)$$

$$m^{-1} = \begin{bmatrix} 12 & 15 \\ 19 & 2 \end{bmatrix} (\texttt{mod}\ 26)$$

The message m is invertible. Now onto finding the key. First we define c, the ciphertext that m encrypts to.

$$c = \begin{bmatrix} 3 & 10 \\ 3 & 7 \end{bmatrix} (\texttt{mod}\ 26)$$

Now we can derive the key.

$$c = mK(\texttt{mod}\ 26)$$

$$K = m^{-1}c(\texttt{mod}\ 26) = \begin{bmatrix} 12 & 15 \\ 19 & 2 \end{bmatrix} \begin{bmatrix} 3 & 10 \\ 3 & 7 \end{bmatrix} (\texttt{mod}\ 26) = \underline{\underline{\begin{bmatrix} 3 & 17 \\ 11 & 22 \end{bmatrix}}}$$

1.1.2

With the key K obtained, we now wish to decrypt the text **`HFFP`** mapping to values **`[7,5,5,15]`**.

$$m = cK^{-1} = \begin{bmatrix} 7 & 5 \\ 5 & 15 \end{bmatrix} \begin{bmatrix} 3 & 17 \\ 11 & 22 \end{bmatrix}^{-1} (\texttt{mod}\ 26) = \begin{bmatrix} 7 & 5 \\ 5 & 15 \end{bmatrix} \begin{bmatrix} 14 & 1 \\ 19 & 9 \end{bmatrix} (\texttt{mod}\ 26) = \begin{bmatrix} 11 & 0 \\ 17 & 10 \end{bmatrix}$$

The values **`[11,0,17,10]`** maps to the text **`lark`**.

Exercise 1.2

1.2.1

We are to consider $m \times m$ matrices with entries from $\mathbb{Z}_{26}$. We know that the following holds:

$$\det(AB) = \det(A) \cdot \det(B)$$

We have an invertible $m \times m$ matrix A over $\mathbb{Z}_{26}$, where $A = A^{-1}$. We wish to prove:

$$\det(A) = \pm 1\ (\texttt{mod}\ 26)$$

We know that A is invertible, hence we can claim that A is orthogonal.

$$A^{-1} = A^T$$

We know the definition of for an inverse matrix, using identity matrix I.

$$A \cdot A^{-1}\ (\texttt{mod}\ 26) = I$$

We can now substitute A^{-1} with A^T and reduce.

$$A \cdot A^T\ (\texttt{mod}\ 26) = I$$

$$\det(A \cdot A^T\ (\texttt{mod}\ 26)) = \det(I) = 1$$
$$\det(A) \cdot \det(A^T)\ (\texttt{mod}\ 26) = 1$$

We know that the determinant of a square matrix and it's transpose are equal.

$$\det(A) \cdot \det(A)\ (\texttt{mod}\ 26) = (\det(A))^2\ (\texttt{mod}\ 26) = 1$$

We can now conclude our proof:

$$\det(A) = \pm 1\ (\texttt{mod}\ 26)$$

1.2.2

We wish to show that there are 736 2×2 matrices A over $\mathbb{Z}_{26}$ for which it holds that $A = A^{-1}$. We split the problem into two cases. We first consider the problem modulo 2 and then modulo 13.

$\mathbb{Z}_2$

A matrix modulo 2 that is the inverse of itself only has 4 types where $b = 0$:

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

In total we have 4 self-inverse matrices over $\mathbb{Z}_2$.

$\mathbb{Z}_{13}$

A matrix modulo 13 that is the inverse of itself has likewise modulo 2 those 4 types as wel where $b = 0$:

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

If $a = 0$ and $b \neq 0$ then $\frac{1}{ad-bc} = -1$ has a solution where $c = \frac{1}{b}$. Since there are 12 possible values for b where $b \neq 0$ there are 12 more types of this kind:

$$\begin{pmatrix} 0 & b \\ \frac{1}{b} & 0 \end{pmatrix}$$

If $bc \neq 0$ then we have $a^2 + bc = 1$. Therefore $1 - bc$ has to be square modulo 13. Hence we have:

$$1 - bc \in \{0, 1, 3, 4, 9, 10, 12\}$$

Since $bc \neq 0$ then:

$$bc \in \{1, 3, 4, 9, 10, 12\}$$

There are 12 invertible elements in $\mathbb{Z}_{13}$. For any choice of invertible b, there are 6 options for bc, each gives one option for c, each, in turn gives 2 options for a.

$$6 * 12 * 1 * 2 = 144$$

We isolate c in $a^2 + bc = 1$ and get that $c = \frac{1-a^2}{b}$. Therefore we have 144 types of this kind of matrix:

$$\begin{pmatrix} a & b \\ \frac{1-a^2}{b} & -a \end{pmatrix}$$

Lastly we have 12 each of these types:

$$\begin{pmatrix} 1 & 0 \\ c & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$$

But however only the two first types have to be counted, because the last two types have already been counted among the type of size 144. Which means that we have:

$$4 + 12 + 144 + 24 = 184$$

In total we have 184 self-inverse matrices over $\mathbb{Z}_{13}$.

$\mathbb{Z}_{26}$

Since $\mathbb{Z}_{26}$ is the direct product of $\mathbb{Z}_{13}$ and $\mathbb{Z}_2$ we can muiltiply the number of self-inverse matrices over these two and get the number of self-inverse matrices over $\mathbb{Z}_{26}$.

$$184 * 4 = 736$$

We have therefore shown that there are 736 2×2 matrices A over $\mathbb{Z}_{26}$ for which it holds that $A = A^{-1}$.

Exercise 1.3

1.3.1

We consider the Vigénere cryptosystem. We know the following ciphertext encrypted using the Vigénere crpytosystem.

```
PATGSJKGSPFPCTSSKHOIGSDHNBCUHVIHKSHVBKPBQLEGVFSHPLTQFLYRWS
RLYBSSRPPPPGIUOTUSHVPTZSVLNBCHCIWMIZSZKPWWZLZKXJWUCMWFCBCA
ACBKKGDBHOAPPMHVBKPBQLDXKWGPPXSZCUZHCNCVWGSOGRAWIVSTPHROFL
BHGHVLYNQIBAEEWWGYAMJFBDDBRVVLKIIWAPOMXQOSHRPBHPYBEOHLZPDI
ZKXXCCZVJZTFHOWGIKCDAXZGCMYHJFGLPATKOYSTHBCAPHTBRZKJJWQRHR
```

We wish to compute the most likely period of the key by using the index of coincidence. We do this by arranging the ciphertext in $(j \times c)$ matrices. Instead of showing all our created matrices when computing index of coincidence. We skip right ahead to the (6 x c) matrix, we found to be the likely period of key. We arrange the ciphertext in this matrix.

```
PKCONIBEPYYPOPNWKZCCKABDPZWAPBYEADKOHYZXJWAYPSPKH
AGTIBHKGLRBPTTBMPKMAGPKXXHGWHHNEMBIMRBPXZGXHATHJR
TSSGCKPVTWSPUZCIWXWADPPKSCSIRGQWJRIXPEDCTIZJTHTJ
GPSSUSBFQSSGSSHZWJFCBMBWZNOVOHIWFVWQBOICFKGFKBBW
SFKDHHQSFRRIHVCSZWCBHHQGCCGSFVBGBVAOHHZZHCCGOCRQ
JPHHVVLHLLPUVLIZLUBKOVLPUVRTLLAYDLPSPLKVODMLYAZR
```

We compute the index of coincidence for each row vector and we get the following six numbers:

$$0.065, 0.059, 0.051, 0.061, 0.071, 0.082.$$

We have computed the index of coincidence of each row in $(j \times c)$ matrix for all (likely) values of j, where $j = 1, \ldots 7$. This gives us the following:

Period	Index of coincidence
1	0.0433
2	0.047 0.044
3	0.049 0.054 0.049
4	0.052 0.036 0.044 0.043
5	0.039 0.038 0.039 0.046 0.042
6	**0.065 0.059 0.051 0.061 0.071 0.082**
7	0.033 0.038 0.035 0.041 0.043 0.04 0.041

We are therefore able to conclude that the period is most likely six.

1.3.2

We wish to find the plaintext message of the ciphertext. We arrange the ciphertext in a $6 \times c$ matrix. First we have to find the key therefore for each row we do the following:
For i:=0 to 25 do

1. shift all letters i positions backwards in the alphabet
2. compute the distribution of the resulting characters
3. compute the distance of this distribution from the distribution in a typical English text

We define the distance between two distributions as the "sum of squared differences". We therefore use this formula for calculating the distance.

$$d(i) = \sum_{\ell=1}^{25} (p_\ell - q_\ell(i))^2,$$

for i $= 0, \dots, 25$, p_ℓ for $\ell = 0, \dots, 25$ is the probability distribution of letters in English text and $q_\ell(i)$ for $\ell = 0, \dots, 25$ is the probability distribution of letters in this row when each letter is shifted i positions back in the alphabet.
We do this for each row.

First row

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$d(i)$	0.07	0.08	0.07	0.08	0.08	0.08	0.06	0.05	0.07	0.07	0.05	0.04	0.08	0.09	0.07	0.07	0.09	0.08	0.08	0.08	0.07	0.06	**0.02**	0.06	0.07	0.08

It follows that the computed distances are lowest for $i = 22$, which corresponds to the key character ”W”.

Second row

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$d(i)$	0.06	0.07	0.07	0.06	0.06	0.07	0.06	0.07	0.05	0.07	0.08	0.08	0.07	0.06	0.07	0.04	0.08	0.09	0.08	**0.02**	0.07	0.08	0.07	0.06	0.07	0.07

It follows that the computed distances are lowest for $i = 19$, which corresponds to the key character ”T”.

Third row

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$d(i)$	0.06	0.05	0.05	0.07	0.04	0.05	0.06	0.07	0.06	0.07	0.07	0.04	0.07	0.08	0.05	**0.01**	0.06	0.06	0.05	0.07	0.08	0.06	0.05	0.07	0.06	0.06

It follows that the computed distances are lowest for $i = 15$, which corresponds to the key character ”P”.

Fourth row

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$d(i)$	0.08	0.04	0.07	0.07	0.07	0.06	0.08	0.08	0.06	0.08	0.06	0.08	0.08	0.07	**0.02**	0.08	0.08	0.08	0.05	0.08	0.07	0.08	0.08	0.06	0.07	0.06

It follows that the computed distances are lowest for $i = 14$, which corresponds to the key character ”O”.

```
thesecondbrigadewaspreparingtomovetofrance
ingreatsecrecyhedecideditwasunsafetotakeher
intobattlesowhiledrivingthroughlondonontheway
tofrancehevisitedlondonzooandaskedthemtocare
forthecubuntilhisreturnwhichheoptimistically
anticipatedwouldbenolongerthantwoweeksof
coursethewarwasnottoendsoquickly
```

Figure 1: The plaintext message

Fifth row

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$d(i)$	0.08	0.09	0.07	0.05	0.08	0.1	0.09	0.08	0.09	0.08	0.08	0.09	0.09	0.07	**0.02**	0.07	0.09	0.08	0.08	0.09	0.08	0.07	0.1	0.09	0.06	0.05

It follows that the computed distances are lowest for $i = 14$, which corresponds to the key character ”O”.

Sixth row

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$d(i)$	0.10	0.10	0.10	0.06	0.08	0.12	0.10	**0.02**	0.08	0.10	0.10	0.07	0.11	0.09	0.10	0.10	0.10	0.08	0.08	0.09	0.09	0.09	0.09	0.08	0.09	0.10

It follows that the computed distances are lowest for $i = 7$, which corresponds to the key character ”H”.

Finding the plaintext message

We have found the key which is ”WTPOOH”. We follow the decryption for the Vigénere crpytosystem which is:

$$d_k(y_1, \ldots, y_n) = (y_1 - k_1, \ldots, y_n - k_n)$$

The figures above describe the plaintext message.

the second brigade was preparing to move to france
in great secrecy he decided it was unsafe to take her
into battle so while driving through london on the way
to france he visited london zoo and asked them to care
for the cub until his return which he optimistically
anticipated would be no longer than two weeks of
course the war was not to end so quickly

Figure 2: The plaintext message with space added for readability