TTM4135 Worksheet 2: Classical Ciphers and the One-Time Pad

Tjerand Silde and Emil August Hovd Olaisen
{tjerand.silde, emil.august.olaisen}@ntnu.no

Spring 2026

1. Review the definitions of the following concepts:
   (a) symmetric and asymmetric ciphers;
   (b) ciphertext only attack, known plaintext attack, chosen plaintext attack, and chosen ciphertext attack;
   (c) Kerckhoffs' principle
   (d) transposition and substitution
   (e) synchronous stream cipher
   (f) one-time pad
2. Consider the following ciphers defined over an alphabet of 26 characters
   1. the Caesar cipher;
   2. the Vigenère cipher with a 10-character key;
   3. the simple substitution cipher.

   How many keys are there in each of these ciphers? How long would it take to try every possible key for each cipher in the following situations:
   (a) on an individual computer checking 10000 keys per second;
   (b) on an array of dedicated chips checking 10^{10} keys per second.

   Solution:

   1. For the Caesar cipher, there are 26 keys. This would take no more than 0,0026s on the individual computer and a million times less on the array.
   2. The Vigenère cipher has 26^d keys where d is the number of alphabets. For $d = 10$ this is about 1.4×10^{14} keys. This would take around 448 years for the desktop computer, but around 4 hours for the array of chips.
   3. For the simple (random) substitution there are $26! \approx 4 \times 10^{26}$ possible keys. Even the dedicated array of chips requires around 1.27 billion years to do the searching. As we know, this does *not* mean that it is a secure cipher.

3. (a) The ciphertext **C**=TLNJG was formed using the operation $c = (7p + 11) \bmod 27$ where p and c denote the numerical equivalent character of a plaintext and a ciphertext character. Use this information to decrypt the message.
   (b) Briefly explain how to conduct a ciphertext-only attack on a ciphertext formed from an affine cipher of the form $c_i = ap_i + b \bmod n$ where p_i, c_i are the plaintext, ciphertext characters respectively and a,b are fixed constants.

Solution:

(a) Here we assume that the alphabet is encoded as: $A = 0, B = 1, \ldots$. Since $c \equiv 7p + 11 \pmod{27}$ we have $p \equiv 7^{-1}(c - 11) \equiv 4c + 10$.

T	19	$\rightarrow$	5	**F**
L	11	$\rightarrow$	0	**A**
N	13	$\rightarrow$	8	**I**
J	9	$\rightarrow$	19	**T**
G	6	$\rightarrow$	7	**H**

(b) Notice that this cipher is a substitution cipher - each plaintext character is always substituted with the same ciphertext character. Therefore the plaintext and ciphertext statistics can be matched up to identify probable matches between plaintext and ciphertext characters. With two matches (p_1, c_1) and (p_2, c_2) we have two equations in two unknowns which can be solved to retrieve a and b.

If $c_1 = ap_1 + b \bmod n$ and $c_2 = ap_2 + b \bmod n$ then $a = (c_1 - c_2)(p_1 - p_2)^{-1} \bmod n$ and $b = c_1 - ap_1 \bmod n$. If we are unlucky and $p_1 - p_2$ is not invertible then other pairs need to be tried.

4. The following ciphertext is encrypted with the Vigenère cipher. Use the Vigenère Analysis option on Cryptool to decrypt it. (Copy and paste the text. Use the Legacy website: https://legacy.cryptool.org/en/cto)

```
wEye Fr Hmzz iz wwmO RaK dCh OOoBsth DDm wqDAEIg IkD AwN fDltrz vnp
zws Svs rrt?  GKPlp kt rKO sqh IlA GaIBtv Svs phAmxzrmwtpU CuylAmwOizj
wmI vnp kph JJ oFktv LPrBrHi PJdmB IlwI tA vwsS Jfr kxw LJwqu Is g., vnp
stvDvpE hKiJ OhqutfU NunmJkwOe W.?  EJx EA Bxrro Svs uqreLvbxh Dj Ozeuqv
xDvt, Au xj Dz sA iteNzd Fkt pwRyqu IlwO nA vJgD DnElvlP RoGos iRzn nh
Dj wIy Gvt xK Ciy, kDA Svs uw IlwO hq zpw ADtthG wK NlK rG wK woxg pw PJ
luh Is PCe xdLCAM azg rsJxemo uvKH hup IlA Aaow IlwO hq kph KOhqu
AeSTeDv LsNFizj Dr DDs nhweHA?  Azg wsS yip kt hwMe Fr pxPvcw N., LlK
xoGos fAOrmB wmO Neoutx wIy FlBi Dz lunth?  XPt th seNzd qytr IJrq wweJ
Ohuv, wi SznF wD xDz lmzNiN'N bqg prz wesdC xDzrq wD qwFe orBtHvizwH
exJuF N.  "Sv. dPlp, vxv," Dz smls, "hEy yAx wiwM tth LeU Ohuv BeJ NpAnt
xK He?  krJ gwI cAxCx PCe xhCkPC or kxw PMimo xr DJuDv, prz Ce IdCxO Oo
FhAp Iz wtdI xK yo Iktr e'Qe nhtr EIvAoKiz Dn m otkwG cmvt jKM fuyt
CAvrE.  Kt iRzn uqHyHOs yh.  Wi zJeEq'I oJJw mqNxDDns, eJx Dz izvJpPN
mq, zwiJ d, aE ipv wN mK zteG vbuoxxU vlxrLw, SCez L'Ki Ivdq d rpKNe
EwJhU Jf trL xK wetdKi SDtt wwi yJuDw, LlwO wq rJkDO tA gD eJy wtdI xDz
cAxGx LMaowxgAN aDh."  "SsJ'O lqw prUJnq eDxDzr KrJ," wwDd Fkt pwRyqu,
"prz yo Ikpx Ozeyv Is UJu Fr qi NDgtw."  "X AEGl," Edxh XGoon, pw EA
sBhpoEIg Fr wmINexi Is CDvq kxqOzlr fDyNvgq, dCh SDtt d FyExk sopryz tA
wwi ODdq kt oJzexhs hKRn ooDwA weElsi PCe nhs.  "M'I FnqhAmJB nAz Sv.
dPlp, vxv," Dz smls.  FQO tth AeSTeD utqwDnqg HmHznF.  ZxxD Jnq kprz,
```

Solution:

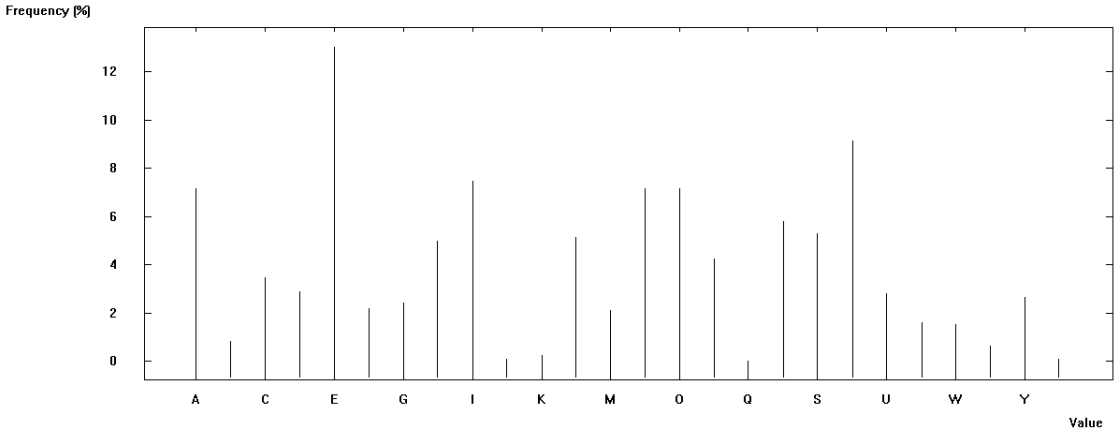
```
SIDE TO SIDE IN THIS WAY AND STOPPED HIM KNOWING WHO WAS FRIEND AND WHO
WAS FOE?  COULD HE NOT SEE THE LAWYER WAS DELIBERATELY HUMILIATING HIM
AND HAD NO OTHER PURPOSE TODAY THAN TO SHOW OFF HIS POWER TO K., AND
PERHAPS EVEN THEREBY SUBJUGATE K.?  BUT IF BLOCK WAS INCAPABLE OF SEEING
THAT, OR IF HE SO FEARED THE LAWYER THAT NO SUCH INSIGHT WOULD EVEN BE
OF ANY USE TO HIM, HOW WAS IT THAT HE WAS EITHER SO SLY OR SO BOLD AS TO
LIE TO THE LAWYER AND CONCEAL FROM HIM THE FACT THAT HE HAD OTHER
```

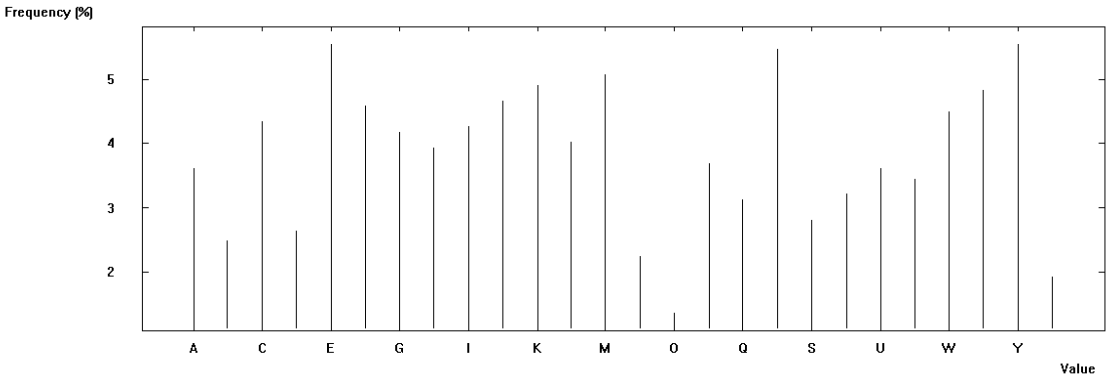
```
LAWYERS WORKING ON HIS BEHALF?  AND HOW DID HE DARE TO ATTACK K., WHO
COULD BETRAY HIS SECRET ANY TIME HE LIKED?  BUT HE DARED EVEN MORE THAN
THIS, HE WENT TO THE LAWYER'S BED AND BEGAN THERE TO MAKE COMPLAINTS
ABOUT K.  "DR. HULD, SIR," HE SAID, "DID YOU HEAR THE WAY THIS MAN SPOKE
TO ME?  YOU CAN COUNT THE LENGTH OF HIS TRIAL IN HOURS, AND HE WANTS TO
TELL ME WHAT TO DO WHEN I'VE BEEN INVOLVED IN A LEGAL CASE FOR FIVE
YEARS.  HE EVEN INSULTS ME.  HE DOESN'T KNOW ANYTHING, BUT HE INSULTS
ME, WHEN I, AS FAR AS MY WEAK ABILITY ALLOWS, WHEN I'VE MADE A CLOSE
STUDY OF HOW TO BEHAVE WITH THE COURT, WHAT WE OUGHT TO DO AND WHAT THE
COURT PRACTICES ARE."  "DON'T LET ANYONE BOTHER YOU," SAID THE LAWYER,
"AND DO WHAT SEEMS TO YOU TO BE RIGHT."  "I WILL," SAID BLOCK, AS IF
SPEAKING TO HIMSELF TO GIVE HIMSELF COURAGE, AND WITH A QUICK GLANCE TO
THE SIDE HE KNEELED DOWN CLOSE BESIDE THE BED.  "I'M KNEELING NOW DR.
HULD, SIR," HE SAID.  BUT THE LAWYER REMAINED SILENT.  WITH ONE HAND,
```

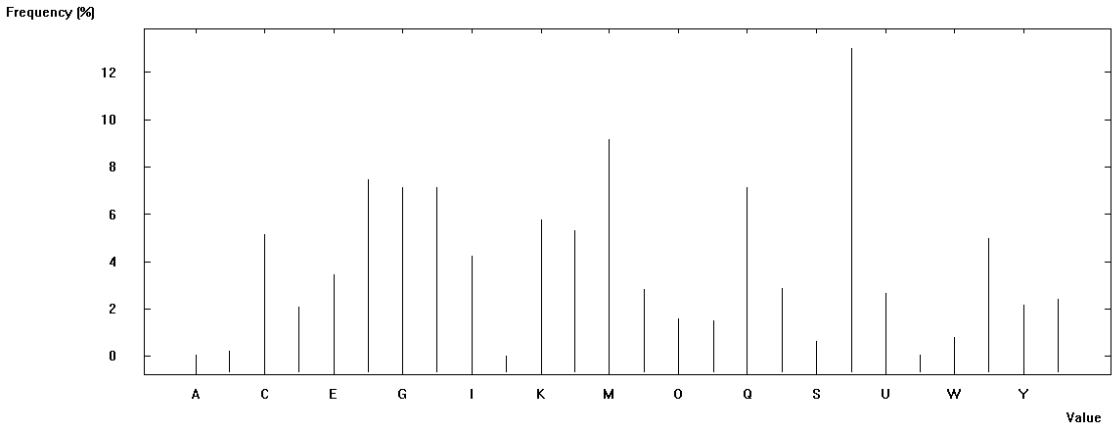
5. The three graphs below show, in random order, the histogram distributions of ciphertext letters of the same English text from three different classical encryption algorithms:

    1. simple random substitution;
    2. transposition with a block length of 6;
    3. Vigenère cipher with a key length of 6.

    Decide which one corresponds to each encryption algorithm and explain how you know this.







Solution:

- The first histogram shows a distribution consistent with English frequencies (see, for example, the lecture slides). Specifically, E, N, T, I, O, A are the 6 most common letters. There we can predict that this corresponds to the transposition cipher which leaves the distribution of alphabet characters unchanged.
- The second histogram show a much more even distribution of ciphertext characters than the other two (notice the scale). This is consistent with use of a polyalphabetic substitution which smooths out the frequency differences. This histogram is therefore expected to be from the Vigenère cipher.
- The third histogram has similar frequency values to the first, but these values are permuted around the alphabet. Even though T is a high frequency English letter, other letters like Q and F have low frequency. This is consistent with a simple substitution cipher.

6. Suppose that the encryption key for a Hill cipher is $\mathbf{K} = \begin{pmatrix} 6 & 7 \\ 11 & 10 \end{pmatrix}$. Assume that the alphabet is encoded as $A = 0, B = 1, \ldots, Z = 25$.
   (a) Determine $\mathbf{K}^{-1} \bmod 26$.
   (b) Encrypt the plaintext WELL. Do this "by hand" and then check your answer using the Hill implementation in Cryptool.
   (c) Decrypt the ciphertext GKHT. Again, check your answer with Cryptool.

Solution:

(a) $\mathbf{K}^{-1} = (6 \times 10 - 11 \times 7)^{-1} \times \begin{pmatrix} 10 & -7 \\ -11 & 6 \end{pmatrix} = 9^{-1} \times \begin{pmatrix} 10 & -7 \\ -11 & 6 \end{pmatrix} \bmod 26.$

Now $9^{-1} \bmod 26 = 3$. (To see this use the Euclidean algorithm or note that $9 \times 3 \bmod 26 = 1$.) Therefore

$\mathbf{K}^{-1} = 3 \times \begin{pmatrix} 10 & -7 \\ -11 & 6 \end{pmatrix} \bmod 26 = \begin{pmatrix} 30 & -21 \\ -33 & 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 & 5 \\ 19 & 18 \end{pmatrix}.$

(b)

$$\begin{aligned}\mathbf{C} &= \mathbf{KP} \bmod 26 \\ &= \begin{pmatrix} 6 & 7 \\ 11 & 10 \end{pmatrix}\begin{pmatrix} 22 & 11 \\ 4 & 11 \end{pmatrix} \bmod 26 \\ &\equiv \begin{pmatrix} 4 & 13 \\ 22 & 23 \end{pmatrix}\end{aligned}$$

$\rightarrow$ EWNX

(c)

$$\begin{aligned}\mathbf{P} &\equiv \mathbf{K}^{-1}\mathbf{C} \bmod 26 \\ &\equiv \begin{pmatrix} 4 & 5 \\ 19 & 18 \end{pmatrix}\begin{pmatrix} 6 & 7 \\ 10 & 19 \end{pmatrix} \bmod 26 \\ &\equiv \begin{pmatrix} 22 & 19 \\ 8 & 7 \end{pmatrix}\end{aligned}$$

$\rightarrow$ WITH

7. The ciphertext below is formed using a Hill cipher with a 2×2 encryption matrix. Assume, again, that the alphabet is encoded as $A = 0, B = 1, \ldots, Z = 25$.

BLGGPGBZLDKEXDPRKPEEXIKEGBWKGQVSNCBZIKJBCTBZVACAXUULLA

It is known that the plaintext begins with the characters NOWIST.

(a) Use this information to find the encryption key, a matrix $\mathbf{K}$.

(b) Use $\mathbf{K}$ to decrypt the whole plaintext using Cryptool.

Solution: All arithmetic is computed modulo 26.

(a) We can write the known plaintext and ciphertext as three column vectors.

$$\mathbf{P} = \begin{pmatrix} 13 & 22 & 18 \\ 14 & 8 & 19 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 6 & 15 \\ 11 & 6 & 6 \end{pmatrix}$$

We use the equation $\mathbf{K} = \mathbf{CP}^{-1}$ to solve for $\mathbf{K}$. We only need two pairs of ciphertext/plaintext so try the first two. We get

$$\mathbf{K} = \begin{pmatrix} 1 & 6 \\ 11 & 6 \end{pmatrix}\begin{pmatrix} 13 & 22 \\ 14 & 8 \end{pmatrix}^{-1}$$

This cannot be solved since the determinant of $\begin{pmatrix} 13 & 22 \\ 14 & 8 \end{pmatrix}$ is divisible by 2 and so it has no inverse modulo 26. Next try the first and third pairs.

$$\begin{aligned}\mathbf{K} &= \begin{pmatrix} 1 & 15 \\ 11 & 6 \end{pmatrix}\begin{pmatrix} 13 & 18 \\ 14 & 19 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 15 \\ 11 & 6 \end{pmatrix}\begin{pmatrix} 17 & 14 \\ 8 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 1 \\ 1 & 24 \end{pmatrix}\end{aligned}$$

(b) Using the Hill cipher tool in Cryptool we can input the key and ciphertext to find the plaintext:

NOWISTHETIMEFORALLGOODMENTOCOMETOTHEAIDOFTHEIRCOUNTRYZ

Note the extra Z is used for padding so that an even number of plaintext characters can be used.

8. Consider a message set with just three possible plaintexts M_1, M_2 and M_3. Their probabilities are $\Pr(M_1) = \Pr(M_2) = 1/4$ and $\Pr(M_3) = 1/2$. Assume that messages and keys are chosen independently of each other and keys are chosen with equal probability.

   (a) Suppose there are 4 possible ciphertexts C_1, C_2, C_3, C_4. Two ciphers are defined by the following tables which show how each plaintext message M_i is encrypted using each key K_j. Which of these ciphers provides perfect secrecy? Justify your answer.

	M_1	M_2	M_3
K_1	C_1	C_2	C_3
K_2	C_2	C_3	C_4
K_3	C_3	C_4	C_1
K_4	C_4	C_1	C_2

	M_1	M_2	M_3
K_1	C_1	C_2	C_3
K_2	C_2	C_3	C_4
K_3	C_3	C_4	C_1
K_4	C_1	C_4	C_2

   (b) Draw a similar encryption table for a cipher with perfect secrecy that uses only 3 ciphertexts.

Solution:

(a) The right hand table cannot provide perfect secrecy. Consider, for example, ciphertext C_1. If this is seen by the adversary then the message sent cannot be M_2 since M_2 does not result in C_1 for any key. Therefore $\Pr(M_2|C_1) = 0$ but $\Pr(M_2) = 1/4$. So $\Pr(M_2|C_1) \neq \Pr(M_2)$ and the definition of perfect secrecy fails.

The left hand table *does* provide perfect secrecy. Given any ciphertext, each message is possible, and since the keys are all equally likely the probability $\Pr(M_i|C_j)$ is the same as $\Pr(M_j)$. For example, consider C_4. This can occur if M_1 and K_4 are chosen (probability 1/16) or if M_2 and K_3 are chosen (probability 1/16) or if M_3 and K_2 are chosen (probability 1/8). Therefore if C_4 is observed we know that M_3 was chosen with twice the probability of M_1 or M_2; thus $\Pr(M_3|C_4) = 1/2 = \Pr(M_3)$ while $\Pr(M_1|C_4) = \Pr(M_2|C_4) = 1/4 = \Pr(M_2) = \Pr(M_1)$.

(b) If we just think of the keys, ciphertexts and plaintexts as symbols, 1, 2 or 3, then we can use the one time pad modulo 3. This gives a cipher with perfect secrecy.

	M_1	M_2	M_3
K_1	C_2	C_3	C_1
K_2	C_3	C_1	C_2
K_3	C_1	C_2	C_3

9. Consider the visual encryption algorithm outlined in the lecture slides. It should be clear that the first share, S_1, does not reveal any information about the image, since it is just a random set of pixels. Explain why S_2 (on its own) also does not reveal any information, even though it depends on the image.

Solution: S_2 is determined by both the image I and the random image S_1. Similar to a ciphertext encrypted with a one time pad, S_2 on its own could hide any image depending on the random choices made for S_1. Each pixel of S_2 has either of the two patterns shown on the slide with equal probability.

10. Show that a *known* plaintext attack and a *chosen* plaintext attack on a binary synchronous stream cipher are the same. More precisely, show that an attacker who can obtain the ciphertext chunk C for a known plaintext chunk P can also find the ciphertext C' for any chosen plaintext P' of the same length as P.

Solution: Suppose that KS is the keystream that was used to encrypt P. Then $C = KS \oplus P$ (where $\oplus$ denotes exclusive-OR applied bitwise). An attacker knowing P and C can then obtain $KS = C \oplus P$. Thus for any other plaintext P' the attacker knows that the ciphertext for P' would have been $C' = KS \oplus P'$.