NTNU Department of Information Security and Communication Technology

TTM4135 Applied Cryptography and Network Security
Semester Spring, 2023

Worksheet 2: Classical ciphers and the one time pad

QUESTION 1

Review the definitions of the following concepts. They are things that you would be expected to know in the final exam.

(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

QUESTION 2

Consider the following ciphers defined over an alphabet of 26 characters (excluding the space)

- the Caesar cipher;
- the Vigenère cipher with a 10-character key;
- 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 10,000 keys per second;

(b) on an array of dedicated chips checking 10^{10} keys per second.

QUESTION 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.

cont/...

QUESTION 4

The following ciphertext is encrypted with the Vigenère cipher. Use Cryptool Online to decrypt it. (Copy it from the PDF and paste it into Cryptool.)

```
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,
```

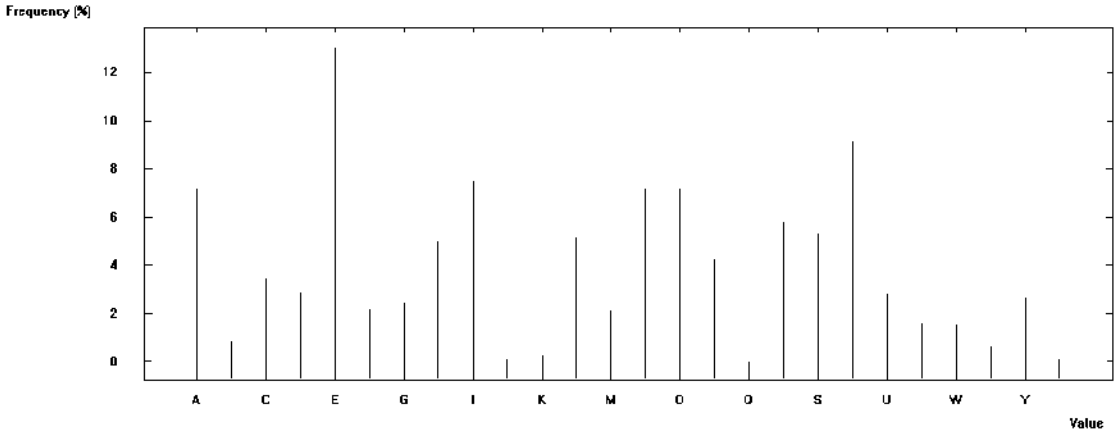
QUESTION 5

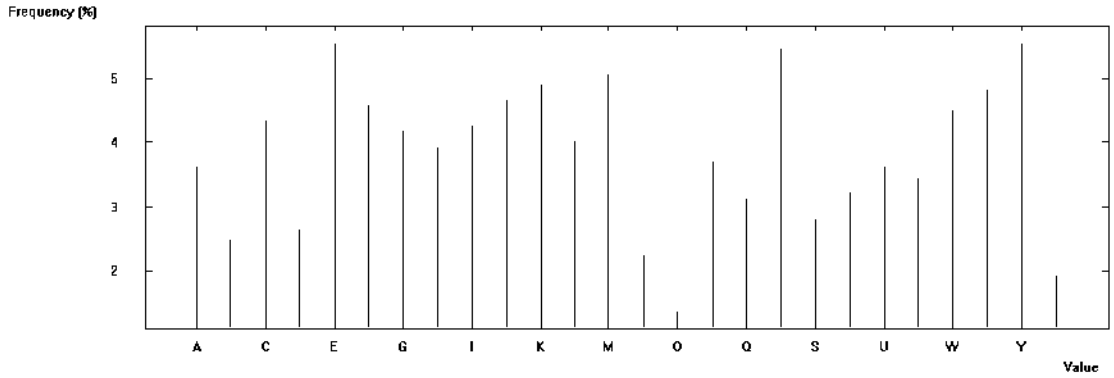
The three graphs below show, in random order, the histogram distributions of ciphertext letters of the same English text from three different classical encryption algorithms:

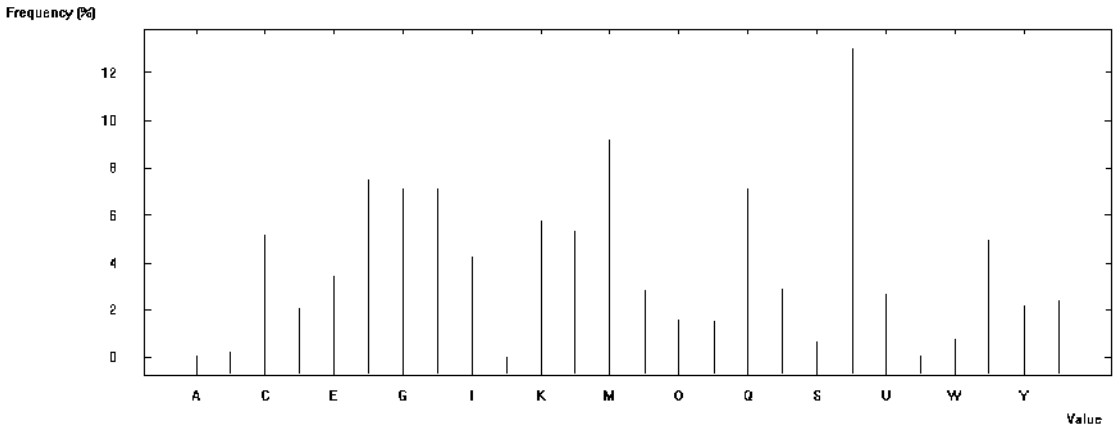
- simple random substitution;
- transposition with a block length of 6;
- Vigenère cipher with a key length of 6.

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

cont/...







QUESTION 6

Suppose that the encryption key for a Hill cipher is $K = \begin{pmatrix} 6 & 7 \\ 11 & 10 \end{pmatrix}$. Assume that the alphabet is encoded as $A = 0, B = 1, \ldots, Z = 25$.

(a) Determine $K^{-1} \bmod 26$.

(b) Encrypt the plaintext WELL. Do this "by hand" and then check your answer using the Hill implementation in Cryptool Online.

(c) Decrypt the ciphertext GKHT. Again, check your answer with Cryptool Online.

cont/...

QUESTION 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 K.

(b) Use K to decrypt the whole plaintext using Cryptool Online.

QUESTION 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.

QUESTION 9

Consider the visual encryption algorithm outlined in the slides 24–26 of Lecture 4. 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.

QUESTION 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.