17.02.2020

BAHCESEHIR UNIVERSITY
CMP5121 – NETWORK SECURITY AND CRYPTOGRAPHY

HOMEWORK #1

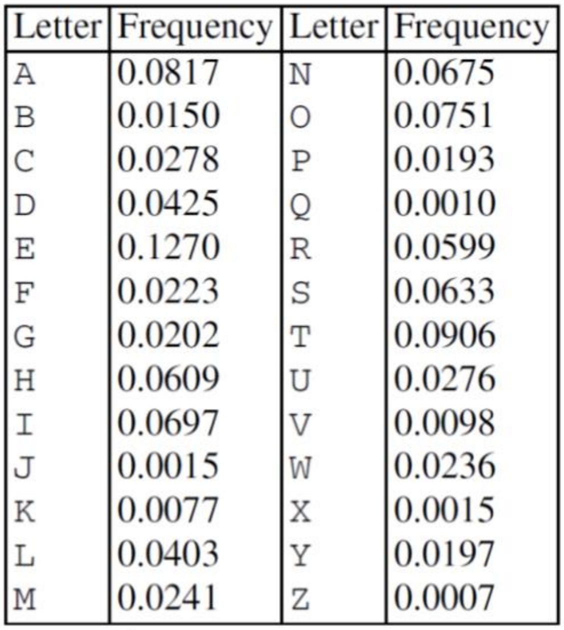
1. **The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key.**

```
lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx
irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx
ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi iwokwxwvmkvr mkd ijyr
ynib urymwk nkrashmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr
fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx
rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w
dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj
djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w jxxru
yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb
```

a) **Compute the relative frequency of all letters** A...Z **in the ciphertext. You may want to use a tool such as the open-source program CrypTool for this task. However, a paper and pencil approach is also still doable.**

b) **Decrypt the ciphertext with the help of the relative letter frequency of the English language (see Table 1). Note that the text is relatively short and that the letter frequencies in it might not perfectly align with that of general English language from the table.**

Table 1. Relative letter frequencies of the English language



Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

17.02.2020

2. **This problem deals with the affine cipher with the key parameters $a = 7, b = 22$. Decrypt the text below:**

   ```
   Falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj
   ```

3. **We will now analyze a pseudorandom number sequence generated by a LFSR characterized by $(p_2 = 1, p_1 = 0, p_0 = 1)$.**

   a) What is the sequence generated from the initialization vector$(s_2 = 1, s_1 = 0, s_0 = 0)$?
   b) What is the sequence generated from the initialization vector$(s_2 = 0, s_1 = 1, s_0 = 1)$?
   c) How are the two sequences related?

4. **Compute the first two output bytes of the LFSR of degree 8 and the feedback polynomial $x^8 + x^4 + x^2 + x + 1$ where the initialization vector has the value FF in hexadecimal notation.**