Homework 1
Due: 23:59, Wednesday, 02/14/2018

1. (30 points.) The following cipher-texts have been obtained using the substitution cipher. Decrypt the ciphertext without knowledge of the key. Your solution should contain a detailed explanation as to how you arrived at the solution.

Bigram Frequency in the English language can be found here:
http://en.wikipedia.org/wiki/Bigram

Trigram Frequency in the English language can be found here:
http://en.wikipedia.org/wiki/Trigram

Here is the ciphertext for the substitution cipher:

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

Remarks:
1. 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 (Cryptool — Educational Tool for Cryptography and Cryptanalysis. https://www.cryptool.org/.) for this task. However, a paper and pencil approach is also still doable.
2. Decrypt the ciphertext with the help of the relative letter frequency of the English language. 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.

2. Compute the values of x without a calculator:
(1) (10 points.) 6/5 mod 7
(2) (10 points.) $x = 3^{20} \bmod 13$
(3) (10 points.) $7^x = 11 \bmod 13$

3. (10 points.) What is the multiplicative inverse of 5 in Z_{11} and Z_{12}?

4. Now, we want to extend the affine cipher from Sec. 1.4.4 of textbook such that we can encrypt and decrypt messages written with the full German alphabet. The German alphabet consists of the English one together with the three umlauts, Ä, Ö, Ü, and the (even stranger) "double s" character ß. We use the following mapping from letters to integers:

A ↔ 0	B↔ 1	C↔ 2	D↔ 3	E↔ 4	F↔5
G ↔ 6	H↔ 7	I↔ 8	J↔ 9	K↔10	L↔11
M ↔12	N↔13	O ↔14	P↔ 15	Q ↔16	R↔17
S ↔18	T ↔19	U ↔ 20	V ↔ 21	W ↔ 22	X ↔23
Y ↔ 24	Z ↔ 25	Ä ↔ 26	Ö ↔ 27	Ü ↔ 28	ß ↔ 29

(1) (10 points.) What are the encryption and decryption equations for the affine cipher?
(2) (10 points.) How large is the key space of the affine cipher for this alphabet?
(3) (10 points.) The following ciphertext was encrypted using the key (a = 17 and b = 1). What is the corresponding plaintext?

Ä U ß W ß