CSC6223 Privacy- Assignment 1

Deadline Oct 5, 2018

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

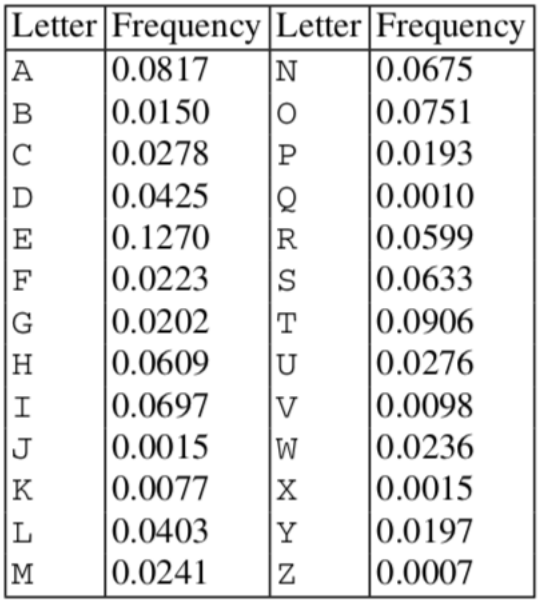
   lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt

   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 (Cryptool-Educational Tool for Cryptography and Cryptanalysis. https://www.cryptool.org/.) 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 the following table). 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.

   c) Who wrote the text?



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

2. As we learned in this chapter, modular arithmetic is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters.
   Let's start with an easy one: Compute the result without a calculator.
   a) $15 \cdot 29 \bmod 13$
   b) $2 \cdot 29 \bmod 13$
   c) $2 \cdot 3 \bmod 13$
   d) $-11 \cdot 3 \bmod 13$
   The results should be given in the range from 0,1,..., modulus-1. Briefly describe the relation between the different parts of the problem.

3. In a company, all files which are sent on the network are automatically encrypted by using AES-128 in CBC mode. A fixed key is used, and the IV is changed once per day. The network encryption is file-based, so that the IV is used at the beginning of every file.
   You managed to spy out the fixed AES-128 key, but do not know the recent IV. Today, you were able to eavesdrop two different files, one with unidentified content and one which is known to be an automatically generated temporary file and only contains the value 0xFF. Briefly describe how it is possible to obtain the unknown initialization vector and how you are able to determine the content of the unknown file.

4. With the Euclidean algorithm we finally have an efficient algorithm for finding the multiplicative inverse in Z_m that is much better than exhaustive search. Find the inverses in Z_m of the following elements a modulo m:
   1) $a = 7$, $m = 26$ (affine cipher)
   2) $a = 19$, $m = 999$
   Note that the inverses must again be elements in Z_m and that you can easily verify your answers.

5. Verify that Euler's Theorem holds in Z_m, $m = 6,9$, for all elements a for which $\gcd(a,m) = 1$. Also verify that the theorem does not hold for elements a for which $\gcd(a, m) \neq 1$.

6. Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA.
   a) Which of the parameters $e_1 = 32$, $e_2 = 49$ is a valid RSA exponent? Justify your choice.
   b) Compute the corresponding private key $K_{pr} = (p,q,d)$. Use the extended Euclidean algorithm for the inversion and point out every calculation step.

7. Encrypt the following messages with the Elgamal scheme ($p = 467$ and $\alpha = 2$):
   1. $k_{pr}=d=105$, $i=213$, $x=33$
   2. $k_{pr}=d=105$, $i=123$, $x=33$
   3. $k_{pr}=d=300$, $i=45$, $x=248$
   4. $k_{pr}=d=300$, $i=47$, $x=248$
   Now decrypt every ciphertext and show all steps.