Homework 1

1 Caesar Ciphers

1. Encrypt the message

   For duty, duty must be done;
   the rule applies to everyone.

   using a Caesar cipher with a shift of six letters. (Dont worry about encrypting the punctuation.)

2. The message

   ESTYRD LCP DPWOZX LD ESPJ DPPX.

   is a ciphertextencrypted using a Caesar cipher (the shift amount is not provided). What is the plaintext message?

3. Can you find two English words other than sleep and bunny, with at least four letters, that encrypt to each other under a Caesar cipher? What are the longest such words you can find?

4. Alice sends Bob a ciphertext encrypted using a Caesar cipher. Bob knows the shift amount, but being a beginner in cryptography at this stage, he accidentally encrypts it rather than decrypting it. Fortunately, by doing so, he still recovers the original plaintext. What was the shift amount?

6 Suppose Alice starts with a plaintext message and encrypts it using a Caesar cipher with a shift of k letters. Since she is also just learning about cryptography at the moment, she explores what happens when she encrypts the encrypted ciphertext, using the same shift of k. She does this repeatedly, and eventually she finds that she has decrypted the message. In terms of k, how many times did Alice have to encrypt the message before it became decrypted?(You may assume that the message is in English this time, so that the alphabet has 26 letters.)

2 Substitution Ciphers

1. One issue with substitution ciphers is the difficulty of remembering the key. There is a version of the substitution cipher that uses a key word that makes it easier to remember. To set this up, pick a key word that has no repeated letters (or else delete the repeated letters). Then, append to the key word all the unused letters in the alphabet, starting from the last letter in the keyword. This is a permutation of the letters in the alphabet,

and it serves as the key. For example,if the keyword is LIME, then the full key would be LIMEFGHJKNOPQRSTUVWXYZABCD. That means that we encrypt a as L, b as I, and so forth. The message

VOQDK MABJJ DZAXC ABAEE YCEVC OGDZH RGAJR
UQDKZ KHJOV GHJRG CAJCJ UCKBV LCGHC

was encrypted in this way using the key word APRICOT. What is the plaintext message?

2. What are the advantages and disadvantages of using a permutation as in problem 1 over an arbitrary permutation?

3. The message

   WBJGW RBGRC BRKHW RJKCK RZZDR CDZRW BJLGV
   TNTPT JKCIR LBERH JKCCE IPRMR HPCBR JCARK
   VWBUK VTKBC CBRRM RHYBR NIRSC HRILK WBDCR
   KHPWK JKVRR OTGKC DDCJW KR

   is a ciphertext encrypted using the mechanism in problem 1. What is the plaintext message?

4. The message

   IAOQ UQ G FQOQB FWKI QKWVIM GKJ G LVFPBVU
   WK CMAPM EW RFGPQ AE GKJ A NMGFF UWOQ EMQ
   CWBFJ

   is a ciphertext encrypted using a substitution cipher. What is the plaintext message?

5. The message

   NBPFR KISOQ NFRDB FKJFD XNOIN OJXIX NZXSI DJXIJ NYENO ISDSA SOFBY REJRK IKSKI PFRAR DJZIJ RUSEE JXIZI KADFB JXIJK SODYI OGIOJ SEJIK ADSOG UESOJ JXIAI VKPWX IKIPF RARDJ ENIRU FOJXI GSNDN IDSOG GNDYF RKDIN OOFVI EUXKS DIDFB PFRKY FAUEN YSJIG DJSJI FBANO GJXIA ISONO ZGFID OJASJ JIKNB NJDFO EPNGE IYXSJ JIKFB SJKSO DYIOG IOJSE LNOGS OGIVK PFOIW NEEDS PSDPF RWSEL PFRKA PDJNY WSPNB JXNDP FROZA SOIQU KIDDI DXNAD IEBNO JIKAD JFFGI IUBFK AIWXP WXSJS VIKPD NOZRE SKEPG IIUPF ROZAS OJXND GIIUP FROZA SOARD JCICI IEFMR IOJNO UKSND IFBJX IVIKP GREEF EGGSP DWXNY XXSVI EFOZD NOYIU SDDIG SWSPS OGYFO VNOYI IANBP FRYSO JXSJJ XIKIN ZOFBZ FFGMR IIOSO OIWSD YREJR KIDUS EANID JGSPF BYFRK DIPFR WNEEU FFXUF FXWXS JIVIK DBKID XSOGO IWSOG GIYES KINJD YKRGI SOGAI SOBFK SKJDJ FUUIG DXFKJ NOJXI YREJN VSJIG YFRKJ FBJXI IAUKI DDHFD IUXNO ISOGI VKPFO IWNEE DSPSD PFRWS ELPFR KAPDJ NYWSP NBJXS JDOFJ ZFFGI OFRZX BFKXN AWXNY XNDZF FGIOF RZXBF KAIWX PWXSJ SVIKP YREJN VSJIG LNOGF BPFRJ XJXND LNOGF BPFRJ XARDJ CIJXI OSDIO

JNAIO JSEUS DDNFO FBSVI ZIJSC EIBSD XNFOA RDJIQ YNJIP FRKES OZRNG DUEII OSOSJ JSYXA IOJSE SUESJ FBFKS CSDXB REPFR OZUFJ SJFFK SOFJJ FFBKI OYXBK IOYXC ISOJX FRZXJ XIUXN ENDJN OIDAS PHFDJ EIPFR WNEEK SOLSD SOSUF DJEIN OJXIX NZXSI DJXIJ NYCSO GNBPF RWSEL GFWOU NYYSG NEEPW NJXSU FUUPF KSENE PNOPF RKAIG NIVSE XSOGS OGIVK PFOIW NEEDS PSDPF RWSEL PFRKB EFWKP WSPNB XIDYF OJIOJ WNJXS VIZIJ SCEIE FVIWX NYXWF REGYI KJSNO EPOFJ DRNJA IWXPW XSJSA FDJUS KJNYR ESKEP URKIP FROZA SOJXN DURKI PFROZ ASOAR DJCI

is a ciphertext encrypted using a substitution cipher. What is the plaintext message?