CS5434 – Homework 6

Due Friday December 4th, 2015.

Problem 1

Suppose X is one of nine messages, A through H, where

P(A) = P(B) = P(C) = P(D) = 1/16

P(E) = P(F) = P(G) = P(H) = 1/8

P(I) = 1/4.

What is the entropy of the distribution?

Problem 2

Decrypt the following word, which was encrypted with a Caesar cipher of shift 3.

Dqwhgloxyldq

Problem 3

Suppose we have a strong cryptographic hash – a function which encrypts an input to produce a hash value of fixed size of *n* bits in way in which makes it extremely difficult to deliberately produce collisions. You may assume that the output has perfect entropy.

a) Suppose we have two completely different plaintexts. What is the probability that they will have the same hash, as a function of *n*?
b) Suppose that we have *m* completely different plaintexts. What is the probability that any two of them will have the same hash, as a function of *n* and *m*?

Problem 4

The following cipher-text was encrypted with a single-character substitution cipher of some kind. Decrypt it to determine the English plain-text.

Hint 1) Line breaks were not encrypted, but spaces and punctuation were.

Hint 2) The plain-text is famous.

.xebwcmxb,wfvnwc,z,vwi,fbcwfpxwxebw.fdq,bcwgbxepqdw.xbdqwxvwdqrcwmxvdrv,vdk
fwv, wvfdrxvkwmxvm,rz,nwrvwurg,bdikwfvnwn,nrmfd,nwdxwdq,wybxyxcrdrxvwdqfd
fuuwo,vwfb,wmb,fd,nw,aeful

vx w ,wfb,w,vpfp,nwrvwfwpb,fdwmrzruw fbkwd,cdrvpw q,dq,bwdqfdwvfdrxvkwxb
fviwvfdrxvwcxwmxvm,rz,nwfvnwcxwn,nrmfd,nkwmfvwuxvpw,vneb,lw ,wfb,wo,d
xvwfwpb,fdwgfddu,t.r,unwx.wdqfdw fblww ,wqfz,wmxo,wdxwn,nrmfd,wfwyxbdrxvwx.
dqfdw.r,unkwfcwfw.rvfuwb,cdrvpwyufm,w.xbwdqxc,w qxwq,b,wpfz,wdq,rbwurz,cwdqfdw
dqfdwvfdrxvworpqdwurz,lwrdwrcwfudxp,dq,bw.rddrvpwfvnwybxy,bwdqfdw ,wcqxeunwnxw
dqrcl

gedkwrvwfwufbp,bwc,vc,kw ,wmfvwvxdwn,nrmfd,wttw ,wmfvwvxdwmxvc,mbfd,wttw ,
mfvwvxdwqfuux wttwdqrcwpbxevnlwdq,wgbfz,wo,vkwurzrvpwfvnwn,fnkw qx
cdbeppu,nwq,b,kwqfz,wmxvc,mbfd,nwrdkw.fbwfgxz,wxebwyxxbwyx ,bwdxwfnnwxb
n,dbfmdlwdq,w xbunw ruuwurddu,wvxd,kwvxbwuxvpwb,o,og,bw qfdw ,wcfiwq,b,kw
gedwrdwmfvwv,z,bw.xbp,dw qfdwdq,iwnrnwq,b,lwrdwrcw.xbwecwdq,wurzrvpkwbfdq,bkwdx
g,wn,nrmfd,nwq,b,wdxwdq,wev.rvrcq,nw xb-w qrmqwdq,iw qxw.xepqdwq,b,
qfz,wdqecw.fbwcxwvxguiwfnzfvm,nlwrdwrcwbfdq,bw.xbwecwdxwg,wq,b,wn,nrmfd,nw
dxwdq,wpb,fdwdfc-wb,ofrvrvpwg,.xb,wecwttwdqfdw.bxowdq,c,wqxvxb,nwn,fn
,wdf-,wrvmb,fc,nwn,zxdrxvwdxwdqfdwmfec,w.xbw qrmqwdq,iwpfz,wdq,wufcd
.euuwo,fceb,wx.wn,zxdrxvwttwdqfdw ,wq,b,wqrpquiwb,cxuz,wdqfdwdq,c,wn,fn
cqfuuwvxdwqfz,wnr,nwrvwzfrvwttwdqfdwdqrcwvfdrxvkwevn,bwpxnkwcqfuuwqfz,wf
v, wgrbdqwx.w.b,,nxowttwfvnwdqfdwpxz,bvo,vdwx.wdq,wy,xyu,kwgiwdq,wy,xyu,kw
.xbwdq,wy,xyu,kwcqfuuwvxdwy,brcqw.bxowdq,w,fbdql