

Homework 2

CS 460
Winter 2007
Craig A. Rich

In problems 1–2, perform a cryptanalysis of the given ciphertext Y produced by a secret-key cryptosystem, and give the following:

- a) Find the plaintext X.
- b) Precisely describe the encryption (*not* decryption) algorithm that was used to produce Y from X. If the algorithm is a substitution cipher, clearly state the alphabet of characters to which it applies.
- c) Describe the secret key Z that was used during encryption (*not* decryption).

1 (produced by single substitution)

w"/<Z!ZpzMLM<M8\$DM<G8ZG<G8i<OLi>\$pg<M\$,GDZ/i<Di<MG"gLig<X\$!GZL!M<Mi/L\$"M
giMl1!<,pZDM<G8ZG<8Z[i<pig<gL/iXGpz<G\$<M=iXL,LX<["p!i/Z>LpLGLiM~<D8LX8
ZGGZX:i/M<X\$"pg<iN=p\$LG<G\$<Z,,iXG<ipiXGL\$!<\$"GX\$EiM}<<2z</iZ:L!l<G8i<MiZp
\$!<V"MG<\$!i<[\$GL!l<EZX8L!i~<Z<X/LEL!Zp<X\$"pg<pZ"!X8<Z<[\$GiUMGiZpL!l<[L/"M
G8ZG<X\$"pg<M=/iZg<G\$<i[i/z<EZX8L!i<L!<Z<X\$"!Gz}<<2z<EZ!L="pZGL!l<Z<[\$GL!l
EZX8L!i<,\$/<Z<,iD<EL!"GiM<Z,Gi/<G8i<ipiXGL\$!~<Z<X\$//="G<[\$p"!Gii/<=\$pp
D\$/:i/<X\$"pg<giGi/EL!i<8\$D<iZX8<=i/M\$!<D8\$<"Mig<G8ZG<EZX8L!i<[\$Gig}<<}<8iMi
Z!g<EZ!z<\$G8i/<ZGGZX:M<Z/i<,iZML>pi}

1"/G8i/E\$/i~<>iXZ"Mi<G8i<OLi>\$pg<MzMGiE<M",,i/M<,\$E<MzMGiELX<,pZDM~<!\$G
V"MG<LE=piEi!GZGL\$!<gi,iXGM~<Di<XZ!\$G<X\$!Xp"gi<G8ZG<G8i<pLMG<\$,
["p!i/Z>LpLGLiM<G8ZG<Di<=/iMi!G<L!<G8LM</i=\$/G<LM<iN8Z"MGL[i}<<j!giig~<i[i!
ZM<Di<D/LGi~<Di<Z/i<!"X\$[i/L!l!<iD<["p!i/Z>LpLGLiM<Z!g<piZ!/L!l<\$,
ZggLGL\$!Zp<["p!i/Z>LpLGLiM<>iL!l<Lgi!GL,Lig<>z<\$G8i/M}<<KzMGiEM<DLG8
Z/X8LGiXG"/Zp<DiZ:!iMMiM<Gi!g<G\$<>i<,/ZlLpiUUUi[i!<ZM<:\$D!<,pZDM<Z/i<,LNig~
!iD<\$!iM<Gi!g<G\$<X\$Ei<G\$<pL18G}

PZ/G<\$,<G8i<=/E\$ELMi<\$,<ipiXG/\$!LX<[\$GL!l<LM<G8ZG<GiX8!\$p\$1LXZp<Z!g
=/\$Xig"/Zp<MZ,il"Z/gM<XZ!<>i<X\$E>L!ig<G\$<X\$!g"XG<ipiXGL\$!M<E\$/i<MiX"/ipz
G8Z!<i[i/<>i,\$/i}<<}<8i<OLi>\$pg<MzMGiE<g\$im<!\$G<pL[i!<="<G\$<G8LM<=/E\$ELMi~
8\$Di[i/~<>iXZ"Mi<LGM<["p!i/Z>LpLGLiM<Zpp\$D<Z/<iZM\$!Z>pz<M\$=8LMGLXZGig
ZGGZX:i/<G\$<M"/E\$!"G<ZpE\$MG<i[i/z<GiX8!\$p\$1LXZp<>Z//Li/<G8ZG<LM<L!<="pZXi}
'M<Z</iM"pG~<G8i<MiX"/LGz<\$,<ipiXGL\$!M<X\$!g"XGig<\$!<G8i<OLi>\$pg<MzMGiE
gi=i!g<ZpE\$MG<i!GL/ipz<\$!<G8i<,iXGL[i!iMM<\$,<ipiXGL\$!<="/Xig"/iM}

K\$"/Xi<e\$gi<Si[Lid<\$,<G8i<OLi>\$pg<|GGL!l<KzMGiE
X\$EELMML\$!ig<>z<G8i<eZpL,\$/!LZ<KiX/iGZ/z<\$,<KGZGi
c"pz<5&~<5&&-

2 (produced by multiple substitution)

A}30qRKCP, _GI+(pyM={+p=R:{6p|E^H_JIb}EpyMwp, 1PZr4Cotbi+Obirsn=\$KhGi^HMh
=nh^D9JP+5McJ6\$^UZDqD_d]PzqDs05C:P]0^5CzG&, G1^Y\$J6Dw>G^R01MJ0^CHnz-wi>}(
vSq6ujqRJOb@|YG{\JOH^z@, 05_&EoqR10{^bZ:{I460DH{:4HhJ^Gzztjxb5o:ZoEc}=y{^

/@r]pwZ\$steR, o|4q+=SzRt-MEJ6DwEpyRtGieoYEt;>^hn%] ^D@qhwvGpH] IxnE+=P, 0b-
3Suzr:D5JWDjM5K0}@=YR+Gzo(G5E{W:vP%woZ^bSHEM=&Ptvb|G]-qSC_^{U}!nrxWID
(4>yR6KKb=9tuZ]ExG&s}>[IJ^n0\$]{^RH4>uD\+3R]-x@E+D@6+nqIbC\$IxM|']]a^<^
>G_Sq4rD={\:^r&{oGv-\+3\$z0G1MtEUG:uHU\$|MHRzdt!S3zu^JZnrS>G+}ewbjRHK-D@>YG
'DhM&(PyR0]OrJv}=ow1@q5R=p3zMwEDwU4^y\$|O9tzGn1^Z_wWp+UuCxw3@|, \$5]rb
, o(DH-r|P6owIUeE]^E:u-:-Sie^YuoZIZd:OMYS|o^W

Ve+IxM]hR^O{ODH+-InH, 09:^IwvpdJE4yowq]H_G|weD=w^}5-SvR>0&6}:CGI:Ix\$0=txp5, {
bHtEU\${:o:nqqK0HKbHGw, \$1^'MO']w)xMwHp{YGZE:05, S0r>%]0-]=GqS^6PZEwr}J>S-U+6D
v4>yoEws^rUJj|b, S^6{+cUD0oJ{MY@=^I%}x4{H*Ew3ooZJrU}=}SCxz%]1MIIo, \:4H, &u6
iMn=-]rUR+;MhR=ng]FD((@5^YP6^b50:Fbvvu{-uDZ*0]j=oeR=MHYR]i}=&yoG!uZ_w^DhR
OR^|Rr:YDSqh]pzz}s+izps{]6}]CbtS5MT!b{ \$, \:jDrMHI04zq%&y^zquH_] ^bHeu, R5^'\$]05
Ixo^>t!|Dh@YE-^

/%]MiiM^E^1Mqd&-0h^ZC+c0IxJcx4Ew00ty5DcZtuH&Y>d!rDC=4!x%] ^>YqR-wn-
W-R^@>urd:6U=]^_x&b3{Y@=0r%\W:6xM+^}HE|b1G=-^pq]^hMntrxPI]yRRj0H_t{ \$^@=uId
(GEUbh0+{o^=MEJ(py\$0:ExG(J(b=R&0(jmZor>P3zr9&6U\$+;FFwUp0t, =nsH&nZ]DSEY>%
i=]vtIxo:-^}iIsn>GJ=p, ^}+-RItpH, J=pu-Gh&M%o3>Dc0]p({}ZC:{D(Mt0\$^S|uEd+RTjo=6-^

W)xo|o]u-&H}&|Rp{DZ:sxdt|\$_@qnI]|{-xb@q,], u{YD@>p_o]}!\$ZK0}@|^o+nj!|DPYxR{
6x4I&vnd+0HwrxG+MZh:3MJ({}=M&{\$^S=\$\]YxGnjR>9w(D=o]05ER>bjG>n3zo9:\$n-^\$=&Ib
{In5, p=, ^N\$9tnH, t\$p-OR>}6D:'o>6^e%\W]/M|ZP=, +Ld, E\+YUPu=(PZw)e+rUR+-R^@=uE%
Yb((uIIRoJeb=:4&_qD34z+0HhS-6>d]n{-}Yu4EuD5J^pzzMh+EUGJ<27Jm-biIsP|oKhMiuZR,
>n, ubQ:;]>@ (9:{P0h]^Z&n5toKvnuqJ^ZIo=1^Gs&Ixu{:sGRy^

)xoJ;]=@(\:cUO^U:>Rj|o{RZr-&=G-\$n>YU:uHOI^rSr0}5{t45, +^}vjPH0o0:{S^U]p{
ADID|bzP9&k)l):"43{\+[]>IU=Sj:??@((4Zwn5hJ.^>_u5^PJ)\$Yx9tS|CG, wIxo+;FFw6D
3P^yJncPdJe|bv&rU4Iw{EnZYM&^H]nwi}|vnq&!M6^60DH:Ex^0]cRRy^

kZZR:/|bPYx\$
<EPiitg|urM=\wF[L]w[Rs0^Yb(
X@zd+f9]8BB#

- 3 An n -symbol permutation is a one-to-one function $\pi: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, which can be defined by a vector $(\pi(1), \pi(2), \dots, \pi(n))$. For each permutation π , there is a unique inverse permutation $\pi^{-1}: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ such that $\pi^{-1}(\pi(i)) = \pi(\pi^{-1}(i)) = i$, for $i = 1, \dots, n$. A *transposition cipher* is a secret-key cryptosystem in which the encryption function $E: \Sigma^n \times (\{1, \dots, n\} \rightarrow \{1, \dots, n\}) \rightarrow \Sigma^n$ and decryption function $D: \Sigma^n \times (\{1, \dots, n\} \rightarrow \{1, \dots, n\}) \rightarrow \Sigma^n$ are defined by

$$\begin{aligned} E(X_1 X_2 \dots X_n, Z) &= X_{Z(1)} X_{Z(2)} \dots X_{Z(n)}, \\ D(Y_1 Y_2 \dots Y_n, Z) &= Y_{Z^{-1}(1)} Y_{Z^{-1}(2)} \dots Y_{Z^{-1}(n)}, \end{aligned}$$

where the secret key Z is an n -symbol permutation.

- a) Complete the methods `encrypt` and `decrypt` so that they implement the functions E and D . You can assume that the lengths of the actual array arguments are n :

```
static char[] encrypt(char[] x, int[] z)
static char[] decrypt(char[] y, int[] z)
```

- b) Show that for all $X \in \Sigma^n$, $D(E(X, Z), Z) = X$.

- 4 Show that for joint random variables X, Y ,

$$H(X, Y) = H(X) + H(Y | X).$$

- 5 Show that a secret-key cryptosystem in which $Y = E(X, Z)$ and $X = D(Y, Z)$ satisfies

$$H(Y | X, Z) = 0 \text{ and } H(X | Y, Z) = 0.$$