Errata for the examples and exercises in *Cryptanalysis* by Gaines

The changes in **red** are to correct the resulting plaintexts. Items highlighted in yellow are uncertain.

page 35, exercise 26

```
IKOTH NNEHN EEIRC RAGEL ORNOH KTWTC HOHEI
ESSWW TNETR HAREO LSPLA AGEAE RLDBR YEUIT
RTREN IDTHE IADEI ENDPD ABRAE CRKEM TAOAU
TOTSY NBPES NUHES RAHES UPD
```

page 48, figure 43

```
ENTHV CCOTX REMUS OEUYE ISGAU AMAHY
TAEID EXTNB HBNSE IRAST DANVN XGGEO
ICRLB XCSUT LTESR
```

page 52, exercise 33, seven letters missing in middle of plaintext

```
VINSR CFEAE OOHSE FHLET FHUNS TNCLT SLCIA EESHR
HSIRE TTMTS ETEPD TSOIN MRTTH TLOLR UBE
```

page 66, exercise 40, something is wrong with the highlighted letters:

```
TEHAN EMGSL LIWSN ETTAC KYEIA AEBPS OURPE
MOCEE TUNRI STERS AFOET ORTDA ERTEF DINCA
SERET TUOPW ARURE FFOYA EEDFO RDRCR
```

page 125, exercise 110

```
JQQYP IRSFQ YJNEU RUVEF VWPEB QFGTE MKUKG
RWETZ IDVIQ QSZIH KWMCE KBFJQ QXTRF VRJKO
ATEEN JUMSN GLPIB SOASR YSAXR UOJGW MVRUS
VDQQR DPPKP LIC
```

page 137, exercise 116

```
WLPCV MOGKE EIFMU RWWFH VMFFW EYXAV UBICZ
OJMLC HVXYF KSCUS XILMG BQIDB WIFGB IQZGZ
HFJYP MKIGV PTWYK WZHWM ZHWIF APSDN WFHED
```

SCXAV OEBYY OKCOY UIHUJ LHUDX PPWVV HPFWY
LGFBV EJMAA GBPIE BAVUV QLZNL PWAJW

page 158, exercise 128

OOUJV JMKNC BUQLP FULAS AZFTG MPBVA YVSQJ
LFAWS PCHAE IUNRS MFVWS SOOHM EBEAM KFAAX
RHKZR JQAO**I** AVMEI BTOPD JGPRJ NFRXT IIGXF
KDHXA FTHJQ HLARK TGDLP SBMVY EEVAO ACSMU
VUWCV CTSKS MWLON PAOOH MWWPY POHIL GAZQB
QUZBQ PKMBO VKWJH PJAGD CHXGW QBKOG YAKSI
WNWEX QNUS**U** CVOEY HYJJC BTBVJ QMNSP ARVPX
OAGTA VLVCZ BDIXN FMWUE ZLNNN WBMOX GTCPK

page 158, exercise 130

TBFNQ XEFDG FWEAF XSQUN IGAHE UNBBJ LOBQP
HFAKA SNXGB PEEJW WLZJO MLLAP RVYTN MXHYV
OSESQ VOAQM OGVPA JKPYI UZFQG YJYTL DFELQ
ZLWYY UYZNE PPFWB RWMEE F**R**WXJ WEPRV YBUMP
ZZMTS BUKKB ALKZI LQALZ KKFSX ZUSTG JTHAR
GSBXI WVLZB ZMPIK YIURH RVWCV AUFVL WFQZU
DIGFW HTZMS FBKTZ UTRKI VFZXW LCAUJ PANVS
EOZUX GIXDS XMGQE LQTVB LEIDI ALLAI NOENL
VJIOI SWQTD ECTM

page 171, figure 139

YVNGK YEGDP ZEAYK HSMDQ KKWSJ IQ**V**IO
KCFKQ JPMLB JXGKC ZDBGN GQBDQ MEONK
XTYAD DDGJR XRXFW GDAYT QSGGC GPBYO
CLWKC BICFE ZDGJW KUFKC BUIZY BKEKC
GKTAO QCBYQ UUFZG GZYFN FMJVZ BLQJU
VMMJT AEFVS MENKQ JEIZY ALQYR XRXFR
OUFVS VVVVP KTBKC GOMIK BQVZN BINAO
CEVVJ FVUZS BKMKC GPMDT KKYAD DDYZC
BTKVS GQWIT ZDAKP GWBIO NDGRC HPBHU
GKTQH GUVZN YXMLH FSMDQ KKWZQ UDAMT
ZDBJO PEULR YUGKU ZEUSJ ZDBOD RESIO
RLABL JRSZQ YQVFL

page 184, exercise 138

LLDRK YCRFA SEVSU KTDUL XVK**E**V CABLY UPYMR
KBEXU BTELW PJFPT IIUQQ KTFCT PSKQL WNDAP
BFAES NMPRK APTTS HFKBZ RMGPP YVMSA IFNPZ
ALTSU SAUDN LXAAZ YPUCH KNPYV MSIAX KKDBE
TPSAT PKPSY VTAYE APBTE LWPJF PTAXN

page 197, exercise 144

SOVFO GSGUF VIJRI FMOUI CFTTI KZYZZ ZUIFQ
QLOWU VAFJF IWWLN CRGJF EMVVN NCDHW TAJN**W**
ARDB

page 197, exercise 145

YYIZC UOFYV HQYHT BEBSX PTSYC RMRXL XEAGU
YLPUQ BUUQN YUSOQ MOOSP UGIJI IFFFA LIRGG
FGEHH NTEGY ZSMCO FUDEM XOGIK KVBNK WKPQX
MGDLA IFNHM XTUME ZXYZG NAPDW CDMNC TTHN**J** FD

page 197, exercise 146

XEITB BBBVM XRSJP YLKEN YKSZK FRWLG SAYEA
VIXIX DUVDU RJGEI BANZF HDCCY COYRV ABKWB
RHFKK FXSEJ YTFNL RNIVK VKQHI QHIJL PGOU**J**
VFCFT SHLID VDDM**P**

page 197, exercise 147

ECGMH TYTAJ BTHNG AWKLI BEMNR HTDGN GPDAO
QAXRP ZPFHD DXIEA U**B**SYC IXCWV RHPBO IXY**P**Y
DVWNR **N**XOOK KIHFO XDSVL VWWCL IHZHV WRLHW
MMIEE AHGQY RSRLK LWZTJ AYWFN SSUCV ZLPXP
SEEEY RTHDH TZNUP URMGK ZNTYE QDEZE NNH**W**M
INRLP SSWPY MCRUB JZYCR NLMAS MEUCL RMDYR
NESTO BVJEU DVLOT SQBJH BNRLB VDXJP XNIGF
ICQJY QZXQG KBLFQ UBQKN ELSSL YGTLF LTDZZ
YKEER HKLWL IMRNJ SOOJP QCAUD MEIBB QXAHC
VAJCM GXBIC DKVCL GQIBS CFVFW QNAXI DRZSX
RBIWR CQR

page 208, exercise 149 (spelling of place name)

OS CF WD OG DR AN PO AS OA DH SD EH XK FU
CN DR **PF** UK SD

page 208, exercise 153

YG NG CR FV FZ RI OU KZ CW OW BQ GQ IH HL
YW EG NG QM WX RT KP VE CA IG QI VD QI GN
GZ IZ QY QR HY NG XN AB AK OX NY WC WC TN
OX DH NE IH IH YR IS QY WC HI UI UI IR QE
WS RW LG WR AB GW VW CA RQ XM ER QM RE CW
ZI RQ XW QW GH YC AY YO VO NE RL PG CG WI
NX VW CA NX QM LH IG RQ WT GO UI GZ EG XN
IW OU XT WO LH IG RQ XM WS QY TX IR IQ XM
OG DU AB RM AK UM RG ZR XA PM RW LD KG HI
XK LC RT KP VE FO NX XK WR WS QY UR ZX YL
AT UI RH TR AV WS DH WQ PM AK IW OU WT DE
IR WX RQ XZ SI GU QN IR XN IR YN IG GY TR
ZX YU RU YL IQ YA RU KG QM PD QM IY HA WS
FE RW GH RB HA QI QM GI QC QR UL WV AB NX
GO HA FR IY QY B**M** QM YH NG IQ RU YL IQ BL
P**O** QM RU GU IR TX SI GQ LQ DX XO EV BM CR
FV GV AB GE RZ GQ YH HA RW YM NE YM BL VW
PS

page 215, exercise 161 (photocopying error)

EGWGW GEGTU CLCUO XGKZT EGOBG BYLWM IQNKQ
YENFS CLHMN YBXSE TNIWO CEGCB FCTCS ZTVGB
EAEGT URKFK BEGKX BCTGZ YLXCH YEGCU OXYTQ
FADQT TCUNB OGCOH XCEWE CUVEG COCXY XGBEA
YTKXF QCOTB XNEGT UCONT OPELE KUVUN TOCNG
NGBKW CEECS ZKWNH EIKCC REGCT EGTUR KFKTB
RGMWX CFGQN ICEBP EEWEN BKIYF KFDOF EGNUC
BGMTZ TFXCE WECFV DTTUZ TENEG WGLFM CTOV**L**

Corrections to the solutions

30. keyword **BERKELEY**

40. keyword is not FRANK; taken off counterclockwise

41. description does apply to 40, but keyword is not DAMON

90. Devout **h**aik-beclad hadji...

148. key **5,4,1,2,3** with keyword **TRAMP**