**MTH6115 Cryptography Exercises 1 Solutions**

Q1

ORJNE RGURV QRFBS ZNEPU

Most common letters are R (4) and N, E, U (2). So lets try the Caeser cyphers which take e to either R, N, E, or U as a first attempt. Taking e to R corresponds to a cyclic shift of 13 letters to the right and deciphers the ciphertext as

BEWARE THE IDES OF MARCH

Q2 (a)

```
MAXSK CGPIY AILNI GPTQI YXPHA XYINP LGHAX HALYU XGVXQ KTXMA XAIPF
NKCBA HIQKG BSKNL HMAXI PPNXM MXPLH HKBCJ MKSSL YXLGA XNZIG QJDIQ
QXHGL YKQIM SLGBX NMSLG IQQJS KCGPK GXQIM HYNXI MXPMH IZTIM MAXQL
YUXPL HIWCX CXSKN ZXPIA XIPKS AXNLG AXNZL GPXPB LGBHK DINPM HAXMA
IPKDL GLHMY IBXPM HIQQI HHAXM CFMLP LINJT KMHKS SLYXF CHHAX GMAXG
KPPXP NXIQL MLGBH AIHHA LMQXH HXNDI MHAXQ IMHMA XDKCQ PXVXN MXGPH
ALMMH IZTHA XQIMH MAXDK CQPXV XNQLY UBKKP MHIZT WCXCX MTCHG LYKQI
LGIPI JQKGB SCNJJ KCFKC BAHHA KCMIG PMIGP HAXGH AXSKQ QKDLG BDXXU
HAXTN LYXKS ZILQD XGHCT IBILG BKKPK GXZKN XKSQL SXMPC HLXMP LMYAI
NBXPS KNHAX VXNJQ IMHHL ZXIII
```

```
X 63 12.19%      C 19        W 2
H 43  8.32%      S 17
I 42  8.12%      B 15
M 39  7.54%      Y 14
K 35  6.77%      T 9
L 35  6.77%      D 9
A 33  6.38%      Z 9
P 33  6.38%      J 8
G 30  5.80%      F 4
Q 27  5.22%      V 4
N 23  4.49%      U 4
```

Case 1 Take $X = e$

```
MAeSK CGPIY AILNI GPTQI YePHA eYINP LGHAe HALYU eGVeQ KTeMA eAIPF
NKCBA HIQKG BSKNL HMAeI PPNeM MePLH HKBCJ MKSSL YeLGA eNZIG QJDIQ
QeHGL YKQIM SLGBe NMSLG IQQJS KCGPK GeQIM HYNeI MePMH IZTIM MAeQL
YUePL HIWCe CeSKN ZePIA eIPKS AeNLG AeNZL GPePB LGBHK DINPM HAeMA
IPKDL GLHMY IBePM HIQQI HHAeM CFMLP LINJT KMHKS SLYeF CHHAe GMAeG
KPPeP NeIQL MLGBH AIHHA LMQeH HeNDI MHAeQ IMHMA eDKCQ PeVeN MeGPH
ALMMH IZTHA eQIMH MAeDK CQPeV eNQLY UBKKP MHIZT WCeCe MTCHG LYKQI
LGIPI JQKGB SCNJJ KCFKC BAHHA KCMIG PMIGP HAeGH AeSKQ QKDLG BDeeU
HAeTN LYeKS ZILQD eGHCT IBILG BKKPK GeZKN eKSQL SeMPC HLeMP LMYAI
NBePS KNHAe VeNJQ IMHHL ZeIII
```

Using letter frequencies we probably have either $H = t$ or $I = t$. There are 13 occurrences of $H * e$ and 11 of these are $HAe$. There are 2 occurrences of $I * e$ once as $IAE$ and once as $IBE$. So, if $X = e$, then we probably have $H = t$ and $A = h$.

Case 1.1 Take $H = t$ and $A = h$.

```
MheSK CGPIY hILNI GPTQI YePth eYINP LGthe thLYU eGVeQ KTeMh ehIPF
NKCBh tIQKG BSKNL tMheI PPNeM MePLt tKBCJ MKSSL YeLGh eNZIG QJDIQ
QetGL YKQIM SLGBe NMSLG IQQJS KCGPK GeQIM tYNeI MePMt IZTIM MheQL
YUePL tIWCe CeSKN ZePIh eIPKS heNLG heNZL GPePB LGBtK DINPM theMh
IPKDL GLtMY IBePM tIQQI ttheM CFMLP LINJT KMtKS SLYeF Ctthe GMheG
KPPeP NeIQL MLGBt hItth LMQet teNDI MtheQ IMtMh eDKCQ PeVeN MeGPt
hLMMt IZTth eQIMt MheDK CQPeV eNQLY UBKKP MtIZT WCeCe MTCtG LYKQI
LGIPI JQKGB SCNJJ KCFKC Bhtth KCMIG PMIGP theGt heSKQ QKDLG BDeeU
theTN LYeKS ZILQD eGtCT IBILG BKKPK GeZKN eKSQL SeMPC tLeMP LMYhI
NBePS KNthe VeNJQ IMttL ZeIII
```

The sequence $C\ Bhtth$ suggests that $B = g$ and $C = u$.
Take $B = g$ and $C = u$

```
MheSK uGPIY hILNI GPTQI YePth eYINP LGthe thLYU eGVeQ KTeMh ehIPF
NKugh tIQKG gSKNL tMheI PPNeM MePLt tKguJ MKSSL YeLGh eNZIG QJDIQ
QetGL YKQIM SLGge NMSLG IQQJS KuGPK GeQIM tYNeI MePMt IZTIM MheQL
YUePL tIWue ueSKN ZePIh eIPKS heNLG heNZL GPePg LGgtK DINPM theMh
IPKDL GLtMY IgePM tIQQI ttheM uFMLP LINJT KMtKS SLYeF utthe GMheG
KPPeP NeIQL MLGgt hItth LMQet teNDI MtheQ IMtMh eDKuQ PeVeN MeGPt
hLMMt IZTth eQIMt MheDK uQPeV eNQLY UgKKP MtIZT Wueue MTutG LYKQI
LGIPI JQKGg SuNJJ KuFKu ghtth KuMIG PMIGP theGt heSKQ QKDLG gDeeU
```

```
theTN LYeKS ZILQD eGtuT IgILG gKKPK GeZKN eKSQL SeMPu tLeMP LMYhI
NgePS KNthe VeNJQ IMttL ZeIII
```

The sequence $Wueue$ occurs twice. This looks like *queue* so try $W = q$

```
MheSK uGPIY hILNI GPTQI YePth eYINP LGthe thLYU eGVeQ KTeMh ehIPF
NKugh tIQKG gSKNL tMheI PPNeM MePLt tKguJ MKSSL YeLGh eNZIG QJDIQ
QetGL YKQIM SLGge NMSLG IQQJS KuGPK GeQIM tYNeI MePMt IZTIM MheQL
YUePL tIque ueSKN ZePIh eIPKS heNLG heNZL GPePg LGgtK DINPM theMh
IPKDL GLtMY IgePM tIQQI ttheM uFMLP LINJT KMtKS SLYeF utthe GMheG
KPPeP NeIQL MLGgt hItth LMQet teNDI MtheQ IMtMh eDKuQ PeVeN MeGPt
hLMMt IZTth eQIMt MheDK uQPeV eNQLY UgKKP MtIZT queue MTutG LYKQI
LGIPI JQKGg SuNJJ KuFKu ghtth KuMIG PMIGP theGt heSKQ QKDLG gDeeU
theTN LYeKS ZILQD eGtuT IgILG gKKPK GeZKN eKSQL SeMPu tLeMP LMYhI
NgePS KNthe VeNJQ IMttL ZeIII
```

The next most common letters are $I$ and $M$. I can see nothing special about the distribution of $I$, but there are many digrams $Mh$ and $Mt$ and $MM$. So it looks like $M = s$.
Case 1.1.1 Try $M = s$.

```
sheSK uGPIY hILNI GPTQI YePth eYINP LGthe thLYU eGVeQ KTesh ehIPF
NKugh tIQKG gSKNL tsheI PPNes sePLt tKguJ sKSSL YeLGh eNZIG QJDIQ
QetGL YKQIs SLGge NsSLG IQQJS KuGPK GeQIs tYNeI sePst IZTIs sheQL
YUePL tIque ueSKN ZePIh eIPKS heNLG heNZL GPePg LGgtK DINPs thesh
IPKDL GLtsY IgePs tIQQI tthes uFsLP LINJT KstKS SLYeF utthe GsheG
KPPeP NeIQL sLGgt hItth LsQet teNDI stheQ Istsh eDKuQ PeVeN seGPt
hLsst IZTth eQIst sheDK uQPeV eNQLY UgKKP stIZT queue sTutG LYKQI
LGIPI JQKGg SuNJJ KuFKu ghtth KusIG PsIGP theGt heSKQ QKDLG gDeeU
theTN LYeKS ZILQD eGtuT IgILG gKKPK GeZKN eKSQL SesPu tLesP LsYhI
NgePS KNthe VeNJQ IsttL ZeIII
```

We have the sequence $...gt\ hItth\ Ls$. This looks like '...g that this'. So try $I = a$ and $L = i$.

```
sheSK uGPaY haiNa GPTQa YePth eYaNP iGthe thiYU eGVeQ KTesh ehaPF
NKugh taQKG gSKNi tshea PPNes sePit tKguJ sKSSi YeiGh eNZaG QJDaQ
QetGi YKQas SiGge NsSiG aQQJS KuGPK GeQas tYNea sePst aZTas sheQi
YUePi taque ueSKN ZePah eaPKS heNiG heNZi GPePg iGgtK DaNPs thesh
aPKDi GitsY agePs taQQa tthes uFsiP iaNJT KstKS SiYeF utthe GsheG
```

```
KPPeP NeaQi siGgt hatth isQet teNDa stheQ astsh eDKuQ PeVeN seGPt
hisst aZTth eQast sheDK uQPeV eNQiY UgKKP staZT queue sTutG iYKQa
iGaPa JQKGg SuNJJ KuFKu ghtth KusaG PsaGP theGt heSKQ QKDiG gDeeU
theTN iYeKS ZaiQD eGtuT agaiG gKKPK GeZKN eKSQi SesPu tiesP isYha
NgePS KNthe VeNJQ astti Zeaaa
```

The next most common letter is $K$. The sequence $ghtthKusa$ indicates $K$ is equal to the one remaining vowel.
Take $K = o$

```
sheSo uGPaY haiNa GPTQa YePth eYaNP iGthe thiYU eGVeQ oTesh ehaPF
Nough taQoG gSoNi tshea PPNes sePit toguJ soSSi YeiGh eNZaG QJDaQ
QetGi YoQas SiGge NsSiG aQQJS ouGPo GeQas tYNea sePst aZTas sheQi
YUePi taque ueSoN ZePah eaPoS heNiG heNZi GPePg iGgto DaNPs thesh
aPoDi GitsY agePs taQQa tthes uFsiP iaNJT ostoS SiYeF utthe GsheG
oPPeP NeaQi siGgt hatth isQet teNDa stheQ astsh eDouQ PeVeN seGPt
hisst aZTth eQast sheDo uQPeV eNQiY UgooP staZT queue sTutG iYoQa
iGaPa JQoGg SuNJJ ouFou ghtth ousaG PsaGP theGt heSoQ QoDiG gDeeU
theTN iYeoS ZaiQD eGtuT agaiG gooPo GeZoN eoSQi SesPu tiesP isYha
NgePS oNthe VeNJQ astti Zeaaa
```

The sequence $ghtth\ ousaG\ PsaGP$ looks like '...ght thousands aGP...' so try $G = n$ and $P = d$

```
sheSo undaY haiNa ndTQa Yedth eYaNd inthe thiYU enVeQ oTesh ehadF
Nough taQon gSoNi tshea ddNes sedit toguJ soSSi Yeinh eNZan QJDaQ
Qetni YoQas Singe NsSin aQQJS oundo neQas tYNea sedst aZTas sheQi
YUedi taque ueSoN Zedah eadoS heNin heNZi ndedg ingto DaNds thesh
adoDi nitsY ageds taQQa tthes uFsid iaNJT ostoS SiYeF utthe nshen
odded NeaQi singt hatth isQet teNDa stheQ astsh eDouQ deVeN sendt
hisst aZTth eQast sheDo uQdeV eNQiY Ugood staZT queue sTutn iYoQa
inada JQong SuNJJ ouFou ghtth ousan dsand thent heSoQ QoDin gDeeU
theTN iYeoS ZaiQD entuT again goodo neZoN eoSQi Sesdu tiesd isYha
NgedS oNthe VeNJQ astti Zeaaa
```

The next most common letter in $N$ so probably $N = r$. The sequence $tshea\ ddNes\ sedit\ toguJ$ looks like '...t she addressed it to guJ...' so take $N = r$.

```
sheSo undaY haira ndTQa Yedth eYard inthe thiYU enVeQ oTesh ehadF
```

```
rough taQon gSori tshea ddres sedit toguJ soSSi Yeinh erZan QJDaQ
Qetni YoQas Singe rsSin aQQJS oundo neQas tYrea sedst aZTas sheQi
YUedi taque ueSor Zedah eadoS herin herZi ndedg ingto Dards thesh
adoDi nitsY ageds taQQa tthes uFsid iarJT ostoS SiYeF utthe nshen
odded reaQi singt hatth isQet terDa stheQ astsh eDouQ deVer sendt
hisst aZTth eQast sheDo uQdeV erQiY Ugood staZT queue sTutn iYoQa
inada JQong SurJJ ouFou ghtth ousan dsand thent heSoQ QoDin gDeeU
theTr iYeoS ZaiQD entuT again goodo neZor eoSQi Sesdu tiesd isYha
rgedS orthe VerJQ astti Zeaaa
```

The sequence *sh ehadF rough taQon gSori tshe* looks like 'she had brought along for it. She' So take $F = b$, $Q = l$, $S = f$.

```
shefo undaY haira ndTla Yedth eYard inthe thiYU enVel oTesh ehadb
rough talon gfori tshea ddres sedit toguJ soffi Yeinh erZan lJDal
letni Yolas finge rsfin allJf oundo nelas tYrea sedst aZTas sheli
YUedi taque uefor Zedah eadof herin herZi ndedg ingto Dards thesh
adoDi nitsY ageds talla tthes ubsid iarJT ostof fiYeb utthe nshen
odded reali singt hatth islet terDa sthel astsh eDoul deVer sendt
hisst aZTth elast sheDo uldeV erliY Ugood staZT queue sTutn iYola
inada Jlong furJJ oubou ghtth ousan dsand thent hefol loDin gDeeU
theTr iYeof ZailD entuT again goodo neZor eofli fesdu tiesd isYha
rgedf orthe VerJl astti Zeaaa
```

Take $Y = c$, $T = p$, $U = k$, $V = v$, $J = y$, $Z = m$, $D = w$

```
shefo undac haira ndpla cedth ecard inthe thick envel opesh ehadb
rough talon gfori tshea ddres sedit toguy soffi ceinh erman lywal
letni colas finge rsfin allyf oundo nelas tcrea sedst ampas sheli
ckedi taque uefor medah eadof herin hermi ndedg ingto wards thesh
adowi nitsc ageds talla tthes ubsid iaryp ostof ficeb utthe nshen
odded reali singt hatth islet terwa sthel astsh ewoul dever sendt
hisst ampth elast shewo uldev erlic kgood stamp queue sputn icola
inada ylong furyy oubou ghtth ousan dsand thent hefol lowin gweek
thepr iceof mailw entup again goodo nemor eofli fesdu tiesd ischa
rgedf orthe veryl astti meaaa
```

She found a chair and placed the card in the thick envelope she had brought along for it. She addressed it to Guy's office. In her manly wallet Nicola's fingers finally found one last creased stamp. As she licked it, a queue

formed ahead of her in her mind, edging towards the shadow in its caged stall at the subsidiary post office. But then she nodded realising that this letter was the last she would ever send, this stamp the last she would ever lick. Good. Stamp queues put Nicola in a daylong fury. You bought thousands and then the following week the price of mail went up again. Good. One more of life's duties discharged for the very last time.

(b) Suppose the substitution cipher used in (a) is an affine substitution. Then there exist integers $A, B$, $0 \leq A, B \leq 25$, such that, if we label the letters of the alphabet as $a = 0, b = 1, c = 2, \ldots, z = 25$, the permutation $\pi$ which determines the cipher could be expressed as $\pi(i) \equiv Ai + B \pmod{26}$ for all $0 \leq i \leq 25$. Since $\pi$ replaces $a$ by $I$, we have $\pi(0) = 8$. Hence $B = 8$. Since $\pi$ replaces $b$ by $F$, we have $\pi(1) = 5$. Thus $A + 8 \equiv 5 \pmod{26}$ and $A \equiv -3 \equiv 23 \pmod{26}$. Thus $A = 23$. Hence $\pi(2) \equiv 23 \times 2 + 8 \equiv 54 \equiv 2 \pmod{26}$. This would imply that $\pi$ replaces $c$ by $C$, which is not the case. Thus the cipher is not affine.

Q3 (a)

| nonzero element | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| inverse element | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |

(b)

| invertible element | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| inverse element | 1 | 5 | 7 | 11 |

(c)

$$\begin{aligned} 288 &= 8 \times 35 + 8 \\ 35 &= 4 \times 8 + 3 \\ 8 &= 2 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

Hence $\gcd(35, 288) = 1$ so 35 is invertible in $\mathbb{Z}_{288}$. We have

$$\begin{aligned} 1 &= 3 - 2 = 3 - (8 - 2 \times 3) = 3 \times 3 - 8 = 3(35 - 4 \times 8) - 8 = 3 \times 35 - 13 \times 8 \\ &= 3 \times 35 - 13(288 - 8 \times 35) = 107 \times 35 - 13 \times 288 \end{aligned}$$

Hence $107 \times 35 \equiv 1 \pmod{288}$ so the inverse of 35 in $\mathbb{Z}_{288}$ is 107.
(d) The prime factorization of 288 is $288 = 2^5 \times 3^2$. So

$$\phi(288) = 2^4 \times (2 - 1) \times 3 \times (3 - 1) = 2^5 \times 3 = 96$$