Solutions to MATH3411 Problems 84–92

84.

a)

key	F	I	S	H	E	L	I	M	I	N	A	T	E	T	H	E	P	E	R	I
plaintext	E	L	I	M	I	N	A	T	E	T	H	E	P	E	R	I	O	D	I	C
ciphertext	J	T	A	T	M	Y	I	F	M	G	H	X	T	X	Y	M	D	H	Z	K

b)

key	F	I	S	H	J	T	A	T	R	G	A	M	V	Z	H	Q	K	D	Y	Y
plaintext	E	L	I	M	I	N	A	T	E	T	H	E	P	E	R	I	O	D	I	C
ciphertext	J	T	A	T	R	G	A	M	V	Z	H	Q	K	D	Y	Y	Y	G	G	A

c)

key	F	R	E	D	D	I	D	Y	O	U	G	E	T	T	H	E	R	I	G	H	T	A	N	S
plaintext	D	I	D	Y	O	U	G	E	T	T	H	E	R	I	G	H	T	A	N	S	W	E	R	S
ciphertext	I	Z	H	B	R	C	J	C	H	N	N	I	K	B	N	L	K	I	T	Z	P	E	E	K

Here, plaintext feedback was used, and the message was "DID YOU GET THE RIGHT ANSWERS[?]".

85.

a. The given frequencies freq1 and freq2 indicate how many times each letter occurs in an odd position and in an even position, respectively. For instance, A has freq1 $= 0$ since it does not appear in any odd position; however, it appears twice in an even position, so freq2 for A is 2.
Adding the two frequencies gives the overall frequencies:

i	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
f_i	2	4	6	3	1	5	3	4	3	8	7	11	6	6	2	0	3	0	7	1	6	7	10	3	23	5

Then $I_c = \dfrac{\sum \binom{f_i}{2}}{\binom{n}{2}} = \dfrac{(\sum_i f_i^2) - n}{n^2 - n} = \dfrac{(2^2 + 4^2 + \cdots + 5^2) - 136}{136^2 - 136} \approx 0.06024.$
(Here, $n = 136$ is the total number of letters). By the approximation from Kasiski's method,

$$r \approx \frac{0.0273n}{(n-1)I_c - 0.0385n + 0.0658} \approx 1.2534$$

It would appear that the keyword length is about $r \approx 1.25$, so perhaps $r = 1$ or $r = 2$.

b. The letter frequencies for the odd-positioned letters and for the even-positioned letters are sometimes quite different from each other; for instance, Y appears 21 times in an odd position but only 2 times in an even position. This would be highly unlikely if only a single ($r = 1$) Caesar cipher had been used, and also rules out odd key lengths. From a), it is unlikely that the key length is greater than 2, so even key lengths of 4 or more are highly unlikely. We conclude that the key length $r = 2$ is highly likely.

c. We need to guess 2 Caesar ciphers, for the odd and even letter positions, respectively. First, we could guess that, for the odd positions, the frequently occurring Y might be encrypt the letter E; this uses the Caesar cipher given by the letter U. Decrypting with this cipher all odd-positioned letters gives

```
TZEN  IYEF  EJEU  IHHW  RMSW  SSSW  RAEK  OXCS  EKAJ  CAPZ
EJST  AKEV  OFTZ  EDEL  TWRK  OXAC  EQWG  RVFG  RFES  RDYL
HJEW  HMNV  RWDQ  ESRK  TZEN  IYEF  EJEU  IHPW  ROAK  CGNK
IVEJ  EVUF  BJES  KSBD
```

Next, we could consider the most frequent letters in the even positions to guess the cipher for E; these are J, K, and W, each appearing 7 times and respectively corresponding to the Caesar ciphers given by F, G, and S. Trying out each of these to see whether they decipher the message into something meaningful, we find that the Caesar cipher given by S does the trick:

```
THEV  IGEN  EREC  IPHE  RUSE  SASE  RIES  OFCA  ESAR  CIPH
ERSB  ASED  ONTH  ELET  TERS  OFAK  EYWO  RDFO  RNEA  RLYT
HREE  HUND  REDY  EARS  THEV  IGEN  EREC  IPHE  RWAS  CONS
IDER  EDUN  BREA  KABL
```

The message is then

THE VIGENERE CIPHER USES A SERIES OF CAESAR CIPHERS BASED ON THE
LETTERS OF A KEYWORD[.] FOR NEARLY THREE HUNDRED YEARS THE VIGENERE
CIPHER WAS CONSIDERED UNBREAKABL[E.]

86.

a. If we call M the message matrix and C the cipher matrix, then $C = AM$, so we can decipher by calculating $M = A^{-1}C$ where A^{-1} is the inverse of A modulo 29:

$$A^{-1} = (8 \times 2 - (-3) \times (-7))^{-1} \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = (-5)^{-1} \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = (-6) \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 10 & 18 \\ 13 & 17 \end{pmatrix}$$

Here, we used that $5^{-1} = 6$ in $\mathbb{Z}_{29}$.

For the ciphertext $\mathbf{c} =$ `LUVBRU`, the cipher matrix is $C = \begin{pmatrix} 14 & 24 & 20 \\ 23 & 4 & 23 \end{pmatrix}$. The message matrix is then

$$M = A^{-1}C = \begin{pmatrix} 10 & 18 \\ 13 & 17 \end{pmatrix} \begin{pmatrix} 3 & 22 & 5 \\ 22 & 3 & 13 \end{pmatrix}$$

The message $\mathbf{m}$ was therefore `ATTACK`.

b. Here, the cipher matrix C and the message matrix M are as follows.

$$C = \begin{pmatrix} 28 & 26 & 5 & 11 & 11 & 8 & 28 \\ 4 & 25 & 18 & 3 & 28 & 23 & 0 \end{pmatrix} \qquad M = \begin{pmatrix} 10 & 14 & 17 & \cdots & m_{17} \\ 7 & 14 & m_{23} & \cdots & m_{27} \end{pmatrix}$$

Note that $C = AM$, and in particular that $C' = AM'$ where C' and M' are the 2×2 submatrices of C and of M given by the first two columns of these matrices:

$$C' = \begin{pmatrix} 28 & 26 \\ 4 & 25 \end{pmatrix} = \begin{pmatrix} -1 & -3 \\ 4 & -4 \end{pmatrix} \qquad M' = \begin{pmatrix} 10 & 14 \\ 7 & 14 \end{pmatrix}$$

To decode the ciphertext given by C, we want to calculate $M = A^{-1}C = (C'M'^{-1})^{-1}C = M'C'^{-1}C$. Let us first calculate C'^{-1}, noting that $16^{-1} = 20$ in $\mathbb{Z}_{29}$,

$$C'^{-1} = ((-1) \times (-4) - (-3) \times 4)^{-1} \begin{pmatrix} -4 & 3 \\ -4 & -1 \end{pmatrix} = 16^{-1} \begin{pmatrix} -4 & 3 \\ -4 & -1 \end{pmatrix} = 20 \begin{pmatrix} -4 & 3 \\ -4 & -1 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 7 & 9 \end{pmatrix}$$

Then

$$M = M'C'^{-1}C = \begin{pmatrix} 10 & 14 \\ 7 & 14 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 7 & 9 \end{pmatrix} \begin{pmatrix} -1 & -3 & 5 & 11 & 11 & 8 & -1 \\ 4 & -4 & 18 & 3 & -1 & -6 & 0 \end{pmatrix} = \begin{pmatrix} 10 & 14 & 17 & 24 & 20 & 4 & 6 \\ 7 & 14 & 7 & 7 & 27 & 17 & 27 \end{pmatrix}$$

The message $\mathbf{m}$ is `HELLO EVERYBODY.`

c. Yes (I would at least); meaningful messages would be very rare (just how rare can be a challenge for you to think about - or you can read the end of the chapter!).

87.

a. First, we see that $\phi(n) = \phi(19 \times 29) = \phi(19)\phi(29) = 18 \times 28 = 504$.

$$\begin{aligned} \texttt{H} \to 10 \equiv m \to m^e \to 10^{55} \equiv 409 \pmod{551} \\ \texttt{I} \to 11 \equiv m \to m^e \to 11^{55} \equiv 182 \pmod{551} \end{aligned}$$

We therefore send the ciphertext $\mathbf{c} = (409, 182)$.

b. Since $e^2 = 55^2 \equiv 1 \pmod{504}$, we see that $d \equiv e^{-1} \equiv e \equiv 55 \pmod{504}$. Therefore,

$$\begin{aligned} 302^d \equiv 302^{55} \equiv 17 \pmod{551} \to \texttt{O} \\ 241^d \equiv 302^{55} \equiv 13 \pmod{551} \to \texttt{K} \end{aligned}$$

The message is $\mathbf{m} = \texttt{OK}$.

88. First, we see that $\phi(n) = \phi(17 \times 23) = \phi(17)\phi(23) = 16 \times 22 = 352$.
Since $3e = 3 \times 235 \equiv 1 \pmod{352}$, we see that $d \equiv e^{-1} \equiv 3 \pmod{352}$.
Therefore,

$$\begin{gathered}
366^d \equiv 366^3 \equiv 15 \pmod{391} \to \texttt{M} \\
14^d \equiv 14^3 \equiv 7 \pmod{391} \to \texttt{E} \\
126^d \equiv 126^3 \equiv 20 \pmod{391} \to \texttt{R} \\
126^d \equiv 126^3 \equiv 20 \pmod{391} \to \texttt{R} \\
3^d \equiv 3^3 \equiv 27 \pmod{391} \to \texttt{Y} \\
249^d \equiv 249^3 \equiv 5 \pmod{391} \to \texttt{C} \\
258^d \equiv 258^3 \equiv 10 \pmod{391} \to \texttt{H} \\
126^d \equiv 126^3 \equiv 20 \pmod{391} \to \texttt{R} \\
148^d \equiv 148^3 \equiv 11 \pmod{391} \to \texttt{I} \\
30^d \equiv 30^3 \equiv 21 \pmod{391} \to \texttt{S} \\
45^d \equiv 45^3 \equiv 22 \pmod{391} \to \texttt{T} \\
366^d \equiv 366^3 \equiv 15 \pmod{391} \to \texttt{M} \\
58^d \equiv 58^3 \equiv 3 \pmod{391} \to \texttt{A} \\
30^d \equiv 30^3 \equiv 21 \pmod{391} \to \texttt{S}
\end{gathered}$$

The message is $\mathbf{m} = \texttt{MERRY CHRISTMAS}$.

89.

a.

$$\begin{gathered}
\texttt{HE} \to 10, 7 \to 10 \times 29 + 7 = 297 \equiv m \to m^e \to 297^{17} \equiv 1037 \pmod{1147} \\
\texttt{LL} \to 14, 14 \to 14 \times 29 + 14 = 420 \equiv m \to m^e \to 297^{17} \equiv 424 \pmod{1147} \\
\texttt{O\_} \to 17, 2 \to 17 \times 29 + 2 = 495 \equiv m \to m^e \to 495^{17} \equiv 991 \pmod{1147}
\end{gathered}$$

We therefore send the ciphertext $\mathbf{c} = (1037, 424, 991)$.

b. First, we see that $\phi(n) = \phi(1147) = \phi(31 \times 37) = \phi(31)\phi(37) = 30 \times 36 = 1080$.
In contrast to the previous questions, our simple guesses for d do not work, so we need to use a more systematic approach, for instance by using the Euclidean Algorithm backward and forwards on 1080 and 17:

$$\begin{gathered}
1080 = 63 \times 17 + 9 \\
17 = 1 \times 9 + 8 \\
9 = 1 \times 8 + 1
\end{gathered}$$

and so

$$\begin{aligned}1 &= 9 - 8\\ &= 9 - (17 - 9)\\ &= 2 \times 9 - 17\\ &= 2(1080 - 63 \times 17) - 17\\ &= 2 \times 1080 - 127 \times 17\end{aligned}$$

We see that $-127 \times 17 \equiv 1 \pmod{1080}$, so $d \equiv -127 \equiv 953 \pmod{1080}$: $\quad d = 953$.

90.

a. For $n = 10033$, $\lceil\sqrt{n}\rceil = 101$, so

t	$2t+1$	$s^2 = t^2 - n$	$s \in \mathbb{Z}$?
101	203	168	×
102	205	371	×
103	207	576	✓

so $t = 103$ and $s = \sqrt{576} = 24$, and $a = s + t = 127$ and $b = t - s = 79$. Both a and b are prime, so we have the following prime factorisation: $10031 = n = ab = 127 \times 79$.

b. $\phi(n) = \phi(10033) = \phi(127 \times 79) = \phi(127)\phi(79) = 126 \times 78 = 9828$.
To find d, we can test some simple guesses but if this does not work, then we can instead use the Euclidean Algorithm backward and forwards on 9828 and 1787:

$$\begin{aligned}9828 &= 5 \times 1787 + 893\\ 1787 &= 2 \times 893 + 1\end{aligned}$$

and so

$$\begin{aligned}1 &= 1787 - 2 \times 893\\ &= 1787 - 2 \times (9828 - 5 \times 1787)\\ &= 11 \times 1787 - 2 \times 9828\end{aligned}$$

We see that $11 \times 1787 \equiv 1 \pmod{9828}$, so $d \equiv 11 \pmod{9828}$: $\quad d = 11$.

c. Note that $c^d = 8695^{11} \equiv 3123 \pmod{10033}$ and that $3123 = 29^2 \times 3 + 29 \times 20 + 20$, so $(a_1, a_2, a_3) = (3, 20, 20)$; in other words, the key is `ARR`. We can now decode:

key	A	R	R	I	A	M	T	H	E	P	I	R	A	T	E	K
plaintext	I	A	M	T	H	E	P	I	R	A	T	E	K	I	N	G
ciphertext	I	R	D	B	H	Q	I	P	V	P	B	V	K	B	R	Q

Here, plaintext feedback was used, and the message was `I AM THE PIRATE KING`.

91.

a. $k \equiv g^e \equiv 15^7 \equiv 42 \pmod{53}$

b. Noting that $5^{-1} = 32$ in $\mathbb{Z}_{53}$ (which can be found by trial and error or by the Euclidean Algorithm),

$$\begin{aligned} y &= g^x = 15^5 \equiv 44 \pmod{53} \\ r &= y \equiv 5 \pmod{13} \\ s &= x^{-1}(h + er) \equiv 32(9 + 7 \times 5) \equiv 32 \times 44 \equiv 1 \pmod{13} \end{aligned}$$

Alice' signature is then $(5, 1)$.

c. Here, $r = 2$ and $s = 4$, and $s^{-1} = 4^{-1} = 10$ in $\mathbb{Z}_{13}$. Therefore,

$$\begin{aligned} u_1 &= s^{-1}h = 10 \times 10 \equiv 9 \pmod{13} \\ u_2 &= s^{-1}r = 10 \times 2 \equiv 7 \pmod{13} \\ z &= g^{u_1}k^{u_2} \equiv 15^9 \times 42^7 \equiv 8 \not\equiv 2 \equiv r \pmod{13} \end{aligned}$$

The message is not genuine.

92.

a. There are $|K| = 26^r$ keys, so $n_0 \approx \left\lceil \frac{\log_2(26^r)}{3.2} \right\rceil \approx \lceil 1.47r \rceil$

b. There are $|K| = 5^s \times 21^s = 105^s$ keys, so $n_0 \approx \left\lceil \frac{\log_2(105^s)}{3.2} \right\rceil \approx \lceil 2.10s \rceil$

c. There are $|K| = (26!)^r$ keys, so $n_0 \approx \left\lceil \frac{\log_2(26!)^r}{3.2} \right\rceil \approx \lceil 27.6r \rceil$

d. There are $|K| = 10!$ keys, so $n_0 = \left\lceil \frac{\log_2 10!}{3.2} \right\rceil = \lceil 6.81 \rceil = 7$

e. There are $|K| = 2^{56}$ keys, so $n_0 = \left\lceil \frac{\log_2 2^{56}}{3.2} \right\rceil = \left\lceil \frac{56}{3.2} \right\rceil = \lceil 17.5 \rceil = 18$

f. There are $|K| = 2^{512}$ keys, so $n_0 = \left\lceil \frac{\log_2 2^{512}}{3.2} \right\rceil = \left\lceil \frac{512}{3.2} \right\rceil = \lceil 160 \rceil = 160$

g. There are $|K| = 1024 \times 512 = 536576$ keys, so $n_0 = \left\lceil \frac{\log_2 536576}{3.2} \right\rceil = \lceil 167680 \rceil = 167680$