# <u>**Solutions to Assignment 2**</u>

Barr 2.3: 2, 3a, 3b, 4*, 7, 10*

2. The keywords PRIME MINISTER are to be used to construct a mixed cipher alphabet by columnar transposition.

(a) Obtain the cipher alphabet.

Using the procedure outlined on Page 85, we obtain the following:

```
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
P A K R Y B L Z I C O M D Q E F U N G V S H W T J X
```

(b)

`ITISM UCHEA SIERT OBECR ITICA LTHAN TOBEC ORREC T` is enciphered as

`IVIGD SKZRP GIRNV EARKN IVIKP MVZPQ VEARK ENNRK V`

(c)

`PFNRK RYRQV RDAPM DGPFN IQKIF MR` is deciphered as

`APREC EDENT EMBAL MSAPR INCIP LE`

3.

(a) Deciphered message: THREE MAY KEEP A SECRET IF TWO OF THEM ARE DEAD.

(b) EDUCATION HAS BECOME A PRISONER OF CONTEMPORANEITY. IT IS THE PAST, NOT THE DIZZY PRESENT, THAT IS THE BEST DOOR TO THE FUTURE.

4.* Following the procedure described from pages 85-90, the original plaintext is found to be: FOURSCORE AND SEVEN YEARS AGO OUR FATHERS BROUGHT FORTH ON THIS CONTINENT A NEW NATION CONCEIVED IN LIBERTY AND DEDICATED TO THE PROPOSITION THAT ALL MEN ARE CREATED EQUAL. Keyword: LINCOLN

7. Using the Polybius checkerboard, the deciphered quote reads: A SHORT SAYING OFT CONTAINS MUCH WISDOM.

10. Note that there are 26 possibilities for A, 25 possibilities for B, 24 possibilities for C and so on. Thus there are 26! = 403291461126605635584000000 = $4.03 \times 10^{26}$ possible substitution keys. The computer takes $10^{-9}$ seconds to check one key, so in the worst case scenario where the computer has to go through all 26! possibilities, it would take the computer $4.03 \times 10^{26}$ keys x $10^{-9}$ sec/key = $4.03 \times 10^{17}$ sec = $1.28 \times 10^{10}$ years.

B.1 Use Induction to show that $1^3+2^3+\ldots+n^3 = (1/4)n^2(n+1)^2$

Base case (Show statement holds for $n=1$):

$1^3 = 1$. $\quad 1/4\,(1)^2(1+1)^2 = 1/4\,(1)(4) = 1$.

$1 = 1$ ✓.

Next,

Assume statement holds for $n$. Show statement holds for $n+1$.

Statement holds for $n \Rightarrow 1^3+2^3+\ldots+n^3 = (1/4)n^2(n+1)^2$

What is required to show is $1^3+2^3+\ldots+n^3+(n+1)^3 = 1/4\,(n+1)^2((n+1)+1)^2$

$= 1/4\,(n+1)^2(n+2)^2$.

$1^3+2^3+\ldots+n^3 = (1/4)n^2(n+1)^2$ (By Assumption).

$$\begin{aligned}
\Rightarrow 1^3+2^3+\ldots+n^3+(n+1)^3 &= 1/4\,n^2(n+1)^2 + (n+1)^3 \\
&= (n+1)^2\left[1/4\,n^2 + n+1\right] \\
&= (n+1)^2 \frac{1}{4}\left[n^2+4n+4\right] \\
&= \frac{1}{4}(n+1)^2\left[(n+2)^2\right] \\
&= 1/4\,(n+1)^2(n+2)^2 \text{ As required}
\end{aligned}$$

Thus, by induction,

$1^3+2^3+\ldots+n^3 = (1/4)n^2(n+1)^2$ for all natural numbers $n$.

---

Note how the proof works. We proved the statement was true for $n=1$ and that if the statement is true for $n$, it is true for $n+1$.
So, since the statement is true for $n=1$ it is true for $n=2$ which in turn implies it is true for $n=3$, and so on.

B2* Evaluate the function $f(x) = x^2+x+41$ at $x=1,2,3$
Decide whether the value of $f(x)$ is prime for all natural numbers $x$.

$f(1) = 43$
$f(2) = 47$
$f(3) = 53$.

Now, $f(x)$ is prime for $x = 1, 2, \ldots, 39$. But that does not imply that $f(x)$ is prime for all natural numbers $x$.
Lets try and find a counter-example i.e. an $x$ for which $f(x)$ is not prime.
Instead of trying random $x$'s when trying to find an $f(x)$ that is not prime, simply note the following:

$$f(x) = x^2 + x + 41.$$

After staring at $f(x)$ for a while, it is clear that $f(41)$ will not be prime:

$$f(41) = 41^2 + 41 + 41 = 41(41+1+1).$$

41 divides the right hand side so, it must divide the left hand side, and so we know $f(41)$ is not prime.
On Inspection,

$$f(41) = 1763 = 41 \times 43.$$

So indeed $f(41)$ is not prime.

Thus having found a counter example, we have proved that $f(x)$ is not prime for all natural numbers $x$.