1. Consider the following PRAM CRCW algorithm FACTORIAL($L, n$) that stores the values $n \ldots 1$ in a singly-linked list $L$ on $n$ processors, where $y(i)$ refers to the number stored in processor $i$. The algorithm returns $n!$ using the List-Prefix approach.

```
FACTORIAL($L, n$)
1    while next(i) ≠ NIL for some processor i
2        foreach processor i, in parallel
3            if next(i) ≠ NIL
4                then
6        return y(n)
7    return y(n)
```

(a) (3 points) Show the two missing lines of pseudocode from the FACTORIAL algorithm above.
4: $y(next(i)) = y(i) \times y(next(i))$
6: $next(i) = next(next(i))$

(b) (3 points) Given the initial linked-list below for computing 5!, show the linked-list after each iteration of the main loop of FACTORIAL.

1. $5 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$
2. $5 \rightarrow 20 \rightarrow 12 \rightarrow 6 \rightarrow 2$
3. $5 \rightarrow 20 \rightarrow 60 \rightarrow 120 \rightarrow 24$
4. $5 \rightarrow 20 \rightarrow 60 \rightarrow 120 \rightarrow 120$

(c) (1 point) Give the asymptotic running time of the parallel FACTORIAL algorithm.
$\Theta(\lg n)$
(d) (1 point) Give the asymptotic running time of the best serial algorithm for computing $n!$.
   $\Theta(n)$

(e) (1 point) Give the speedup of the parallel FACTORIAL algorithm.
   Speedup = (best serial) / (parallel) = $\Theta(n)/\Theta(lg\ n) = \Theta(n/\ lg\ n)$

2. Suppose you select the two prime numbers $p = 11$ and $q = 13$ to generate public and secret keys in the RSA cryptosystem.

(a) (1 point) What is the formula and value of $n$?
   $n = pq = 143$

(b) (1 point) What is the formula and value of $\phi(n)$?
   $\phi(n) = (p - 1)(q - 1) = (10)(12) = 120$

(c) (2 points) What is the value of the smallest odd $e > 1$ that is relatively prime to $\phi(n)$ from part (b)? Show your work.
   Two numbers are relatively prime if their greatest common divisor (gcd) is 1.
   $\gcd(3,120) = 3$
   $\gcd(5,120) = 5$
   $\gcd(7,120) = 1$, so $e = 7$

(d) (2 points) What is the value of $d$ that is the multiplicative inverse of $e$ from part (c), modulo $\phi(n)$ from part (b)? Show your work.
   $d = 7^{-1} \mod 120 = 103$

(e) (2 points) Give the public and secret keys generated from the above scenario.
   Public key = $(e, n) = (7, 143)$
   Secret key = $(d, n) = (103, 143)$
3. Consider the string matching problem of finding all occurrences of pattern $P = abcab$ in the text $T = aaabcabad$, where $\Sigma = \{a, b, c, d\}$.

(a) (2 points) Give the prefix function $\pi$ for the pattern $P$.

\[
\begin{align*}
\pi[0] &= 0 \\
\pi[1] &= 0 \\
\pi[2] &= 0 \\
\pi[3] &= 1 \\
\pi[4] &= 2
\end{align*}
\]

(b) (2 points) Give the bad character function $\lambda$ for the pattern $P$ and alphabet $\Sigma$.

\[
\begin{align*}
\lambda[a] &= 4 \\
\lambda[b] &= 5 \\
\lambda[c] &= 3 \\
\lambda[d] &= 0
\end{align*}
\]

(c) (2 points) Give the good suffix function $\gamma$ for the pattern $P$.

\[
\begin{align*}
\gamma[0] &= 3 \\
\gamma[1] &= 3 \\
\gamma[2] &= 3 \\
\gamma[3] &= 3 \\
\gamma[4] &= 3 \\
\gamma[5] &= 1
\end{align*}
\]

(d) (1 point) Using the Knuth-Morris-Pratt algorithm how far is the pattern shifted after the first character mismatch?

The pattern is shifted by 1 after the first mismatch.

(e) (1 point) Using the Boyer-Moore algorithm how far is the pattern shifted after the first character mismatch?

The pattern is shifted by 2 after the first mismatch.