5.1)

a) $\Theta(n)$ because the for loop in line 5

b) $\Theta(n)$ because it returns $n+1$ digit number

c) Yes. Because the running time = output size $\rightarrow$ optimal

d) $\Theta(n^2)$ because nested for loop on line 2 and 4

e) $\Theta(n)$ because it returns 2N digit number

f) no because we do not know a multiplication algorithm that runs in $\Theta(n)$ time

g) $\Theta(n)$ because it has to look at every digit in both numbers (in the worst case)

h) $\Theta(n)$ because the logic is similar to the adding algorithm.

i) $\theta(n^2)$ because the repeat.... loop takes $\theta(n)$ and the for loop on line 9 takes $\theta(n)$

j) $\theta(\log n)$ because it converges quadratically

k) $\theta(n^2)$ because it takes $\theta(n^2)$ running time to perfom the Mod algorithm (multiplication and subtraction) and takes $\theta(n^2)$ running time to perform the DIV algorithm.

l) $\theta(n^3)$ because the for loop on line 3 takes $\theta(n)$ time. Mod and mutiply call take $\theta(n^2)$ time

m) $\theta(N^{\log_2 3})$: (the running time of Karatsuba's algorithm)

n) $\theta(N^{\log_2 3})$

o) $\theta(N^{\log_2 6})$. Powmod calls multiple and mod $\theta(n)$ times → running times $= \theta(n$

→ Total running time $= \theta(N \times N^{\log_2 3})$
$= \theta(N^{\log_2 6})$

k) KthRoot (A, K, N)

$t_0 =$ one (N) // $T_i = 2^i$

$i = 0$

repeat

$i \mathrel{+}= 1$
$t_1 =$ add (T_{i-1}, T_{i-1}, N)

until $t_i(N+1) > 0$ or powerexceeds
(t_i, K, A, N)

$R =$ Zero (N)

for $j = i-1$ downto 0

$r' =$ add (r, t_j)

unless powerexceeds (r', k, a, n)

$r = r'$

return r

5.2)

a) $\Theta(N^{\log_2 6})$ because $D(n)$ can be computed using a simple call to powmod

b) $\Theta\left(\frac{RC}{N}\right)$

c) $\Theta\left(RCN^{\log_2 3}\right)$

d) 0, 1, m-1 are fixed points

e) $E(-n) \equiv -E(n) \mod m$

$E(n_1) \cdot E(n_2) \equiv E(n_1 \times n_2) \mod m$

$E(n_1)^{n_2} \equiv E(n_1^{n_2}) \mod m$

f) Appending a random number and using per-message encryption keys both work because they make the encryption output non-deterministic. The other proposals will no change the fact that a message always loo the same after encryption .