Exercise 1:
In this exercise we consider two Diffie-Hellman-related schemes in the view of the Hidden Number Problem. In what follows we assume a group of prime order $p$ and $\alpha$ being its generator. We set $l = \sqrt{\log p + \log \log p}$. In all cases you should modify the proof of Satz 76.

1. **Key Sharing.** Bob picks a random $r \leftarrow \mathbb{Z}_p$ and send $\alpha^r$ to Alice. Alice picks a random $s \leftarrow \mathbb{Z}_p$ and sends $(\alpha^r)^s$ to Bob. Bob computes $(\alpha^r)^{s/r} = \alpha^s$ which is the shared key. Now $\mathcal{A}$ on input $(\alpha^{r(s+x)}, \alpha^r)$ outputs $l$ MSB of $\alpha^{s+x}$. Apply $\mathcal{A}$ to compute $\alpha^s$ efficiently.

2. **ElGamal Encryption.** For $pk = (p, \alpha, \beta = \alpha^a)$ and $sk = a$: $\operatorname{Enc}_{pk}(m) = (\alpha^r, m\beta^r)$ for some random $r \leftarrow \mathbb{Z}_p$. Let $\mathcal{A}$ be an algorithm that on input $\alpha^{a+x}, \alpha^r, m\beta^r$ outputs $l$ MSB of $m(\alpha^{-r})^x$. Show how to compute $m$ in polynomial time using $\mathcal{A}$.

Exercise 2:
Let $N = p^k$ be a prime-power. Show how to find $k$ and $p$ efficiently.

Exercise 3:
Factor $N = 52907$ using $B = \{2, 3, 5\}$. 