Homework-3 (CS 513)

Due date: November 16 (in the beginning of class)

Collaboration is encouraged. However the writeup should be your own. If you use any resources such as books or the internet, you should make sure you mention this in the homework. If you collaborate with other students then make sure you acknowledge your collaborators.

1. (a) Let $x$ and $y$ be positive $n$-bit integers. Give an algorithm that runs in time polynomial in $n$ that finds a positive integer $z$ (if it exists) such that $x = y^z$.
   
   (b) Let $x$ and $z$ be positive $n$-bit integers. Give an algorithm that runs in time polynomial in $n$ that finds a positive integer $y$ (if it exists) such that $x = y^z$.
   
   (c) Let $x$ be a positive $n$-bit integer. Give an algorithm that runs in time polynomial in $n$ that finds integers $y$ and $z$ (both strictly greater than 1), if they exist, such that $x = y^z$.

2. For an integer $n$, let $\mathbb{Z}_n^*$ denote the set of integers between 1 and $n$ that are coprime to $n$. We say that an integer $a$ is a Fermat witness for compositeness of $n$ if $a^{n-1} \not\equiv 1 \pmod{n}$. Suppose that there exists some $a \in \mathbb{Z}_n^*$ which is a Fermat witness for compositeness of $n$. Then show that there are at least $|\mathbb{Z}_n|/2$ of the numbers between 1 and $n$ are Fermat witnesses for compositeness of $n$. (There were some details missing in the proof that was provided in class.)

3. Consider the following scheme (it is a variation of the Diffie-Hellman-Merkle key exchange protocol) for Alice to send a message to Bob. Alice and Bob agree on a large prime $p$ that is $n$ bits long. Alice wants to send a message $m$ to Bob, where $m$ is a positive integer less than $p$. Alice picks a secret integer $e_A$ such that $e_A$ is coprime to $p - 1$. She also computes $d_A$, where $d_A$ is the inverse of $e_A$ modulo $p - 1$. Bob picks a secret integer $e_B$ such that $e_B$ is coprime to $p - 1$. Alice sends $m_A$ such that $m_A \equiv m^{e_A} \pmod{p}$ to Bob. Bob then computes $m_B \equiv m_A^{e_B} \pmod{p}$ and sends it to Alice. Alice computes $m^* \equiv m_B^{d_A} \pmod{p}$ and sends $m^*$ to Bob. From this exchange, is Bob able to recover the original message that Alice was trying to send to Bob? Is so, prove why Bob is able to efficiently recover the message. If not, then discuss why it might be difficult for Bob to recover the message. Is an eavesdropper able to recover the message?