Cryptographic Protocols

Exercise 5

5.1 Generic Zero-Knowledge Proofs of Knowledge

Construct zero-knowledge proofs of knowledge for the following settings:

a) Let $m$ be an RSA modulus and $e_1, e_2 \in \mathbb{Z}_m$ such that $e_1 + e_2$ is prime. Let $z \in \mathbb{Z}_m^*$. Peggy wants to prove to Vic that she knows a pair $(x, y) \in \mathbb{Z}_m^* \times \mathbb{Z}_m^*$, such that $z = x^{e_1} y^{e_2}$.

b) Let $H$ be a cyclic group of prime order $q$ and let $h_1, h_2, h_3$ be three generators. Peggy wants to prove to Vic that for two values $z_1, z_2 \in H$ she knows values $x_1, x_2, x_3, x_4 \in \mathbb{Z}_q$ such that $z_1 = h_1^{x_3} h_2^{x_1}$ and $z_2 = h_1^{x_2} h_2^{x_4} h_3^{x_1}$.

5.2 RSA-Based Bit Commitments

Let $m = pq$ be an RSA modulus and $e$ be a (publicly known) prime.

a) Let $x \in \{0, 1\}$ and consider the following protocol between two (polynomially bounded) parties $P$ and $V$ that consists of two phases:

- **COMMIT:** $P$, on input $x$, chooses $r \in \mathbb{Z}_m^*$ such that $\text{LSB}(r) = x$ (where $\text{LSB}(r)$ denotes the least significant bit of $r$), computes $c := r^e \in \mathbb{Z}_m^*$, and sends $c$ to $V$.

- **OPEN:** $P$ sends $(r, x)$ to $V$, who verifies that $r^e = c$ and that $\text{LSB}(r) = x$.

Prove the following properties of the above protocol:

i) Show that after the COMMIT phase $V$, there exists $x' \in \{0, 1\}$ such that $V$ will only accept pairs $(r', x')$ in the OPEN phase.

ii) One can show that guessing the least significant bit of an RSA ciphertext (with probability substantially better than $1/2$) is as hard as computing the entire ciphertext. Use this fact to argue that $V$ cannot guess which bit $x$ was used by $P$ in the COMMIT phase.

b) Let $\mu \in \mathbb{Z}_m^*$ be a public ciphertext for which $P$ does not know the decryption. Consider the following protocol between two (polynomially bounded) parties $P$ and $V$ that consists of two phases:

- **COMMIT:** $P$, on input $x$, chooses $r \in \mathbb{Z}_m^*$, computes $c := r^e \mu^x$ in $\mathbb{Z}_m^*$, and sends $c$ to $V$.

- **OPEN:** $P$ sends $(r, x)$ to $V$, who verifies that $c = r^e \mu^x$.

Prove the following properties of the above protocol:

i) Show that after the COMMIT phase $V$, there exists $x' \in \{0, 1\}$ such that $V$ will only accept pairs $(r', x')$ in the OPEN phase.

ii) Argue that $V$ cannot guess which bit $x$ was used by $P$ in the COMMIT phase.
c) What happens in the above protocols if the factorization of $n$ is known to $P$ and what if it is known to $V$? What are the differences between the two protocols in terms of their security guarantees?