Name:

Purdue E-mail:

I collaborated with (...). I affirm that I wrote the solutions in my own words and that I understand the solutions I am submitting.

Homework 5

Due date: Thursday, November 29th 3:00 PM

Question 1 (20 points)

Consider a variant of the Fiat-Shamir transform (Construction 12.9 page 454) in which the signature is (I, s) rather than (r, s) and verification is changed in the natural way. Show that if the underlying identificaiton scheme is secure, then the resulting signature scheme is secure here as well

Question 2 (20 points)

Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ be a signature scheme. In this problem we will show how to obtain a signature scheme $(\mathsf{Gen}', \mathsf{Sign}', \mathsf{Ver}')$ with a *shorter* public key using a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^\ell$. We will assume that H is a random oracle.

- $\mathsf{Gen}'(1^n)$ runs $\mathsf{Gen}(1^n)$ to obtain (pk, sk) with $pk \in \{0,1\}^n$ and then outputs $pk' = H(pk)$ and $sk' = (pk, sk)$. Explain how the algorithms Sign' and , Ver' work.
- Suppose that $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ is a (t, q_{sign}, ϵ)-secure signature scheme meaning that any attacker running in time t and making at most q_{sign} queries to the signature oracle wins the signature forgery game with probability at most ϵ. Show that $(\mathsf{Gen}', \mathsf{Sign}', \mathsf{Ver}')$ is $(t', q_{sign}, q_{oracle}, \epsilon')$-secure with $t' = t - O(q_{sign}n)$ and $\epsilon' = \epsilon - \frac{q_{oracle}}{2^\ell}$ meaning that any attacker running in time t' making at most q_{sign} (resp. q_{oracle}) queries to the signing oracle Sign' (resp. random oracle $H(\cdot)$) wins the signature forgery game with probability at most ϵ'.

Question 3 (20 points)

Let $pk = (N, e = 7)$ (resp. $sk = (N, d)$) denote the public (resp. private) key in a plain RSA signature scheme. Define the function $\mathbf{Int} : \{0,1\}^* \to \mathbb{Z}_N^*$ as follows

$$\mathbf{Int}\left(x_1 \| ... \| x_n\right) = \sum_{i=1}^{n} 2^{n-i} x_i$$

on input string $x = (x_1 \| ... \| x_n) \in \{0,1\}^n$ and let μ denote an ASCII character to byte mapping in which $\mu(0) = 0^8, \mu(1) = 0^7 1, \mu(2) = 0^6 10, \ldots, \mu(9) = 0^4 1001$. Given an ASCII message $m = m_1, \ldots, m_n$ we define $\mathbf{Encode}(m) = \mathbf{Int}\left(\mu(m_1) \| ... \| \mu(m_n)\right)$.

Finally, for and ASCII message m we can set

$$\mathbf{Sign}_{sk}(m) = \mathbf{Encode}(m)^d \mod N \ .$$

Suppose Alice signs the message $m =$ "Please pay Bob the following amount from my bank account (USD): 50". Suppose that Bob obtains $\sigma = \mathbf{Sign}_{sk}(m)$. Explain how Bob can obtain a signature σ' authorizing the bank to transfer more than \$50. How much money can Bob make? Assume that the Bank denies transfers above 750 million (USD) without in person authorization. You may assume that $\mathbf{Encode}(m) < N/2^{64}$.

Question 4 (20 points)

Consider the following Zero-Knowledge Proof for the the DDH problem. In particular, Bob (prover) and Alice (Verifier) are both given a triple (X, Y, Z) where $X, Y, Z \in \langle g \rangle$ are all elements of a cycle group of prime order p. Bob is also given $x, y, z = xy$ such that $X = g^x, Y = g^y$ and $Z = g^z$ and wishes to prove to Alice in Zero-Knowledge that (X, Y, Z) is a DDH triple. Consider the following protocol. 1) Bob picks random integer r_1 and r_2 and sends the triple (X_1, Y_1, Z_1) to Alice where $X_1 = g^{r_1+x}$, $Y_1 = g^{r_2+y}$ and $Z_1 = g^{(r_1+x)(r_2+y)}$. 2) Alice sends a challenge bit b to Bob. 3) Bob reveals $e = r_1 + bx \mod p$ and $f = r_2 + by \mod p$ to Alice. 4) Alice accepts if and only if $X_b = g^e, Y_b = g^f$ and $Z_b = g^{ef}$ where $X_0 := X_1/X$, $Y_0 := Y_1/Y$ and $Z_0 := Z_1/(ZX^fY^e)$.

(a) (2 points) Prove that the protocol is complete.

(b) (3 points) Prove that the protocol is sound in the sense that the probability Alice accepts when (X, Y, Z) is not a DDH triple is at most $\frac{1}{2}$.

(c) (5 points) Prove that the protocol is zero-knowledge (Your proof should work even if the verifier behaves maliciously).

(d) (10 points) Using the Fiat-Shamir paradigm develop a non-interactive version of the above Zero-Knowledge proof (NIZK) in the random oracle model. Your protocol should be complete and should have soundness $2^{-\ell}$ for a security parameter ℓ against any attacker making at most 2^ℓ queries to the random oracle. You should also prove that your protocol is ZK by showing that a simulator can produce an identical looking proof without knowledge of x, y, z (Hint: the simulator should exploit program-ability).

Question 5 (20 points)

Suppose that Alice has a secret bits a_1 and a_2 and that Bob has a secret bits b_1, b_2 and that Alice and Bob want to compute the function $h(a_1, a_2, b_1, b_2) = (b_1 \wedge (b_2 \oplus a_1), (b_2 \vee b_1) \oplus a_1)$ using Yao's Garbled Circuit protocol.

(a) Suppose that Alice selects several random permutations $\pi_1, \pi_2, \ldots, \pi_{100} : \{(0,0), (0,1), (1,0), (1,1)\} \rightarrow \{(0,0), (0,1), (1,0), (1,1)\}$. Write down a garbled circuit that Alice could sends Bob in terms of these permutations. (Note: You do not need to use all 100 permutations in your solution).

(b) Suppose that Alice is malicious, but Bob behaves honestly during the execution of the protocol. Write down a garbled circuit that Alice can send Bob to extract *both* secret bits b_1 and b_2.