CSE 5014: Cryptography and Network Security
2023 Spring Semester Written Assignment # 4
Due: May 30th, 2023, please submit at the beginning of class

Q.1 Let (Gen_1, H_1) and (Gen_2, H_2) be hash functions from which *at least one* is collision-resistant. Decide for the following constructions whether the resulting hash function is *necessarily* collision-resistant and prove your answer (we assume that Gen runs Gen_1 and Gen_2 to obtain a key (s_1, s_2)).

1. $H_a^{(s_1,s_2)}(x) := H_1^{s_1}(x)||H_2^{s_2}(x)$
2. $H_b^{(s_1,s_2)}(x) := H_1^{s_1}(H_2^{s_2}(x))||H_2^{s_2}(H_1^{s_1}(x))$
3. $H_c^{(s_1,s_2)}(x) := H_1^{s_1}(H_2^{s_2}(x)||x)||H_2^{s_2}(H_1^{s_1}(x)||x)$

Q.2 Let (Gen, H) be a collision-resistant hash function with inputs of arbitrary size. We define a MAC for arbitrary-length message by

$$Mac_{s,k}(m) = H^s(k||m).$$

Show that this is not a secure MAC if H is constructed by the Merkle-Damgard transform from an arbitrary collision-resistant hash function h. (Assume that s is known to the attacker)

Q.3

1. We say that a number $y \in \mathbb{Z}_n^*$ is a quadratic residue (QR) if $y = x^2$ for some $x \in \mathbb{Z}_n^*$. Prove that the set of QRs is a subgroup of $\mathbb{Z}_n^*$.
2. Let $p > 1$ be a prime. It can be shown that $\mathbb{Z}_p^*$ is a cyclic group, that is, there exists a generator $g \in \mathbb{Z}_p^*$ such that $\mathbb{Z}_p^* = \{g^1, g^2, \ldots, g^{p-1}\}$. For $y \in \mathbb{Z}_p^*$, let $\log_g(y)$ denote the smallest nonnegative integer i for which $g^i = y$. For example $\log_g(1) = 0$, and $\log_g(g) = 1$. Show that y is a QR in $\mathbb{Z}_p^*$ if and only if $\log_g(y)$ is an even number.

Q.4

The discrete logarithm problem is easy in $\mathbb{Z}_N$ for any integer N and for any generator. Explain this.

Q.5

Consider the cyclic group $\mathbb{Z}_{17}^* = \{1, 2, \ldots, 16\}$ and the mapping f defined by $f(x) = x^2 \bmod 17$ for all x in the group.

1. What is the size of the image set of f, i.e., the set $S = \{f(x) : x \in \mathbb{Z}_{17}^*\}$?
2. How many generators are there in $\mathbb{Z}_{17}^*$?
3. Pick a generator g. What is the probability that, for a randomly chosen $a, b \in \{0, 1, \ldots, 15\}$, the value of g^{ab} is in S?

Q.6

When p and q are distinct odd primes and $N = pq$, the elements in $\mathbb{Z}_N^*$ have either 0 or 4 square roots. A quarter (1/4) of the elements have 4 square roots; the rest have no square root. The four square roots of $x \in \mathbb{Z}_N^*$ look like $\pm a, \pm b$ (of course, $-a$ means $N - a$ since we always work modulo N). Suppose that you are given an efficient deterministic algorithm A that, on input x that has square roots, finds some square root. (If x does not have a square root, it returns $\perp$.)

Use A to make an efficient *probabilistic* algorithm A' that factors N. (Hint: If you can find two square roots of a number, call them a and b, which are not of the form $a = \pm b \bmod N$, then you can factor N. Show how.] **Note**: you only get to call A as a black-box, so you don't know a *priori* which of the square roots it will find.

Q.7 Show that the regular RSA signature scheme is *arbitrarily forgeable* (forging the signature of any challenge message m) if the attacker is allowed to ask the signing oracle. Note that the challenge message m cannot be queried to the signing oracle. (Recall that the RSA signature is $m^d \bmod N$, where d is the private key and $N = pq$)

Q.8 Describe the discrete logarithm problem, Computational Diffie-Hellman (CDH) problem, and Decisional Diffie-Hellman (DDH) problem, respectively. State also the relation of the three assumptions of these three problems, i.e., which one is stronger than another.

Q.9 Recall the El Gamal encryption scheme: the public key is (p, g, h), where g is a generator of $\mathbb{Z}_p^*$ and $h = g^x$, and the private key is x; the encryption scheme is $Enc(m) = (g^y, h^y \cdot m)$, where $y \leftarrow_R \mathbb{Z}_p^*$; the decryption scheme is $Dec(c_1, c_2) = c_2/c_1^x$. The El Gamal signature scheme is: To sign on a message m, $k \leftarrow_R \mathbb{Z}_p^*$ with $\gcd(k, p-1) = 1$,

$$\sigma = Sign_{sk}(m) = (r, s) = (g^k, k^{-1}(m - rx) \bmod (p-1)).$$

To verify a signature $\sigma = (r, s)$, it is accepted if $h^r r^s = g^m$.

(1) Show that El Gamal encryption scheme is *not* secure against the chosen ciphertext attack.

(2) Is El Gamal signature scheme secure against the chosen message attack (allowing to ask the signing oracle) if the *hash-and-sign paradigm* is used.

(3) Assume that the hash-and-sign paradigm is *not* used. Can we forge a signature for any given message m by asking the signing oracle. Note that you cannot ask the oracle about the signature of m.