1. Let $(Gen, H)$ be a collision-resistant hash function. Is $(Gen, \tilde{H})$ defined by $\tilde{H}'(x) = H'(H'(x))$ necessarily a collision-resistant hash function? Justify your answer.

2. Before HMAC, it was common to define a MAC for arbitrary-length message by $Mac_{s,k}(m) = H'(k || m)$ where $H$ is a collision-resistant hash function. Show that this is not a secure MAC if $H$ is constructed via the Merkle-Damgard transform. (Assume the hash key $s$ is known to the attacker, and only $k$ is kept secret. The underlying compression function $h$ is also known to the attacker.)

3. In an RSA encryption scheme, the public key of a user is $e = 31, N = 3599$. What is the private key of this user?

4. In a public-key system using RSA, you intercept a ciphertext $c = 60$ sent to a user whose public key is $N = 155$ and $e = 7$. What is the plaintext $m$?

5. Fix the RSA modulus $N$, and assume there is an adversary $A$ running in time $t$ for which

   $\Pr\left[ A\left(x^e \mod N\right) = x : x \leftarrow \mathbb{Z}_N^* \right] = 0.01.$

   That is, $A$ can decrypt the ciphertext of a random message $x$ with probability 0.01. Construct an adversary $A'$ for which

   $\Pr\left[ A'\left(x^e \mod N\right) = x : x \leftarrow \mathbb{Z}_N^* \right] \geq 0.99.$

   That is, $A'$ can decrypt the ciphertext of a random message $x$ with probability $\geq 0.99$. The running time $t'$ of $A'$ must satisfy $t' \leq \text{poly}(t, \log N)$.

   Hint: use the homomorphism property of RSA.