1. (Hash-then-encrypt MAC). Let H be a collision-resistant hash defined over (M, X), and let $\mathcal{E} = (E, D)$ be a secure block cipher defined over (K, X). Show that the encrypted-hash MAC system (S, V) defined by $S(k, m) := E(k, H(m))$ is a secure MAC. (HINT: Use Theorem 8.1) [4 points]

> As $\mathcal{E} = (E, D)$ be a secure block cipher defined over (K, X), we have two secure $PRFs$, one of which is $E(k, m)$. Any secure PRF can be directly used to build a secure MAC. Then we have a secure MAC $I' = (S', V')$ over (K, X) where:
>
> $$S'(k, m) := E(k, m)$$
> $$V'(k, m, t) := \begin{cases} \text{accept} & \text{if } E(k, m) = t \\ \text{reject} & \text{otherwise} \end{cases}$$
>
> Then We can define a MAC $I = (S, V)$ over (K, M, X) as follows, $t, H(m) \in X$:
>
> $$S(k, m) := S'(k, H(m)) = E(k, H(m)) \quad V(k, m, t) := V'(k, H(m), t) = V'(k, H(m), t) \quad (1)$$
>
> MAC system I' is a secure MAC and the hash function H is collision resistant. Then the dereived MAC system $I = (S, V)$ defined by $S(k, m) := E(k, H(m))$ is a secure MAC.

2. Why is the Merkel-Damgard construction considered to be more secure than traditional hash function constructions, even though both use the “block-chaining” technique to produce a fixed-size output from a potentially large input? [3 points]

> Merkel-Damgard construction uses padding blocks to handle the variable length of the inputs, which increase the property of the collision-resistant and the security for some types of attacks.

3. Assume that $H_1, H_2 : \{0, 1\}^* \to \{0, 1\}^n$ are collision-resistant hash functions. Is the composition of collision-resistant functions $H_3(x) = H_2(H_1(x))$ collision resistant? [3 points]

> H_1 is collision-resistant, so it is difficult to find x_1, x_2 such that $H_1(x_1) = H_1(x_2)$
>
> H_2 is collision-resistant, so it is difficult to find y_1, y_2 such that $H_2(y_1) = H_2(y_2)$
>
> Let $y_1 = H_1(x_1), y_2 = H_2(x_2)$, so it is difficult to find x_1, x_2 such that $H_2(H_1(x_1)) = H_2(H_1(x_2))$.
>
> Therefore, it is still collision-resistant for $H_3(x) = H_2(H_1(x))$.