1 Chapter 12

1.1 Problem.2

Solution: We assume that the one-way function does not exists. Then for any function $f : \{0,1\}^* \to \{0,1\}^*$, there exists a PPT algorithm that can inverts f.
In a one-time one bit signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$. *Gen* generates a public-private key pair (pk, sk) with a security parameter 1^λ. *Sign* takes as input a bit b and the private key sk and outputs the signature σ. Ver takes as input a bit b, a public key pk and the signature σ, and only outputs 1 when σ is a valid signature of b.
If one-way function does not exists, we can construct an algorithm $\mathcal{A}$ to attack the one-time one bit signature scheme Π as follows:

1. Run $\mathsf{Gen}(1^\lambda)$ to generate a key pair (sk, pk).
2. Choose a random bit $b \in_R \{0,1\}$, and ask the signature oracle $\sigma \leftarrow \mathsf{Sign}(sk, b)$.
3. According to the signature σ as output, calls a invert algorithm to invert the *Sign* algorithm, which returns sk in polymal time.
4. Computes with $\sigma' \leftarrow Sign(sk, 1-b)$ and uses $(1-b, \sigma)$ as the input of the Ver algorithm, which return 1 with probability 1.

Thus, we conclude that if one way function does not exists, then secure one-time signature scheme can't exists, which proves the theory.