1

1.a

Given a message-signature pair (m, σ) we can easy forge a new pair: $(m-1, f(\sigma))$ which is valid:

$$f^{n-(m-1)}(x) = f^{n-m+1}(x) = f(f^{n-m}(x)) = f(\sigma)$$

1.b

Assume by contradiction that f^k is not OWP, i.e. there is an adversary A' s.t. $\Pr_x\left[A'(f^k(x)) = x\right] \geq \varepsilon$. Then we construct and adversary A as follows: given $y = f(x)$:

1. Calculate $x' = A'(y)$
2. Calculate and return $f^{k-1}(x')$

Indeed, if A' inverts f^k successfuly, then:

$$x' = f^{-k}(y) = f^{-k}(f(x)) = f^{-k+1}(x)$$

And thus the second step yields: $f^{k-1}(f^{-k+1}(x)) = f^0(x) = x$.
A runs in polinomial time because k is polynomial in. Therefore A is a PPT adversary that inverts f with probability $\geq \varepsilon$, which is a contradition to f being a OWP. Therefore f^k is a OWP.

1.c

Assume by contradiction that there is an PPT adversary A that for every $x \in \{1, \ldots, n\}$, given $(m, \sigma = f^{n-m}(x))$, outputs $\left(m', \sigma' = f^{n-m'}(x)\right)$ where $m' > m$. Denote $k := m' - m > 0$. Note that:

$$f^k(\sigma') = f^{m'-m}(\sigma') = f^{m'-m}(f^{n-m'}(x)) = f^{n-m}(x) = \sigma$$

Therefore $\sigma' = f^{-k}(\sigma)$. But by (1.b) f^k is a OWP. This will lead to a contradition.
Construct A' to invert f^k as follows: given some $\sigma = f^k(\sigma')$:

1. For each $m \in \{1, \ldots, n\}$ check if $f^m(\sigma) = y$.
   (a) When a match is found continue.
   (b) If all checks failed, then stop.
2. Calculate $(m', \sigma') = A(m, \sigma)$
3. return σ'

If A' finds a match in step 1 then: $f^n(x) = y = f^m(\sigma)$, Therefore: $\sigma = f^{n-m}(x)$, i.e. $\sigma$is a signature of m. Thefore the pair given to A in step 2 is valid. If A succeeds, then A' indeed returns the correct σ'. Also note that step 1 takes polynomial time in n.
XXXX

1.d

We will require an additional OWP g. Set $y' = g^n(x)$. Modify the signature of message m to be $(f^{n-m}(x), g^m(x))$. The verification of a pair $(m, (\sigma_1, \sigma_2))$ will be to check that $f^m(\sigma_1) = y$ and that $g^{n-m}(\sigma_2) = y'$. Indeed, if (σ_1, σ_2) is a correct signature of m then:

$$f^m(\sigma_1) = f^{m+n-m}(x) = f^n(x) = y$$
$$g^{n-m}(\sigma_2) = g^{n-m+m}(x) = g^n(x) = y'$$

The first part of the signature pair is exaclty like in the original scheme, and the second part “doesn’t give information” over the first part. Therefore the proof of (1.c) will still hold, preventing forging of sigmatures for $m' > m$. The second part of the signature works in a similar way to prevent forging messages $m' < m$. Therefore this is indeed a one-time signature scheme.