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

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

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.

4.a

Assume $y \notin QR$. Let P^* be a prover, and let z be the number it sends in the first step. Note that:

$$\left(\frac{zy}{N}\right) = \left(\frac{z}{N}\right)\overbrace{\left(\frac{y}{N}\right)}^{=-1} = -\left(\frac{z}{N}\right)$$

Where the symbols above are jacobi symbols. Therefore if z is a QR, then $\left(\frac{zy}{N}\right) = -1$, meaning that zy is not a QR. Now see:

$$\Pr\left[\text{V accepts}\right] = \frac{1}{2}\Pr\left[a_0^2 \equiv z \mid b = 0\right] + \frac{1}{2}\Pr\left[a_1^2 \equiv zy \mid b = 1\right]$$

$$\Pr\left[a_0^2 \equiv z \mid b = 0\right] = \Pr\left[a_0^2 \equiv z \mid b = 0 \wedge z \in QR\right]\Pr\left[z \in QR\right] + \overbrace{\Pr\left[a_0^2 \equiv z \mid b = 0 \wedge z \notin QR\right]}^{=0}\Pr\left[z \notin QR\right]$$

$$\Pr\left[a_1^2 \equiv zy \mid b = 1\right] = \overbrace{\Pr\left[a_1^2 \equiv zy \mid b = 1 \wedge z \in QR\right]}^{=0}\Pr\left[z \in QR\right] + \Pr\left[a_1^2 \equiv zy \mid b = 1 \wedge z \notin QR\right]\Pr\left[z \notin QR\right]$$

The three equiations are from the law of total probality. The zero term in the second line is because z is not a QR, therefore it has no square root. The zero term in the second line is because z is a QR, and as noted at the begining, that implies that zy is not a QR. To summerize:

$$\begin{aligned}\Pr\left[\text{V accepts}\right] &= \frac{1}{2}\left(\overbrace{\Pr\left[a_0^2 \equiv z \mid b = 0 \wedge z \in QR\right]}^{\leq 1}\mathbb{I}_{z\in QR} + \overbrace{\Pr\left[a_1^2 \equiv zy \mid b = 1 \wedge z \notin QR\right]}^{\leq 1}\mathbb{I}_{z\notin QR}\right) \\ &\leq \frac{1}{2}\left(\mathbb{I}_{z\in QR} + \mathbb{I}_{z\notin QR}\right) = \frac{1}{2}\cdot 1 = \frac{1}{2}\end{aligned}$$

4.b

Define $S(y, b)$:

1. Sample $\tilde{r} \leftarrow \mathbb{Z}_N^*$, send $\tilde{z} = \tilde{r}^2 \mod N$
2. If $b = 0$ send $\tilde{a_0} = \tilde{r}$
3. If $b = 1$ sample and send $\tilde{a_1} \leftarrow \mathbb{Z}_N^*$

Obviously $\tilde{z} \approx z$. Need to show that $\tilde{a_b} \approx a_b$. Obviously $\tilde{a_0} \approx a_0$, so it remains to show that $\tilde{a_1} \approx a_1$.
xr is unoformly distributed over $\mathbb{Z}_N^*$ since $r \leftarrow \mathbb{Z}_N^*$ and x is non-random (formal proof similar to the solution of HW1 Q3a).
Therefore $a_1 = xr \approx \tilde{a_1}$.

XXXXX this solution is incorrect since the joint distibution is not indistinguishable. Jonathan's solution is correct...

6.a

We will generate $\{a_i\}_{i=1,\ldots,n}$ by drawing $a_i \leftarrow \mathbb{Z}_p^*$ for $i = 1, \ldots n-1$, and set:

$$a_n = n - (a_1 + \ldots + a_{n-1}) \pmod{\phi(p) = p-1}$$

Note that this gives us:

$$a_1 + \ldots + a_n \equiv a \pmod{\phi(p) = p-1}$$

We will use these values as $\{sk_i\}$. Given a cipher $c = (c_1, c_2)$ each student i will compute:

$$sk_{i,c} = \left(c_1^{-1}\right)^{a_i}$$

Together, all of the students combined can decrypt the message as follows:

$$D_{\{sk_{i,c}\}}(c_1, c_2) = c_2 \prod_{i=1}^{n} sk_{i,c}$$

Indeed, if $c = \left(g^k, m\beta^k\right)$ then:

$$\begin{aligned}
D_{\{sk_{i,c}\}}\left(g^k, m\beta^k\right) &= m\beta^k \prod_{i=1}^{n} \left(\left(g^k\right)^{-1}\right)^{a_i} \\
&= m\beta^k \prod_{i=1}^{n} g^{-ka_i} \\
&= m\beta^k g^{-k\sum_{i=1}^{n} a_i} \\
&\equiv m\beta^k g^{-ka} \\
&= m\left(g^a\right)^k g^{-ka} \\
&= mg^0 \\
&= m
\end{aligned}$$

Note that this scheme is resistant to coalitions of size $< n$. For the coalition $\{1, \ldots, n-1\}$ it is obvious because $a_1, \ldots, a_{n-1}$ are completely random and by themselves are unrelared to the secret a. For a different coalition e.g. $\{2, \ldots, n\}$ the proof is similar to the case of n-out-of-n Secret Sharing as seen in lecture 11, slide 28.