① 1. Given a hash fct. $H : \{0,1\}^* \to \{0,1\}^n$ and a secure (EUF-CMA) digital sign. scheme $\Sigma = (\Sigma.\text{KeyGen}, \Sigma.\text{Sign}, \Sigma.\text{Ver})$ for messages of length n bits, we build a DSS for arbitrary-length messages. We denote the scheme by $\Pi = (\text{KeyGen}, \text{Sign}, \text{Ver})$ s.t. $\text{KeyGen} = \Sigma.\text{KeyGen}$ outputs a pair (sk, vk),

$\text{Sign}(sk, m) = \Sigma.\text{Sign}(sk, H(m))$ where $m \in \{0,1\}^*$,

$\text{Ver}(vk, m, \sigma) = \Sigma.\text{Ver}(vk, H(m), \sigma)$ where σ is a signature.

2. Now, we want to show that Π is EUF-CMA secure assuming that Σ is secure and H is collision resistant. Let $\mathcal{A}$ be an adv. that aims to break Π, i.e.,

$\mathcal{A}$ wins if it outputs a pair (m, σ) s.t. $\text{Ver}(vk, m, \sigma) = 1$ for $(sk, vk) \leftarrow \text{KeyGen}$ and $m \notin \mathcal{L}_\Pi$, where $\mathcal{L}_\Pi$ is the list of messages that $\mathcal{A}$ queries to the oracle ($\mathcal{L}_\Pi = \{(m_i, \sigma_i)\}_{i \in I}$).

To each message m_i in $\mathcal{L}_\Pi$ we can assoiate an hash $H(m_i)$ by doing so we create a second list $\mathcal{L}_\Sigma$. We notice that if (m_i, σ_i) is a valid signature for Π, then $(H(m_i), \sigma_i)$ is a valid signature for Σ. When $(m, \sigma) \notin \mathcal{L}_\Pi$ and it is a valid signature, we have two possibility:

1. $H(m) \notin \mathcal{L}_\Sigma$. In this case, $(H(m), \sigma)$ is a forgery for Σ.
2. $H(m) \in \mathcal{L}_\Sigma$. In this case, there exists $m_i \in \mathcal{L}_\Pi$ s.t. $m \neq m_i$ and $H(m) = H(m_i)$. Hence, we have a collision for H.

With this observation, given an EUF-CMA ad. $\mathcal{A}$ against Π, we get

$$\Pr[\text{EUF-CMA}_{\Pi,\mathcal{A}} = 1] = \Pr[\text{EUF-CMA}_{\Sigma,\mathcal{A}'} = 1 \text{ or } \text{Collision}_{H,\mathcal{A}''} = 1]$$

↳ (i.e. $\mathcal{A}$ wins)

$$\leq \underbrace{\Pr[\text{EUF-CMA}_{\Sigma,\mathcal{A}'} = 1]}_{\text{negl}(n)} + \underbrace{\Pr[\text{collision}_{H,\mathcal{A}''} = 1]}_{\text{negl}(n)} \leq \text{negl}(n)$$

where $\mathcal{A}'$ is an EUF-CMA adv. against Σ that runs $\mathcal{A}$ as subroutine,
$\mathcal{A}''$ is a collision adv. against H that runs $\mathcal{A}$ as subroutine.

② 1. Let $\mathcal{A}'$ be an algo. that aims to distinguish $\mathcal{L}_{sign\text{-}real}$ and $\mathcal{L}_{sig\text{-}fake}$ s.t.

$\underline{\mathcal{A}' \circ L}$ (where L is either $L_{sig\text{-}real}$ or $L_{sig\text{-}fake}$)

$(vk, sk) \leftarrow \text{KeyGen}$

$(m, \sigma) \leftarrow \mathcal{A}$ s.t. $\text{Versig}(m, \sigma) = 1$ (but σ is not generated by $\text{Getsig}(m)$ since no one has the sk)

If $\text{Versig}(m, \sigma) == 1$:

    output "real"

Else :

    output "fake"

$$\Pr[\mathcal{A}' \text{ wins}] = \Pr[\mathcal{A}' \circ L \Rightarrow \text{real} \mid L = L_{sig\text{-}real}] \Pr[L = L_{sig\text{-}real}]$$

$$+ \Pr[\mathcal{A}' \circ L \Rightarrow \text{fake} \mid L = L_{sig\text{-}fake}] \Pr[L = L_{sig\text{-}fake}]$$

$$= 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1.$$

2. In MAC, we use the same key for Gettag and Checktag ($\sim$ Getsig and Versig). So, the key needs to be shared to use Checktag and we cannot make sure who signed it. In RSA-FDH signing and verification keys are different, so only the owner of sk is able to sign a message.

③ $\sigma : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ where $m = \underset{0}{m_k} | \underset{0}{m_{k-1}} | \cdots | m_1 | m_0$ in byte representation

$m \mapsto m^d \mod N$

Let $\mathcal{A}$ be an EUF-CMA adversary s.t. gets $(m, \overset{m^d \bmod N}{\sigma}) \leftarrow \text{Getsig}(m)$, then generates $M' = \{(m^i)^e : i = 1, 2, \ldots, 2^{16}\}$. If there is a valid message $m' = (m^e)^j$ in M' for some j, then $\mathcal{A}$ wins by outputting (m', σ') where $\sigma' = \sigma^{e \cdot j}$.

First, note that $\text{Versig}(m', \sigma')$: $(\sigma')^e = (\sigma^{e \cdot j})^e = ((m^d)^{e \cdot j})^e = (m^{ed})^{j \cdot e} = m^{j \cdot e} = m' \mod N$.

So, $\Pr[\mathcal{A} \text{ wins}] \leq \Pr[\exists m' \text{ in } M' \text{ that is valid}]$.

Next, observe that m' is valid iff $m' \in \mathbb{Z}_N^*$ and first two bytes of m' are zero.

- $m' \in \mathbb{Z}_N^*$ since $m' = m e^j \bmod N$ and $m \in \mathbb{Z}_N^*$.

- Notice that, by assumption, e-th power is a perfect permutation and the ratio of "messages whose first two bytes are 0" to "all messages" is $1/2^{16}$. Therefore, it is expected that among 2^{16} randomly selected messages in $\mathbb{Z}_N^*$, one of them is valid.

More precisely, $\Pr[\exists m' \text{ in } M' \text{ that is valid}] = \Pr\left[\begin{array}{l}\exists m' \text{ whose first two bytes are 00 among} \\ 2^{16} \text{ uni.-randomly selected elt. in } \mathbb{Z}_N^*\end{array}\right]$

$$\approx \frac{\binom{\lfloor \phi(N)/2^{16} \rfloor}{1}\binom{\phi(N)-1}{2^{16}-1}}{\binom{\phi(N)}{2^{16}}}$$

where $\phi(N) = |\mathbb{Z}_N^*|$ and $\lfloor \phi(N)/2^{16} \rfloor \leq$ # elements in $\mathbb{Z}_N^*$ starting with 00.

④ $\hat{H} : \{0,1\}^* \to \mathbb{Z}_N$ (randomly)

Number of outputs of $\hat{H}$ that lie outside of $\mathbb{Z}_N^* = |\mathbb{Z}_N| - |\mathbb{Z}_N^*| = N - \phi(N)$

$= pq - \phi(pq) = pq - (p-1)(q-1) = p+q-1 \approx 2^{1001} - 1$

BONUS: Assume you know an output t of $\hat{H}$ lying outside of $\mathbb{Z}_N^*$, then t is not relatively prime with N. So, $\gcd(N,t)$ is p or q, and $\dfrac{N}{\gcd(N,t)}$ is p or q as well.