Ex 1:

1. $Y_2 = Y_1 \Rightarrow h \cdot g^{-val(Y_2)} = g^{val(Y_1)}$

   $\Rightarrow h = g^{val(Y_1) + val(Y_2)}$

2. in that case $x = \sum_{i=1}^{m} x_i 2^{i-1}$ with $x_i = 1$ for exactly t positions
   the first $t/2$ positions with $x_i = 1$ lead to a set $Y_1 \in \binom{[m]}{t/2}$,
   — last ———————— " ———— $Y_2 \in \binom{[m]}{t/2}$)
   with: $x = val(Y_1) + val(Y_2)$

3. and 4. clear as $\left|\binom{[m]}{t/2}\right| = \binom{m}{t/2}$

Ex 2:

1. see course
2. recompute $Enc(pk, m_b)$ for $b \in \{0,1\}$ and compare ciphertext
3. above attack works for all det. schemes
4. - get signature on some m_0, m_1
     ↳ hom. compute signature on $m_0 \cdot m_1$
   - σ mod N is a signature for $m = \sigma^v \bmod N$
5. - signature: hash message first
   - RSA: pad message with randomness (carefully!)
6. similar to BLS security (last TD)

Ex 3:

1. see 2.QS, adds randomness, mitigates homomorphism-related problems
2. a server could return an error message in case the message is not PKCS conforming, else accept the message w/o error
   ↳ leads to such an oracle
7. given $c \in \mathbb{Z}_n$, choose s_0 until $c_0 = c(s_0)^e \bmod n$ is PKCS conforming
   ↳ obtain $m = c_0^d \in \mathbb{Z}_n$ via Bleichenbacher
   we have: $m = (c(s_0)^e)^d \bmod n$
   $\Rightarrow m \cdot s_0^{-1} = c^d \bmod n$
   $\Rightarrow \underbrace{(m \cdot s_0^{-1})^e}_{\text{signature for } c} = c \bmod n$
11. - an attack breaks a system if it works sometimes, a cryptosystem should be secure always.
    - attacks can be checked via an implementation
      (if it works well in practice, the attack is devastating even if we have no nice theoretical proof)

Remaining questions follow the analysis in:
https://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf
(section 3.2, pages 5-8)