Aufgabe 1)
(a)

$m = m_1 * m_2 \, mod \, n$

d = private Key von Bob

e = public Key

Alice lässt sich Nachricht m1 und m2 von Bob signieren.
Dadurch erhält sich s1 und s2.

(Signatur Algorithmus)

$s_1 = m_1^d \, mod \, n$
$s_2 = m_2^d \, mod \, n$

Außerdem wissen wir, dass gilt:

$d = e^{-1} \, mod \, \varphi(n)$
$a^{\varphi(n)} = 1$

(Verifikations Algorithmus)

$m_1' = s_1^e \, mod \, n$
$m_2' = s_2^e \, mod \, n$

Die Attacke läuft wie folgt ab:
Alice kombiniert s1 und s2 so, dass sie eine Signatur s erhält, sodass gilt:

$s = m^d \, mod \, n$
$m' = s^e \, mod \, n$

Annahme Alice erhält Signatur s durch $s = s_1 * s_2 \, mod \, n$

Wenn dies gilt, kann Alice Nachricht m mit der Signatur s verschicken und jemand anderen im Glauben lassen, dass Bob diese Nachricht signiert hat.

Warum funktioniert dies?

$$s = m^d \, mod \, n = (m_1 * m_2 \, mod \, n)^d = \left((s_1^e \, mod \, n * s_2^e \, mod \, n) \, mod \, n\right)^d$$
$$\equiv \left((s_1^e * s_2^e) \, mod \, n\right)^d \equiv ((s_1 * s_2)^e \, mod \, n)^d \equiv (s_1 * s_2)^{ed} \, mod \, n$$
$$\equiv (s_1 * s_2)^{1+k\varphi(n)} \, mod \, n \equiv (s_1 * s_2) * (s_1 * s_2)^{k\varphi(n)} \, mod \, n$$
$$\equiv (s_1 * s_2) * 1 \, mod \, n \equiv s_1 * s_2 \, mod \, n$$

(b)

Wenn die Bob stattdessen die gehashte Nachricht signiert ändern sich folgende Formeln:

$s_1 = H(m_1)^d \ mod \ n$
$s_2 = H(m_2)^d \ mod \ n$

$H(m_1') = s_1^e \ mod \ n$
$H(m_2') = s_2^e \ mod \ n$

Und es muss für s gelten:

$s = H(m)^d \ mod \ n$
$H(m') = s^e \ mod \ n$

Da es eine Hash Funktion nicht umkehrbar ist hat Alice keine Möglichkeit ein s durch die durch das „Umformen“ von $s = H(m)^d \ mod \ n$ eine Formel, welche nur Alice bekannte Variablen erhält, zu generieren.

$s = H(m)^d \ mod \ n = H((m_1 * \ m_2 \ mod \ n))^d \ \neq \ H(\big((s_1^e \ mod \ n * \ s_2^e \ mod \ n) \ mod \ n\ \big))^d$

2. a) Wenn Alice die Nachricht erst verschlüsselt und dann signiert, dann kann Bob die Signatur von Alice entfernen und die Nachricht trotzdem weiter schicken. Bob kann sogar die Nachricht von Alice als seine ausgeben. Dave hat aber keinen kryptographischen Beweis, dass Alice die Nachricht gesendet hat.

b) Solution 1:
Wenn Alice in ihre Nachricht nicht einfach schreibt, "ich liebe dich" sondern Absender und Empfänger dazu schreibt, dann wird durch die Signatur der Inhalt der Nachricht
vor veränderung geschützt.

Solution 2:
Alice könnte die Nachricht signieren. Dann verschlüsseln und dann den Ciphertext auch signieren.