10

4.2

Samantha has public key $\{N, v\} = \{1562501, 87953\}$.
Adam claims Samantha has signed the documents:

Which of these are valid signatures.

Note: since RSA is being used for signatures, the public key is called v for verity rather than e for encrypt.

a

$h(D) = 119812$ $S = 876453$

✓ **Answer**
$S^v \pmod N$
$= 772481$

No, this is not valid

b

$h(D) = 161153$ $S = 870099$

✓ **Answer**
$S^v \pmod N$
$= 161153$

Yes, this is valid

c

$h(D) = 586036$ $S = 602754$

✓ **Answer**
$S^v \pmod N$
$= 586036$

Yes, this is valid