1. RSA-PSS...
   - A ...uses the textbook RSA scheme with a preprocessed message
   - B ...is used by the textbook RSA scheme as a subroutine
   - C ...has a security reduction in the ROM with a larger security loss than that of RSA-FDH
   - D ...has a security reduction in the ROM with a smaller security loss than that of RSA-FDH
   - E ...can be implemented without random oracles

2. The security analysis of RSS-PSS uses crucially that every message has a unique signature.
   - T True
   - F False

3. When we set \( r \) to be zero (i.e., \( r := 0^{k_0} \)), then RSA-PSS becomes...
   - A ...more secure
   - B ...deterministic (such that the signing algorithm always outputs the same signature for a given message)
   - C ...RSA-FDH