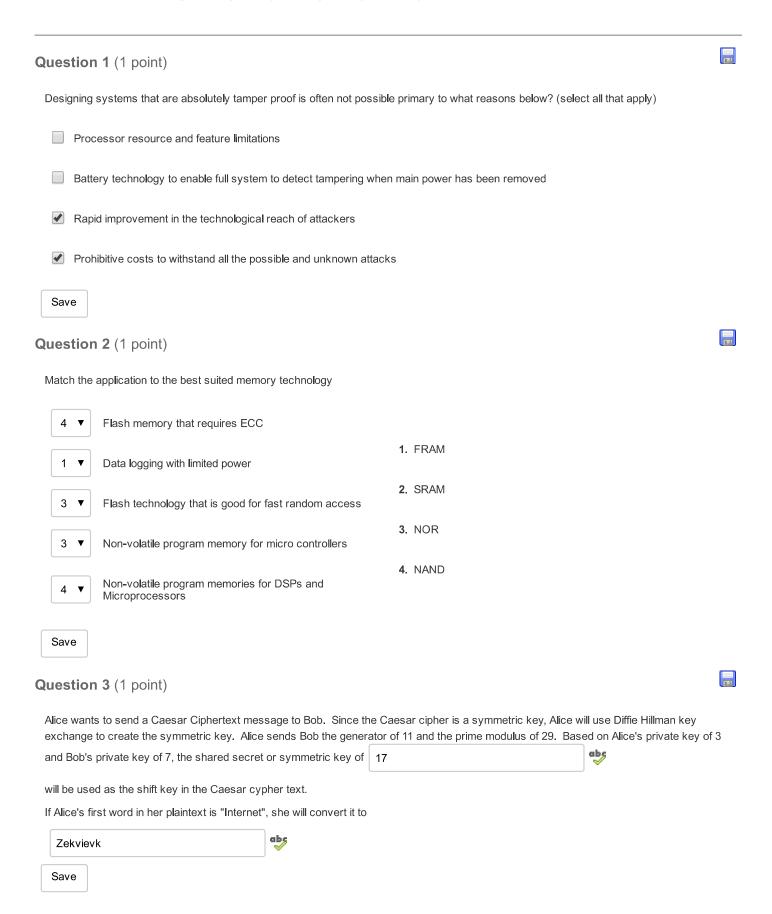
Quiz

Note: It is recommended that you save your response as you complete each question.



Question 4 (1 point) Match all subjects to their description Passive chip that responds only to commands from platform software that aids in the platform software to verify itself. ▼ Secure Boot 2. Keys, encrypted data, NVRAM, and counters 3 ▼ Measured Boot 3. Firmware and operating system boot loaders verify that nothing Objects ▼ has changed in the reboot environment 1 ▼ Firmware simply verifies a signature of the boot loader before executing the boot loader Save Question 5 (1 point) Which encryption algorithms were not included in TPM 1.2 due to legal export regulations or restrictions? AES DES SHA-256 SM2 Save Question 6 (1 point) In the Caesar ciphertex, "Vu hclyhnl, lhjo dllr aol sljabylz dpss il jvclypun ivao aolvyf huk jvujlwaz hz dlss hz ptwsltluapun svd lulynf klzpnu wyhjapilz pu ohykdhyl/mpytdhyl. Ablzkhf dpss il mvjbzpun vu aolvyf huk jvujlwaz dopsl vu Aobyzkhf aol sljabyl dpss il zwspa iladllu aolvyf huk jvujlwaz dpao svd lulynf klzpnu wyhjapjlz.", how many abs 19 (the number) letters is the shift "key." The sixth word, sljabylz, in ciphertext translates to lectures Save **100** Question 7 (1 point) The objective of privacy attacks is to gain knowledge of sensitive information stored, communicated, or manipulated wishing an embedded system.

Save

Question 8 (1 point)



Match all subjects with their descriptions

- 4 ▼ Symmetric encryption
- 1 ▼ Cryptographic engine
- 2 ▼ PCR
- 3 ▼ Attestation
- 5 ▼ Asymmetric encryption

Save

5 ▼

Question 9 (1 point)

Match the term with its definition

Tamper evidence

- 2 ▼ Detection latency
- 4 ▼ Attack detection
- 1 ▼ Attack prevention
- 3 ▼ Attack recovery

Save

- 1. Perform encryption, digital signatures, and hashing
- $\begin{tabular}{ll} {\bf 2.} & Registers that store a representation of the state of software on the platform \end{tabular}$
- 3. Cryptographically prove to another platform that is is in a particular state
- 4. The same key is used for encryption and decryption
- 5. Use public and private key pairs

Technique that makes it difficult to initiate an attack on an embedded system.

- 2. Time interval between the launch of an attack and its detection.
- 3. Techniques used to ensure that the attack is countered, and that the system returns to secure operations ${\bf 3}$
- 4. Techniques to detect an attack on an embedded system.
- 5. Persistent record of an attack on the embedded system

Question 10 (1 point)



Software can also use the TPM to create

monotonically



increasing counters.

Save

Save All Responses

Go to Submit Quiz