Quiz

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

Question 1 (1 point)

Designing systems that are absolutely tamper proof is often not possible primary to what reasons below? (select all that apply)

- [ ] Processor resource and feature limitations
- [ ] Battery technology to enable full system to detect tampering when main power has been removed
- [x] Rapid improvement in the technological reach of attackers
- [x] Prohibitive costs to withstand all the possible and unknown attacks

Save

Question 2 (1 point)

Match the application to the best suited memory technology

4 ▼	Flash memory that requires ECC
1 ▼	Data logging with limited power
3 ▼	Flash technology that is good for fast random access
3 ▼	Non-volatile program memory for micro controllers
4 ▼	Non-volatile program memories for DSPs and Microprocessors

1. FRAM
2. SRAM
3. NOR
4. NAND

Save

Question 3 (1 point)

Alice wants to send a Caesar Ciphertext message to Bob. Since the Caesar cipher is a symmetric key, Alice will use Diffie Hillman key exchange to create the symmetric key. Alice sends Bob the generator of 11 and the prime modulus of 29. Based on Alice's private key of 3 and Bob's private key of 7, the shared secret or symmetric key of 17 will be used as the shift key in the Caesar cypher text.

If Alice's first word in her plaintext is "Internet", she will convert it to

Zekvievk

Save

Question 4 (1 point)

Match all subjects to their description

4 ▼	Secure Boot	1. Passive chip that responds only to commands from platform software that aids in the platform software to verify itself.
3 ▼	Measured Boot	2. Keys, encrypted data, NVRAM, and counters
2 ▼	Objects	3. Firmware and operating system boot loaders verify that nothing has changed in the reboot environment
1 ▼	TPM	4. 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?

- [x] AES
- [x] 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 wyhjapjlz 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

19

(the number) letters is the shift "key." The sixth word, sljabylz, in ciphertext translates to

lectures

Save

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. Perform encryption, digital signatures, and hashing
1 ▼ Cryptographic engine	2. Registers that store a representation of the state of software on the platform
2 ▼ PCR	3. Cryptographically prove to another platform that is is in a particular state
3 ▼ Attestation	4. The same key is used for encryption and decryption
5 ▼ Asymmetric encryption	5. Use public and private key pairs

Save

Question 9 (1 point)

Match the term with its definition

5 ▼ Tamper evidence	1. Technique that makes it difficult to initiate an attack on an embedded system.
2 ▼ Detection latency	2. Time interval between the launch of an attack and its detection.
4 ▼ Attack detection	3. Techniques used to ensure that the attack is countered, and that the system returns to secure operations
1 ▼ Attack prevention	4. Techniques to detect an attack on an embedded system.
3 ▼ Attack recovery	5. Persistent record of an attack on the embedded system

Save

Question 10 (1 point)

Software can also use the TPM to create monotonically increasing counters.

Save

Save All Responses Go to Submit Quiz