



Visit and Download Full Version Certificationtime Exam Dumps
<https://certificationtime.com/updated/adr-001-exam-dumps-pdf/>



CompTIA

Exam Questions ADR-001

CompTIA Mobile App Security+ Certification

<https://certificationtime.com/>





Question No : 1

To prevent a component from being publically accessible via Intents the developer can:

- A. set the attribute android:exported=false in the manifest.
- B. declare the method as private in the Java source.
- C. sign the app because Android protects component access by verifying digital signatures.
- D. add an Intent Filter with the attribute of “private”.

Answer: A

Question No : 2

When storing a PIN used to logon to the app, by applying a cryptographic hash function a developer will:

- A. provide plausible deniability.
- B. mitigate the salt used with the password.
- C. mitigate the location of the encrypted data.
- D. mitigate the password from being recovered.

Answer: D

Question No : 3

Session keys are useful because:

- A. they temporarily provide a mechanism to maintain the state of user interaction.
- B. they are generated on the Android device locally upon startup.
- C. there is only one key to generate.

Get Certified In First Attempt

visit - <https://certificationtime.com/>



D. they are more secure than public/private keys.

Answer: A

Question No : 4

An attacker intercepts and potentially tampers with communication between two entities without the knowledge of either of the two entities. This BEST describes which of the following attacks?

- A. SOCKS proxy attack
- B. Man-in-the-middle attack
- C. TCP relay attack
- D. ARP poisoning attack

Answer: B

Question No : 5

In public key cryptography which problem can occur when the public key is transmitted?

- A. The initialization vector can be determined
- B. The public key can be replaced with a different one
- C. The hash of the data can be decrypted with the private key
- D. The private key can be calculated from the public one

Answer: B

Question No : 6

Adding an Intent Filter to an Activity could cause a security issue because:

Get Certified In First Attempt

visit - <https://certificationtime.com/>



- A. activities with Intent Filters are unprivileged by default.
- B. it bypasses Android's default filters.
- C. activities with Intent Filters are exported by default.
- D. it violates the Android sandbox security model.

Answer: C

Question No : 7

Unencrypted temporary private user data cached in the application directory should be:

- A. moved to the SD card.
- B. wiped on app shut down.
- C. hashed to avoid recovery.
- D. wiped when no longer needed.

Answer: D

Question No : 8

How should a developer securely share data between applications?

- A. Using file permissions on the SD card
- B. Creating world-readable files in the application directory
- C. Defining content providers with permissions
- D. Using a shared SQLite database

Answer: C

Full Access:

Get Certified In First Attempt

visit - <https://certificationtime.com/>



Visit and Download Full Version Certificationtime Exam Dumps

<https://certificationtime.com/updated/adr-001-exam-dumps-pdf/>

<https://certificationtime.com/updated/adr-001-exam-dumps-pdf/>

Get Certified In First Attempt

visit - <https://certificationtime.com/>