
Table of Contents

1. Exam - Introduction

Everything is Data

Overview: These are the exam questions for Principle 2: Everything is Data.

1.1. According to the Information Security Model, what are the three 'Information States?'

Storage, Processing, Transmission

1.2. What are the three 'Security Practices?'

Policies and Procedures, Technology, Education/Awareness/Training

1.3. What are the two main ways of ensuring data confidentiality?

Limiting access (access controls), concealing content (encryption)

1.4. When using a well-known means of encryption, such as an algorithm like AES, upon what part of the cryptosystem does the confidentiality of the encrypted data hinge?

The Key

1.5. True or false: For similarly sized keys, a symmetric encryption system is faster than an asymmetric system.

True

1.6. Describe how a transaction would take place using the hybrid model of encryption (hybrid of symmetric and asymmetric).

The two hosts would exchange public keys (i.e., part of the asymmetric encryption system) and would use the asymmetric system to then create and share a symmetric cryptosystem key; after the key had been shared and agreed upon, the rest of the transaction would be encrypted with the symmetric key and symmetric encryption algorithm.

1.7. Describe how the use of a hash function could give an administrator confidence that some files on his system had not changed.

If the administrator generated hashes of the files in question when they were in a known state and kept that hash for future reference, he could (at any time) generate new hashes and compare those to the hashes on file and would know for certain if the files had changed.