

## Exam Objectives that do NOT Exist in Security+ SY0-401 but ARE in SY0-501

[Click here for the practice tests and exam simulations](#)

OBJ/Sub-OBJ

NEW in 501

### 6.0 Cryptography and PKI No Change add PKI

#### 6.1 Compare and contrast basic concepts of cryptography.

- Salt, IV, nonce **NEW**
- Diffusion **NEW**
- Confusion **NEW**
- Collision **NEW**
- Obfuscation **NEW**
- Random/pseudo-random n **NEW**
- Security through obscurity **NEW**
- Common use cases
  - o Low power devices **NEW**
  - o Low latency **NEW**
  - o High resiliency **NEW**
  - o Supporting obfusca **NEW**
  - o Supporting authentication
  - o Resource vs. securit **NEW**

#### 6.2 Explain cryptography algorithms and their basic characteristics.

- Cipher modes
  - o CBC **NEW**
  - o GCM **NEW**
  - o ECB **NEW**
  - o CTM **NEW**
- Obfuscation
  - o XOR **NEW**
  - o ROT13 **NEW**
  - o Substitution ciphers **NEW**

#### 6.3 Given a scenario, install and configure wireless security settings.

- Authentication protocols
  - o EAP-FAST **NEW**
  - o EAP-TLS **NEW**
  - o EAP-TTLS **NEW**
  - o IEEE 802.1x **NEW**
  - o RADIUS Federation **NEW**
- Methods
  - o PSK vs. Enterprise vs. Open **NEW**
  - o WPS **NEW**

6.4 Given a scenario, implement public key infrastructure.

- Components

- o Object identifiers (CN) **NEW**

- Concepts

- o Online vs. offline CA **NEW**

- o Pinning **NEW**

- Types of certificates

- o Wildcard **NEW**

- o SAN **NEW**

- o Domain validation **NEW**

- o Extended validation **NEW**

- Certificate formats

- o PEM **NEW**

- o PFX **NEW**

- o CER **NEW**

- o P12 **NEW**

- o P7B **NEW**

