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

*Click here for the practice tests and exam simulations*

<table>
<thead>
<tr>
<th>OBJ/Sub-OBJ</th>
<th>NEW in 501</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.0 Cryptography and PKI</strong></td>
<td>No Change add PKI</td>
</tr>
</tbody>
</table>

6.1 Compare and contrast basic concepts of cryptography.
- Salt, IV, nonce
- Diffusion
- Confusion
- Collision
- Obfuscation
- Random/pseudo-random number generation
- Security through obscurity
- Common use cases
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting obfuscation
  - Supporting authentication
  - Resource vs. security constraints

6.2 Explain cryptography algorithms and their basic characteristics.
- Cipher modes
  - CBC
  - GCM
  - ECB
  - CTM
- Obfuscation
  - XOR
  - ROT13
  - Substitution ciphers

6.3 Given a scenario, install and configure wireless security settings.
- Authentication protocols
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- Methods
  - PSK vs. Enterprise vs. Open
  - WPS
6.4 Given a scenario, implement public key infrastructure.

- Components
  - Object identifiers (C)

- Concepts
  - Online vs. offline CA
  - Pinning

- Types of certificates
  - Wildcard
  - SAN
  - Domain validation
  - Extended validation

- Certificate formats
  - PEM
  - PFX
  - CER
  - P12
  - P7B