CompTIA Sec+ SY0-401, Part 8 of 8: Cryptography and Keys

Meet the expert: Ryan Hendricks is an experienced instructor who teaches networking and security courses to IT professionals throughout the nation. He currently has the CompTIA Certified Technical Trainer (CTT+ Classroom) and the Cisco Certified Academy Instructor (CCAI) credentials. He holds certifications from (ISC)2, EC-Council, CompTIA, and Cisco. When not on the podium instructing, he delves into IT books, always looking to learn more and keep up with the latest security topics.

Prerequisites: This course assumes that the user has working knowledge of networks and networking. Ideally, the user should have their CompTIA Network+ certification, but can be replaced with networking experience.

Runtime: 01:24:26

Course description: Here certified technical trainer Ryan Hendricks elucidates the world of cryptography and how IT professionals can use it to support security and confidentiality. Hendricks will explain common encryption algorithms as well as use cases for both symmetric and asymmetric encryption. This course will demonstrate how security certificates work and are validated and also show how hashing algorithms can be used in a production environment.

Course outline:

Cryptology Concepts
- Introduction
- Terminology
- Keyspace
- Symmetric vs. Asymmetric
- Session Keys
- In Band vs. Out of Band
- Block Encryption
- Stream Encryption
- Transport Encryption
- Non-Repudiation
- Hashing
- Key Escrow
- Steganography
- Digital Signatures
- Use of Proven Technologies
- Elliptical Curve & Quantum
- Perfect Forward Secrecy
- Ephemeral Key
- Summary

Symmetric Encryption
- Introduction
- Pros
- Cons
- Key Management
- Data Encryption Standard
- 3DES
- Rivest Cipher 4
- One-Time Pad
- Blowfish/Twofish
- Advanced Encryption Standard
- Summary

Asymmetric Encryption
- Introduction
- Pros
- Cons
- Diffie Hellman
- Rivest Shamir Adleman
- Key Pairs
- PGP/GPG
- Public Key Infrastructure
- Digital Certificate
- Certificate Authority
- Trust Models
- Registration Authority
- Certificate Revocation List
- OSCP
- Certificate Signing Request
- Key Escrow
- Summary

Hashing
- Introduction
- Hashing Concepts
- Collisions
- Hashing Passwords
- Salting
- MD5
- NTLM
- Secure Hash Algorithm
- RIPEMD
- Hashing for Authentication
- HMAC
- Demo: Verify Messages
- Summary