CompTIA Sec+ SY0-501, Part 8 of 9: Cryptography and PKI

Meet the expert: Jason Dion, CISSP No. 349867, is a professor at University of Maryland University College with multiple information technology professional certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Network Defense Architect (CNDA), Digital Forensic Examiner (DFE), Digital Media Collector (DMC), CySA+, Security+, Network+, A+, PRINCE2 Practitioner, and ITIL. He holds a Masters of Science degree in Information Technology with a specialization in Information Assurance

Prerequisites: • Basic familiarity with computer networks, administration, and security is helpful (But, all required information will be covered during the course)
• Completion of the CompTIA A+ and Network+ certifications (Helpful, but not required)

Runtime: 01:31:50

Course description: This course discusses Cryptography, symmetric and asymmetric algorithms, public key cryptography and Key Management. Next it covers hashing, steganography and how to manage Public Key infrastructure as well as digital certificates. Finally, it will go into detail around SSL and TLS, SSH and Virtual Private Networks for the SY0-501 Exam.

Course outline:

Cryptography
• Introduction
• Cryptography
• Symmetric vs Asymmetric
• Symmetric Algorithms
• Public Key Cryptography
• Asymmetric Algorithms
• Pretty Good Privacy
• Summary

Key Management
• Introduction
• Key Management
• One-Time Pad
• Demo: Steganography
• Hashing
• Demo: Hashing
• Hashing Attacks
• Increasing Hash Security
• Summary

Public key Infrastructure
• Introduction
• Public Key Infrastructure
• Digital Certificates
• Demo: Certificates
• Certificate Authorities
• Web of Trust
• Summary

Security Protocols
• Introduction
• Security Protocols
• SMIME
• SSL and TLS
• SSH
• VPN Protocols
• Demo: Setting Up a VPN
• Summary