CASP, Part 1 of 9: Cryptography

Meet the expert: David Bigger is the lead trainer at Bigger IT Solutions. He has been information technology for a little over 20 years and has been training all over the US. He has worked with companies like US Military, Lockheed Martin, General Dynamics, Dominos Pizza, University of Utah and Expedia

Prerequisites: This course assumes that you have familiarity with information technology, basic networking, and basic security concepts. No scripting or “hacking” experience is required. Having windows command line experience as well as having administrative rights on your machine will be helpful.

Runtime: 01:33:10

Course description: Do you want to know more about protecting your data on your computer? Would you like to see the ins and outs of how that happens? Dive into cryptography and learn about encryption algorithms including 3DES and AES. Understand the difference between symmetric encryption and asymmetric encryption, which is a better solution to use in different circumstances, and why. We'll explore some of the tools used to secure data both on your hard drive and through emails, as well as focus on the integrity of your data utilizing hashing to authenticate downloads. Finally, we'll examine public key infrastructure to see how it works under the hood to keep online shopping, banking, and other transactions secure. This course is part of a series covering the CompTIA Advanced Security Practitioner (CASP).

Course outline:

Introduction
- Introduction
- What Is Cryptography?
- Caesar Cipher
- Scytale
- Why Do We Need Cryptography?
- Types of Cryptography
- Block Ciphers
- Transposition Cipher
- Substitution Cipher
- Diffusion Cipher
- Confusion
- Stream Ciphers
- Attacks on Cryptography
- Summary

Symmetric and Asymmetric Encryption
- Introduction
- Symmetric and Asymmetric
- Symmetric Algorithms
- Symmetric Encryption
- Data Encryption Standard (DES)
- 3DES (Triple DES)
- Advanced Encryption Standard
- RC - Rivest Cipher
- Skipjack
- Asymmetric Encryption
- RSA
- Diffie-Hellman
- Elliptic Curve
- El Gamal
- Tools for Encryption
- PGP - Pretty Good Privacy
- GPG - Gnu Privacy Guard
- Summary

Veracrypt
- Introduction
- Demo: Veracrypt
- Demo: Create Encrypted Volume
- Demo: Finishing Up
- Summary

Hashing
- Introduction
- Hashing
- What Is Hashing?
- MD5 Hash
- SHA Hashes
- MAC
- HMAC
- RIPEMD
- Demo: HashCalc
- Demo: Online Hashing Tools
- Summary

Public Key Infrastructure
- Introduction
- PKI - Public Key Infrastructure
- What Is PKI?
- Certificates
- Certificate Authority
- Registration Authority
- CRL
- OCSP
- Key Escrow
- Digital Certificates
- Summary