Chapter 2

Cryptography

Episode 2.01

Episode title: **Cryptography Basics**

Objective: **Overview**

Quick Review

- Cryptography is the practice of disguising information in a way that looks random
- The Caesar cipher is one of the earliest known and simplest ciphers
- The Vigenère cipher employs the Caesar cipher as one element of the encryption process

Episode 2.02

Episode title: **Data Protection**

Objective: **2.1 Explain the importance of security concepts in an enterprise environment.**

Quick Review

- Data at rest is housed physically on some kind of computer storage
- Data in use is housed in RAM and being accessed
- Data in transit is moving through cables and wireless transmission

Episode 2.03

Episode title: **Cryptographic Methods**

Objective: **2.8 Summarize the basics of cryptographic concepts.**

Ephemeral Key

- Temporary
- Provides perfect forward secrecy

Asymmetric Encryption

- Uses a key pair
  - Public key
  - Private key
- Public key is only used to encrypt
- Private key is only used to decrypt

Quick Review

- Ephemeral keys provide perfect forward secrecy due to the temporary nature of the key
- Asymmetric encryption is slow but very useful in exchanging session keys
- Cryptosystems define key properties, communication requirements for the key exchange, and the actions taken through the encryption and decryption process

Episode 2.04

Episode title: **Symmetric Cryptosystems**

Objective: **2.8 Summarize the basics of cryptographic concepts.**

Symmetric Key Algorithms

- Block
  - Encrypts data in chunks
  - Symmetric block algorithm
  - Data Encryption Standard (DES)

Symmetric Block Algorithms

- DES
- Blowfish
- Triple DES (3DES)
- Defined by
  - Key length
  - Block size
  - Number of rounds

Symmetric Key Cryptosystems

- Streaming
  - Encrypt one bit at a time
  - Popular in wireless networking
  - RC4

Quick Review

- Symmetric block algorithms encrypt data in discrete chunks
- Streaming symmetric algorithms encrypt data one bit at a time
- Block algorithms (or ciphers) include the outdated DES, 3DES, and Blowfish, as well as the currently-used AES
- The most used streaming symmetric cipher is RC4

Episode 2.05

Episode title: **Symmetric Block Modes**

Objective: **2.8 Summarize the basics of cryptographic concepts.**

Quick Review

- ECB block modes will always output the same results with the same input
- A binary block is plain text converted into 16-bit, 64-bit, or 128-bit binary ciphertext
- CBC, CFC, OFB, CTR block modes use an initialization vector (IV), which ensure the output block is uniquely different

Episode 2.06

Episode title: **Asymmetric Cryptosystems**

Objective: **2.8 Summarize the basics of cryptographic concepts.**

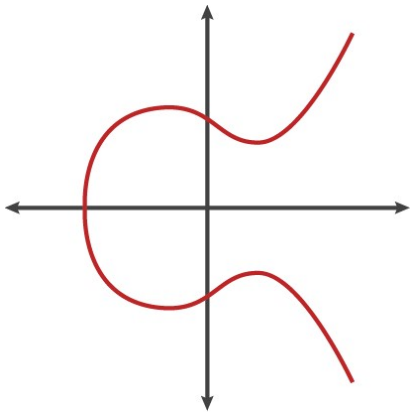
Factoring

- 12
  - 1 X 12
  - 2 X 6
  - 3 X 4
  - 4 X 3
- 11
  - 1 X 11
  - Prime number

Prime Number Factoring

- 11 X 17
  - Equals 187
  - Semi-prime number
- 100,160,063
  - 10,007 X 10,009
- 182,663,117,011,676,687

Elliptic-Curve Cryptography (ECC)



Quick Review

- Public keys are paired with a private key (key pair) when using RSA asymmetric cryptography
- ECC can create a smaller key than RSA and provides the same security with increased performance
- Each public key has a single private key, without the private key the information cannot be decrypted

Episode 2.07

Episode title: **Diffie-Hellman**

Objective: **No objective**

Diffie-Hellman

- Asymmetric algorithm
- Provides a methodology for 2 parties to come up with the same session key

Diffie-Hellman Groups

Group 1	768-bit modulus
Group 2	1024-bit modulus
Group 5	1536-bit modulus
Group 14	2048-bit modulus
Group 19	256-bit elliptic curve
Group 20	384-bit elliptic curve
Group 21	521-bit elliptic curve

Quick Review

- Diffie-Hellman is an asymmetric algorithm often referred to as a key exchange agreement
- Diffie-Hellman groups help by defining the size or type of key structure to use
- Diffie-Hellman can have very large keys

Episode 2.08

Episode title: **Hashing**

Objective: **2.8 Summarize the basics of cryptographic concepts.**

Quick Review

- Hashes are one-way, deterministic, and will produce the same results each time the source is hashed
- The length of the source data does not matter; the hash will be the same exact size
- Hashes are involved with password storage and encryption

Episode 2.09

Episode title: **Understanding Digital Certificates**

Objective: **2.8 Summarize the basics of cryptographic concepts.**

3.9 Given a scenario, implement public key infrastructure.

Quick Review

- Digital signatures verify that the person who sent the public key legitimately owns the private key
- Digital certificates include verification from a third party to authenticate the owner of the digital signature

Episode 2.10

Episode title: **Trust Models**

Objective: **3.9 Given a scenario, implement public key infrastructure.**

Quick Review

- Web of trust uses a network of mutually-trusting peers
- Public key infrastructure (PKI) uses a hierarchical structure with certificate authorities (CAs) and intermediate CAs

Episode 2.11

Episode title: **Public Key Infrastructure**

Objective: **3.9 Given a scenario, implement public key infrastructure.**

Quick Review

- X.509 is a method to query systems that store certificates and also includes standards for constructing digital certificates
- Public Key Cryptography Standards (PKCS) gives details on digital certificate construction and use
- Certificate authorities (CAs) or registration authorities (RAs) identify and authenticate individuals registering for certificate; the middle entities are called intermediate CAs, the entity at the top of the hierarchy is called the root CA
- A self-signed certificate is one that is authorized by the same entity who registers for the digital certificate (these should not be trusted outside an internal network)

Episode 2.12

Episode title: **Certificate Types**

Objective: **3.9 Given a scenario, implement public key infrastructure.**

Quick Review

- Digital certificates store a public key with a digital signature, personal information about the resources, and a second digital signature from a trusted third party
- Digital certificates come in many forms including Web (which includes DV, EV, wildcard, and SAN), e-mail, code-signing, machine/computer, and user

Episode 2.13

Episode title: **Touring Certificates**

Objective: **3.9 Given a scenario, implement public key infrastructure.**

Quick Review

- Expired certificates are included in a certificate authority's published list called a certificate revocation list (CRL)
- P7B files include the certificate and chain certificates, no private key
- P12 files include the certificate, chain certificates, and the private key

Episode 2.14

Episode title: **Cryptographic Attacks**

Objective: **1.2 Given a scenario, analyze potential indicators to determine the type of attack.**

Quick Review

- Cryptographic attacks can be put into three main categories: attack the algorithm, implementation, or key
- Attacking the algorithm is nearly impossible for the most up-to-date standards, as crackable algorithms are usually taken out of production
- Attacking the implementation means taking advantage of weaknesses in how the connection is made
- Attacking the key means somehow figuring out the key in order to break in

Episode 2.15

Episode title: **Password Cracking**

Objective: **1.2 Given a scenario, analyze potential indicators to determine the type of attack.**

2.8 Summarize the basics of cryptographic concepts.

Usernames and Hashed Passwords

username	password hash
root	098f6bcd4621d373cade4e832627b4f6
daemon	501be90e7a4210727034c38555d78490
sys	d00d84d04a6091922be5cd06457f9cfa
user1	437b930db84b8079c2dd804a71936b5f
user2	8277e0910d750195b448797616e091ad

Salting

- Password
  - Timmy123
- Salted password
  - Timmy123Krj8e00
- Salted password hash
  - 075E8E6B3F2A84E12FCA6AB15722E65B3726119E3AD57AB4EBF61638CA7836CF

Quick Review

- Passwords are usually stored in hash format, making them difficult to crack
- Brute-force attacks try character combinations
- Dictionary attacks use lists of probable passwords
- Rainbow tables use pre-calculated hashes of passwords
- Salting and key stretching adds another layer of obfuscation, making passwords even harder to crack than just hashing

Episode 2.16

Episode title: **Password Cracking Demo**

Objective: **1.2 Given a scenario, analyze potential indicators to determine the type of attack.**

2.8 Summarize the basics of cryptographic concepts.