COURSE: SECURITY+ SY0-401

MODULE 6: CRYPTOGRAPHY

Overview

- Given a scenario, utilize general cryptography concepts
- Given a scenario, use appropriate cryptographic methods

Symmetric vs. Asymmetric

A symmetric key is a single cryptographic key used with a secret key (symmetric) algorithm. The symmetric key algorithm uses the same private key for both operations of encryption and decryption.

In an asymmetric key system, each user has a pair of keys: a private key and a public key. Sending an encrypted message requires you to encrypt the message with the recipient's public key. The message in turn gets decrypted by the recipient with his or her private key.

Nonrepudiation and Digital Signatures

Nonrepudiation is intended to provide, through encryption, a method of accountability that makes it impossible to refute the origin of data. It guarantees that the sender cannot later deny being the sender and that the recipient cannot deny receiving the data. Four of the key elements are:

- Proof of origin
- Proof of submission
- Proof of delivery
- Proof of receipt

Symmetric Encryption Algorithms

Symmetric key encryption uses a common shared key or identical key is used between the sender and the receiver. Symmetric algorithms can be classified as either block ciphers or stream ciphers. A stream cipher, as the name implies encrypts the message bit by bit, one at a time. A block cipher encrypts the message in chunks.

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Blowfish Encryption Algorithm
- International Data Encryption Algorithm (IDEA)
- Rivest Cipher (RC2, RC4, RC5, RC6)

Asymmetric Encryption Algorithms

Various asymmetric algorithms have been designed, but few have gained the widespread acceptance of symmetric algorithms. Also because of the additional overhead generated by using two keys for encryption and decryption, asymmetric algorithms require more resources than symmetric algorithms.

- Rivest, Shamir, and Adleman encryption algorithm (RSA)
- Diffie-Hellman key exchange
- El Gamal encryption algorithm
- Elliptic curve cryptography (ECC)

Hashing

A *hash* is a generated summary from a mathematical rule or algorithm and is used commonly as a "digital fingerprint" to verify the integrity of files and messages and to ensure message integrity and provide authentication verification. In other words, hashing algorithms are not encryption methods but offer additional system security via a "signature" for data confirming the original content.

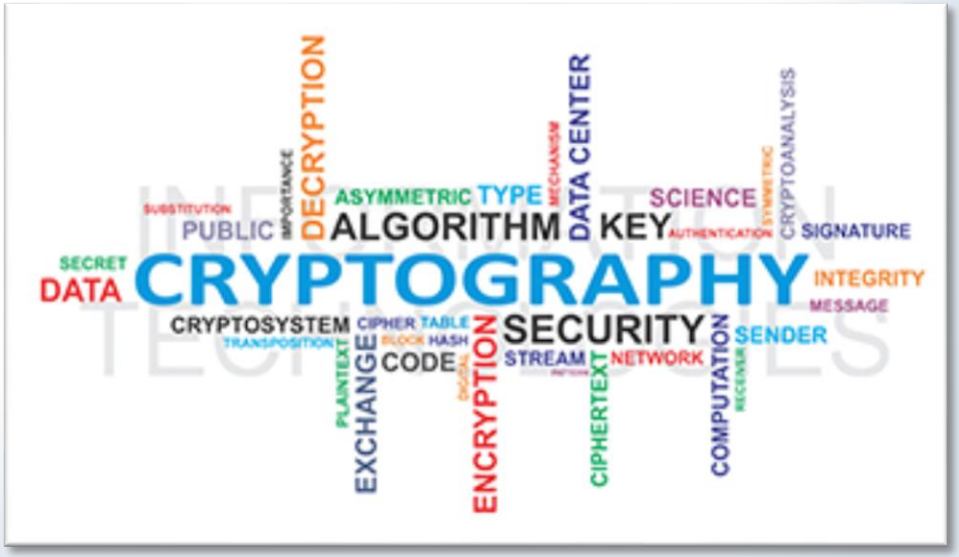
- Secure Hash Algorithm (SHA, SHA-1, SHA-2, SHA-3)
- Message Digest Series Algorithm (MD2, MD4, MD5)

Steganography

Steganography is a word of Greek origin meaning "hidden writing." Steganography is a method for hiding messages so that unintended recipients aren't even aware of any message. Compare this to cryptography, which does not seek to hide the fact a message exists, but rather to just make it unreadable by anyone other than the intended recipients

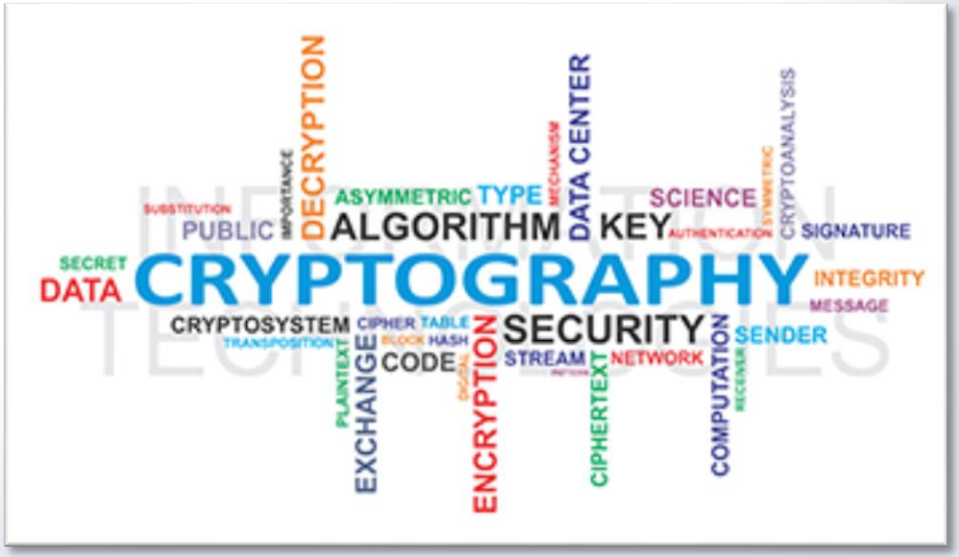
Cryptography Concepts

- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography
- Ephemeral key
- Perfect forward secrecy



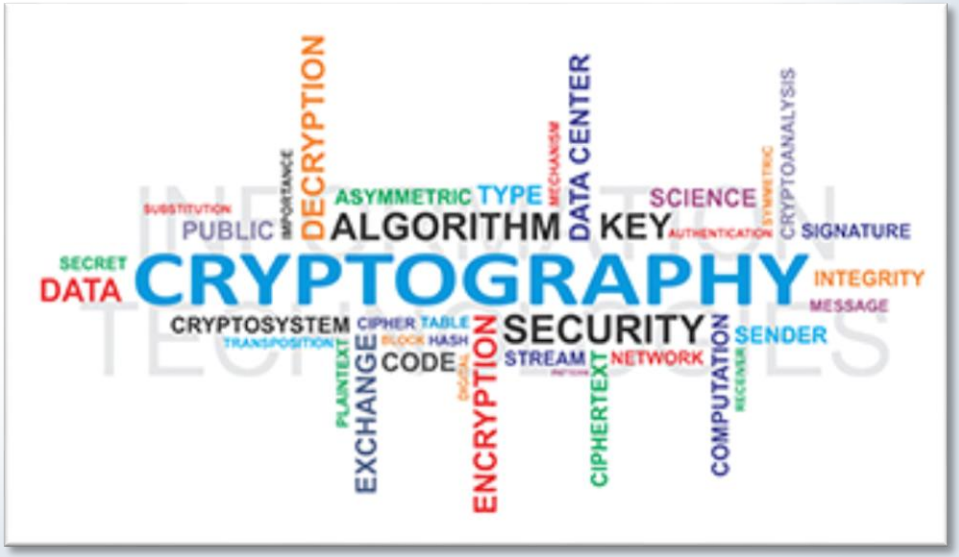
Cryptography Method

- WEP vs. WPA/WPA2 and preshared key
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA



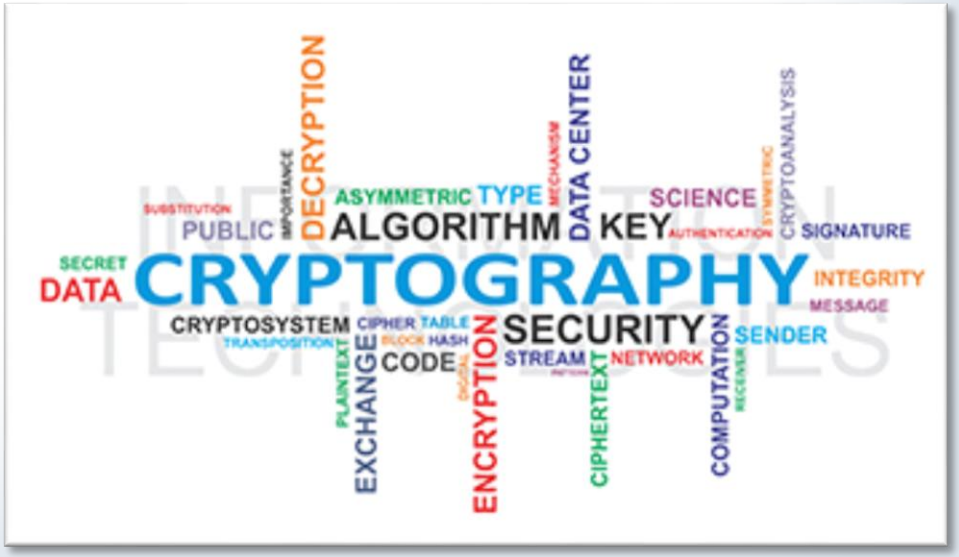
Cryptography Method

- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP



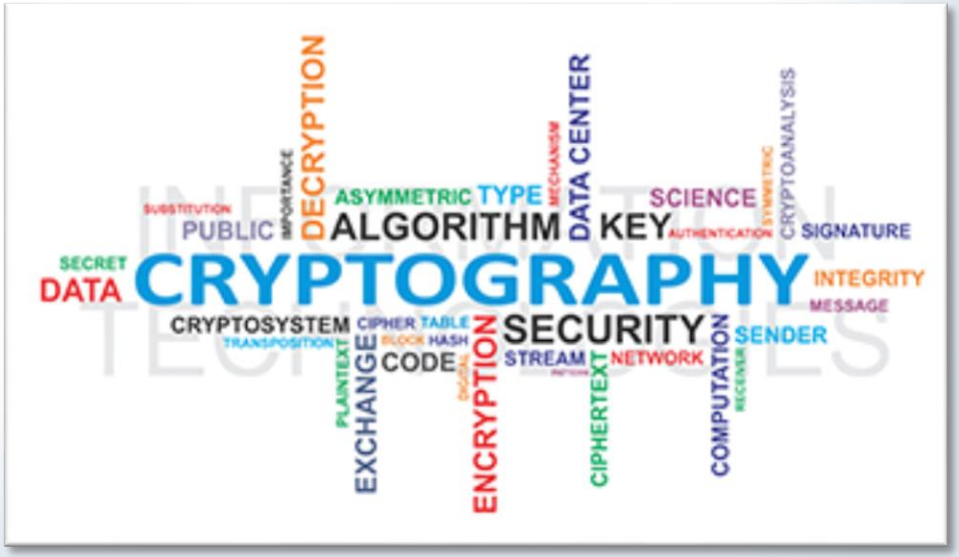
Cryptography Method

- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
  - SSL
  - TLS
  - IPSec
  - SSH
  - HTTPS
- Cipher suites
- Strong vs. weak ciphers
- Key stretching
  - PBKDF2
  - Bcrypt



Cryptography Concepts

- Session keys
- In-band vs. out-of-band key exchange
- Fundamental differences and encryption methods
- Block vs. stream
- Transport encryption
- Non-repudiation
- Key escrow



THANK YOU