J. A. “Drew” Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Cryptography

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Cryptography in Action

- Public key infrastructure
- Digital certificates
- Authentication
- E-commerce
- RSA
- MD-5
- SHA
- SSL
- PGP
- SSH

Key Terms

- **Plain Text/Clear Text**
  - **Original message unencrypted**
- **Cipher Text**
  - **Message that has been transformed by a cipher algorithm**
- **Algorithms**
  - **Formula and discrete steps describing the encryption and decryption process**
  - **i.e. Diffie Helman**
- **Keys**
  - **Discrete piece of info, random in nature, determines the result of output given a cryptographic operation, used to open or unlock an encrypted message**

Symmetric Cryptography

- DES
- Triple DES
- Blowfish
- IDEA
- RC2
- RC3
- RC4
- RC5
- RC6
- AES (Rijndael)
- Twofish

Asymmetric (Public Key) Cryptography

- How does it work?
  - Alice sends a message to Bob after encrypting it with Bob's public key
  - Bob uses his private key to decrypt her message
  - Hash function creates a digital signature to authenticate the message
- Authenticating the Certificate
  - Binding a keypair with a user
- Enter the PKI System
- Building a PKI Structure

Hashing

- MD2
- MD4
- MD5
- MD6
- HAVAL
- RIPE-MD
- SHA-0
- SHA-1
- SHA-2

Attacks – Issues with Cryptography

- Cipher-Text-Only Attack
- Known Plaintext Attack
- Chosen Plaintext Attack
- Chosen Cipher-Text Attack

IPsec

- Set of protocols designed to protect the confidentiality and integrity of data as it flows over a network
- Network layer of OSI model
- Authentication Header
  - Provides services to authenticate data and the sender
- Encapsulating Security Payload
  - Authenticates information and encrypts data

Pretty Good Privacy

- Uses public key encryption
- Email travels to recipient in encrypted form
- Recipient uses PGP to decrypt into plain text
- Can use their private key as a signature
- Can encrypt files using your public key and use your private key to decrypt them

Secure Sockets Layer

- Server presents client with a digital certificate
- Client makes sure the domain name matches
- Once handshake is complete, the client will automatically encrypt all information, which is unreadable in route
- A secret key decrypts the message when it arrives

Summary

- Know the purpose of cryptography
  - Protect the integrity and confidentiality of data
- Understand symmetric vs. asymmetric cryptography
  - Know which is suitable for which situation
- Know your tools and terms