Encryption 101

WAVV 2008

Tony Thigpen - TEI
Jeff Barnard – BSI

Who we are

- Tony Thigpen
  - Thigpen Enterprises, Inc
  - Dino-Protect since 2004
- Jeff Barnard
  - Barnard Software, Inc.
  - Data-Crypt since 2005

Beginnings

- Plutarch noted that Spartan generals wrote their messages on a narrow strip of parchment wrapped around a thin cylinder ("scytale"). When the parchment was unwound, the message appeared as a nonsense sequence of letters and could only be read by wrapping the parchment around another cylinder of the same size.

Beginnings

- In the fifth century BC, a Greek serving in the Persian court sent a message back to Greece calling for an assassination. The message was delivered, tattooed onto the scalp of a trusted slave who had grown his hair back.

Beginnings

- The Greeks also provide the first recorded use of ciphers using numerical substitutions by writing the alphabet into a grid and then using the grid co-ordinates to substitute for each letter in a message.
- Julius Caesar used a simple substitution cipher, using the normal alphabet, but swapping one letter for another.

Modern Methods

- Since WWII, mechanical methods have become more common and are now more prevalent than manual systems.
  - German Enigma machine
- Computer based encryption
  - DES
  - AES
  - Many many others

Keys

- Symmetric vs. Asymmetric
  - Symmetric – one key
  - Asymmetric – two keys
  - Asymmetric “one way” – one key
    - Used for passwords
  - Hash Algorithms
- Length
  - Anything less than 128bits is not secure

Symmetric

- Works well for “in-corporate” data
- Used by many of today’s encryption
  - RC4
  - AES

Asymmetric

- Best choice for “extra-corporate” data transfer
- Public” vs. “Private” keys
  - Data is encrypted using the Public key
  - Data is decrypted using the Private key
- Generation of keys is CPU intensive
- Used by SSL

Key Management

- Key management is usually a larger problem than the encryption itself

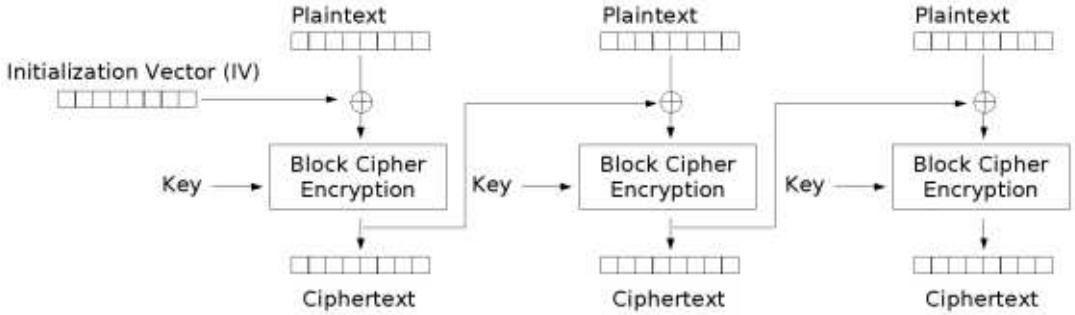
Ciphers

- Character
  - Each character is individually encrypted
  - Can generate recurring characters
- Block
  - A set length block of characters is encrypted as a set
  - Can generate repeating groups of characters
- Stream
  - Adjusts the encryption based on previous data

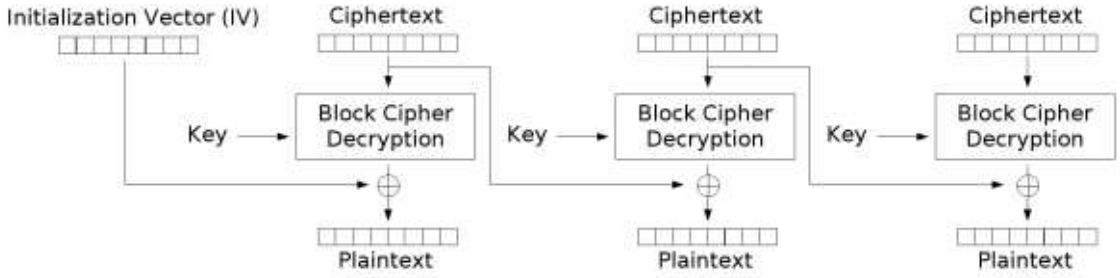
Ciphers

- Modes of operation
  - Used to convert a block cipher into a stream cipher
  - Cipher-block chaining (CBC)
  - Cipher feedback (CFB)
  - Output feedback (OFB)

Ciphers



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

The Internet

- The World Wide Web
- The Internet Threat Model
  - They are out to get you
- The Players
- Goals of Security
  - Confidentially
  - Message Integrity
  - Endpoint Authentication

SSL/TLS

- SSL = Secure Sockets Layer
  - Eric Young
- TLS = Transport Layer Security
  - TLS is SSLv3
- TCP level encryption
- When a connection is made
  - Keys are exchanged
  - Master Key created
- All data encrypted using the Master Key

Key Management

- Public Key Cryptography (PKC)
- Digital Signature
    - Used to 'sign' a message
  - Trusted Third Party
    - Certificate Authority (CA) X.509
      - Issuer name (e.g., Secure Server)
      - Subject name (e.g., Amazon.com)
      - Subject Public Key
      - Digital Signature
      - Expiration date, etc.

OPENSSL

- www.openssl.org
- Standard implementation
- Base for most other implementations
- Authored by Eric Young
- Available for virtually all platforms
- Open source

Hardware Support

- CP Assist for Cryptographic Function (CPACF)
  - Encryption instructions
    - New algorithms added as new machines developed
      - DES
      - AES
      - more
  - No charge

Hardware Support

- Encryption co-processors
  - Crypto Express2
    - Additional cost feature
- Other encryption support
  - Tape drives
    - Monday 9:15 “z/VSE Security Part 2”
    - Tuesday 9:15 “z/VM Tape hardware - Encryption”

Software Encryption

- Software implementations are slower than dedicated hardware
- BSI, CSI, and TEI all support ‘smart’ encryption routines that will use hardware encryption when available yet switch to software based routines if the hardware is not present