2.8

Wednesday, September 20, 2023 6:16 PM

Symmetric algos

- Data encryption standard DES
  - symmetric block cipher
  - 64-bit blocks
  - 56-bit key

3DES - plaintext encrypted 3 times using diff subkeys

- Advanced Encryption Standard
  - AES
  - symmetric block cipher
  - block size 128 bit
  - key size 128, 192, or 256

faster & more secure than DES

Asymmetric algo's

- RSA

  creates digital signatures

- DSA

ECDHE = ECC w/ D-H ephemeral mode

ephemeral keys = perfect forward secrecy

ECC is better than RSA but keys can be compromised and affect all comms

Cryptography prevents single point of

Cryptography prevents single point of fail

Side channel attack - monitor timings like timing, power consume, and electro-magnet w/ physical relation

ECDHE = ephemeral key

ECDH = not ephemeral key

ephemeral only works if client & server support ephemeral keys

RSA / AES supported by browsers

embedding watermarks is example

embedding watermarks

of steganography

used by counterfeit deterrence systems

encode messages within tcp packet data also steganography

Electronic code book ECB - mode of operation that processes encryption in blocks

Cipher block chaining CBC - mode of operation using IV

output of first block combined w/ next block.-

intensive and not as fast as ECB

RC4

symmetric stream cipher