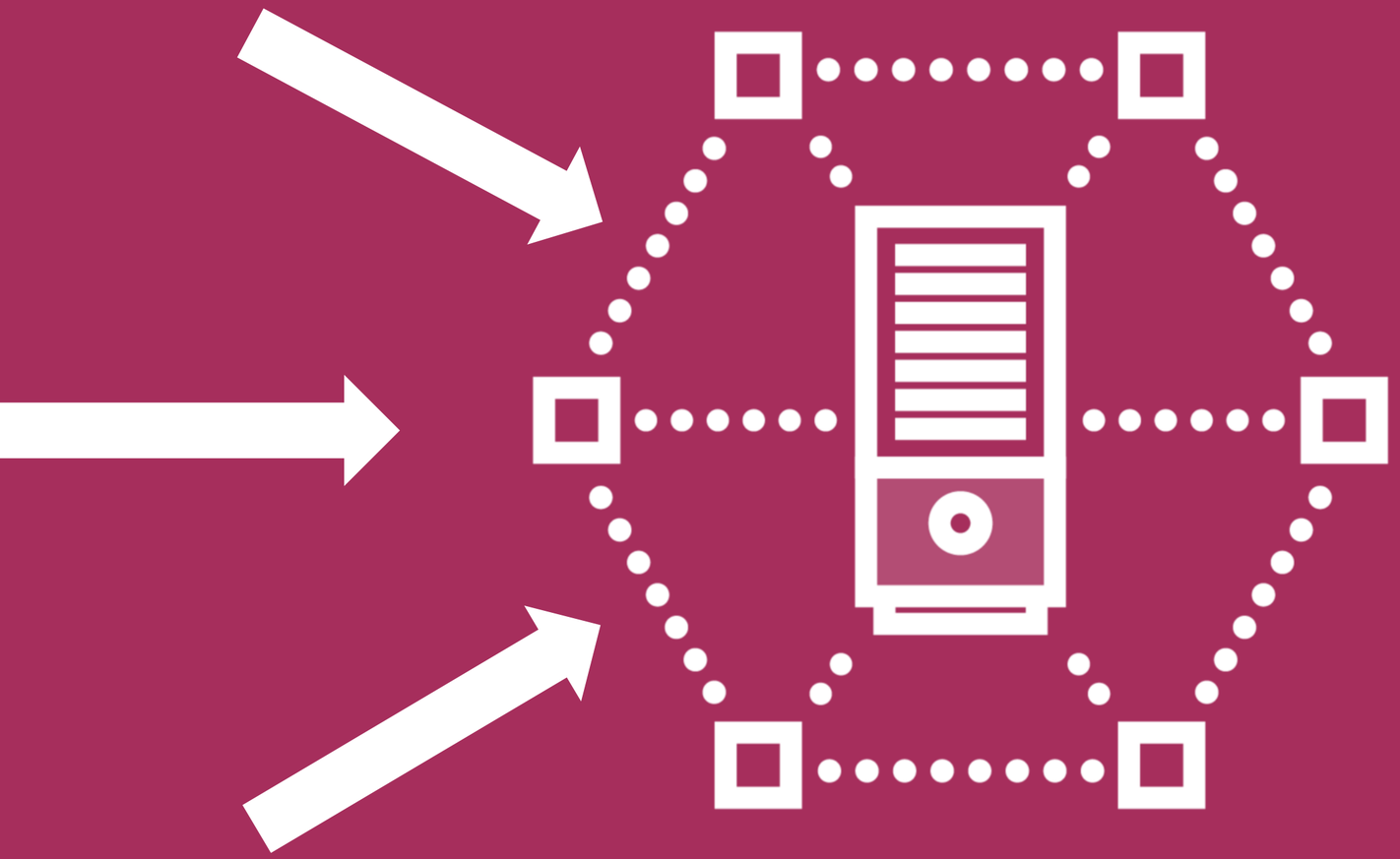
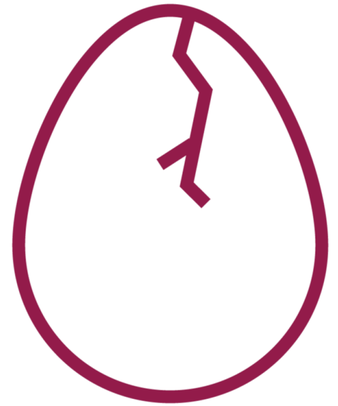
Investigating Cryptanalysis

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith





Identify how the ciphers and cryptosystems are deployed within a particular target

Cryptosystems

A suite of cryptographic algorithms needed to implement a particular security service. A cryptosystem typically consists of three algorithms: one for key generation, one for encryption, and one for decryption.

Cryptanalysis Methods

Linear

Uses a linear approximation

Used on block ciphers

Plaintext attack

Differential

Integral

With enough paired ciphertext information is gathered to reconstruct the key

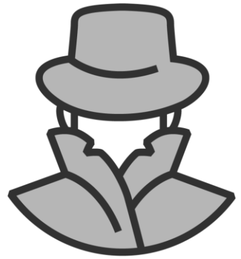
Using brute force a 56-bit DES key could take up to 256 attempts

Cryptanalysis Methods

Linear	Differential	Integral
Uses a linear approximation	Symmetric key algorithms	Useful against block ciphers
Used on block ciphers	Examines differences in the input and it's affect on the output	Based on substitution permutation networks
Plaintext attack	Works with plaintext and ciphertext	Modifications have increased it's capabilities

Code Breaking Methods

Methods



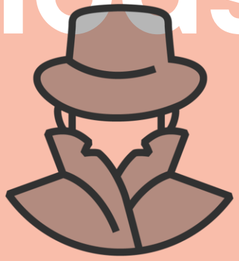
Frequency analysis

Brute force

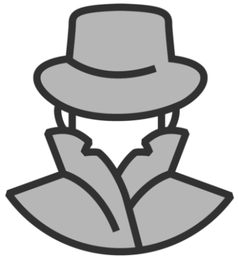
One-time pad

Trickery and deceit

Plaintext



Chosen-ciphertext



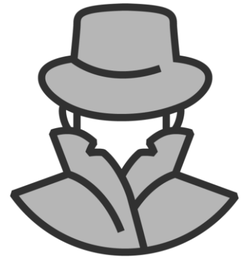
Rubber hose

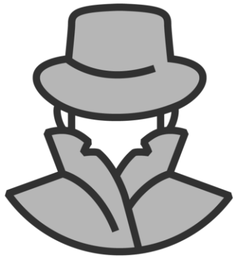
Chosen-key

Plethora

Timing

Man-in-the-middle



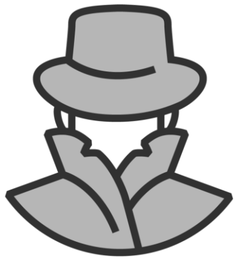


Dictionary

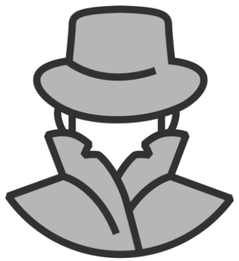
Related-key

Chosen-plaintext

Adaptive chosen-plaintext

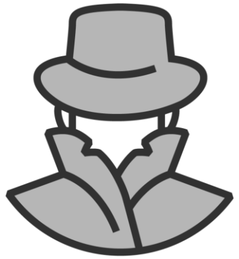


Ciphertext-only



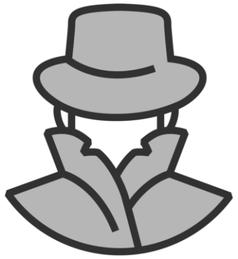
Rainbow table

Plethora



Birthday

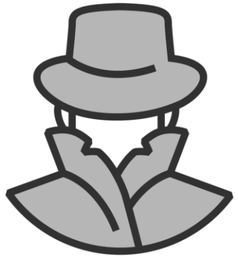
Side-channel



Hash collisions

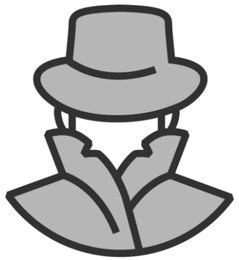
DUHK

Meet-in-the-middle



Padding oracle

DROWN



Cryptanalysis Tools

Cryptanalysis Tools

Cryptools.com

CrypTool 1 (CT1)

CrypTool 2 (CT2)

JCrypTool (JCT)

CrypTool-Online (CTO)

MD5 Decryption Tools

- **MDS Decoder**
- **CrackStation**
- **OnlineHashCrack.com**
- **cmd5.org**

Learning Check

Learning Check

Rubber hose

Frequency analysis

One-time pad

Linear

Differential

Up Next: Reviewing Key Countermeasures