CRYPTOGRAPHY

OBJECTIVES

- CONFIDENTIALITY
- INTEGRITY
- AUTHN & AUTH'Z — PROOF OF ID
- OBFUSCATION — SENSITIVE DATA
- NON-REPUDIATION — ORIGIN & DELIVERY

METHODOLOGY

CLASSICAL

- Transposition
  - groups
  - series
  - columns/rows
  - ciphers: Rail Fence, Route, columnar
- Substitution
  - single
    - Mono alphabetical
      - Atbash
      - Caesar
      - Affine
  - Multiple
    - Poly alphabetical
      - standard alphabet
      - Mix
      - Transformation
      - Progresive — Maquina's Enigma
      - Linear — Vigenere's cipher

KEY TERMS:
- plain text
- cipher text
- key/cryptovariable
- Encryption
- Decryption
- work factor
- Initialization vector
- confusion
- Diffusion

KEY EXCHANGE

out of band	In band
- meet outside - Face to face - USB drives	- Diffie-Hellman - key ESCROW - HSM

MODERN

- Hidden
  - steganography — Hiding data in large files
  - Null cipher — plaintext mixed with large amount of other material/text.
- scrambled
  - 1-way
    - HASHING: MD5, SHA1, SHA2, SHA3
  - 2-way
    - LARGE PRIME NUMBERS
    - SYMMETRIC (PUBLIC KEY)
      - Block
        - CIPHERS
          - DES (64 bit) - Feistel Function - 16 rounds of encryption
          - 3DES (64 bit) - 3x DES, 3 keys - BEING PHASED OUT
          - AES (128 bit) - Rijndael Algorithm - OPEN SOURCE
          - BLOWFISH (64 bit)
          - TWOFISH (128 bit)
      - Stream
        - RC4 - Ron Rivest in 1987 - WEP, WPA, TLS, SSL all support RC4
    - ASYMMETRIC PUBLIC + PRIVATE KEY
      - HARD MATH FACTORING
        - RSA — Rivest Shamir Adelman
        - PGP — sym + Asym
      - DISCRETE LOGS
        - Diffie-Hellman key Exchange
        - ElGamal
        - Elliptic curve → Not based on prime factors
        - DSA Digital Signatures
      - KNAPSACK

MODES

ELECTRONIC CODEBOOK (ECB)	CIPHER BLOCK CHAINING	COUNTER MODE	CIPHER FEEDBACK	OUTPUT FEEDBACK

LEAST SECURE BUT FASTEST

USES INITIALIZATION VECTOR.