



Block Ciphers

Prof. Zeph Grunschlag

Modern Ciphers

Modern ciphers considered successful if all (publicly) known cryptanalytic techniques cannot succeed with better complexity than a brute-force key search.

- Data Encryption Standard (DES)
 - successful relative 56-bit key
 - CPA-resistant relative 55-bit key
 - key-size now too small - “retired”
- Advanced Encryption Standard (AES)
 - key-sizes 128, 192, and 256 bits

Block Cipher

- Defined as a *cryptosystem* with very large plaintext space $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2^n$
- Typically $n \geq 64$ bits
- Round structure
 - Apply same function on intermediate ciphertexts repeatedly N_r times
 - Use different round key K^i defined from K during i 'th round
- Decryption should be similar to encryption

Pseudocode

INPUT: plaintext x , key K

OUTPUT: ciphertext $y = e_K(x)$

ASSUMED: round function g , last round h , key scheduling procedure giving K^i

$$w^0 = x$$

for $i = 1$ to $N_r - 1$

$$w^i = g(w^{i-1}, K^i)$$

$$y = g(w^{N_r-1}, K^{N_r-1})$$

Substitutions

- A **substitution** is a pre-defined random-looking function from length l bitstrings to length k bitstrings
- Stinson defines $l=k$ and insists that the function be bijective - I won't
- Defined using S-boxes on substrings of input - so very efficient in hardware
- Notation
 - S-box: π_S
 - Resulting substitution:

$$\sigma(w) = \pi_S(w_{(1)}) || \pi_S(w_{(2)}) || \cdots || \pi_S(w_{(m)})$$

Coordinate Resampling

- Bits are moved to different locations, and possibly copied, or forgotten
- **permutation**: when domain = codomain
 - Use notation ρ (Greek letter rho)
- **expansion**: when domain < codomain
 - Use notation ξ (Greek letter xi)
- **contraction**: when domain > codomain
 - Use notation κ (Greek letter kappa)

Substitution Permutation Network

- Define substitution σ from predefined S-box
- Predefined permutation ρ
- Round function: $g(w, K^i) = \rho \circ \sigma(w \oplus K^i)$
- Final round - no permutation + whitening:
$$h(w, K) = \sigma(w \oplus K^{N_r-1}) \oplus K^{N_r}$$

Feistel Network - DES

- $N_R = 16$
- Each round breaks intermediate ciphertext w^i into left and right halves w_L^i, w_R^i
- Expansion ξ applied near start of round
- Contracting substitution σ applied mid-round
- Permutation ρ applied near end of round
- Round function:
- $g(w, K^i) = w_R || w_L \oplus \rho(\sigma(\xi(w_R) \oplus K^i))$
- Beginning and end slightly different
 - Apply “initial permutation” IP at start
 - Apply swap and IP^{-1} at end (no key):

$$h(w) = IP^{-1}(w_R || w_L)$$

Rijndael - AES

By Vincent **Rijmen** and Joan **Daemen**

- Initial XOR with first round key
- Substitution $\sigma = \text{SUBBYTES}$ at round-start
- Permutation $\rho = \text{SHIFTRows}$ mid-round
- Linear trans. $\mu = \text{MIXCOLUMNS}$ near end
- Round function: $g(w^i, K^i) = \mu \circ \rho \circ \sigma(w^i) \oplus K^i$
- σ and μ have natural interpretations as field theoretic functions viewing $\mathcal{P} = \mathbb{F}_{2^8}$

Modes of Operation

- ECB - Electronic Code Book
 - Name for doing nothing after encrypting
 - Fails message-indistinguishability
 - Motivates need for randomization in other three modes
- Technically, CBC, CFB, OFB are “stream” ciphers

CBC

Cipher Block Chaining

- First block $y_0 =$ rand. initialization vector (IV)
- Cipher block formula:

$$y_i = e_K(y_{i-1} \oplus x_i)$$

OFB and CFB

OFB: Output Feed-Back

- IV z_0 generates key-stream XOR'ed with plaintexts: $z_i = e_K(z_{i-1})$
- Cipher block formula: $y_i = x_i \oplus z_i$
- **Synchronous** stream cipher

CFB: Cipher Feed-Back

- IV y_0
- Similar to OFB but key-stream generated from cipher blocks: $z_i = e_K(y_{i-1})$
- Cipher block formula: $y_i = x_i \oplus z_i$
- **Asynchronous** stream cipher