Block ciphers and modes of operation. DES, AES.

PV018

Vašek Matyáš

External resources

- Figures used:

  http://williamstallings.com/Security2e.html

- Some slides provided by Henric Johnson, Blekinge Inst. of Techn., Sweden (link above)

- AES standard, etc. (2 presentations in-class)

  http://csrc.nist.gov/CryptoToolkit/aes/rijndael/misc/nissc2.pdf

Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm!
  - Kerckhoff principle

Conventional Encryption Principles

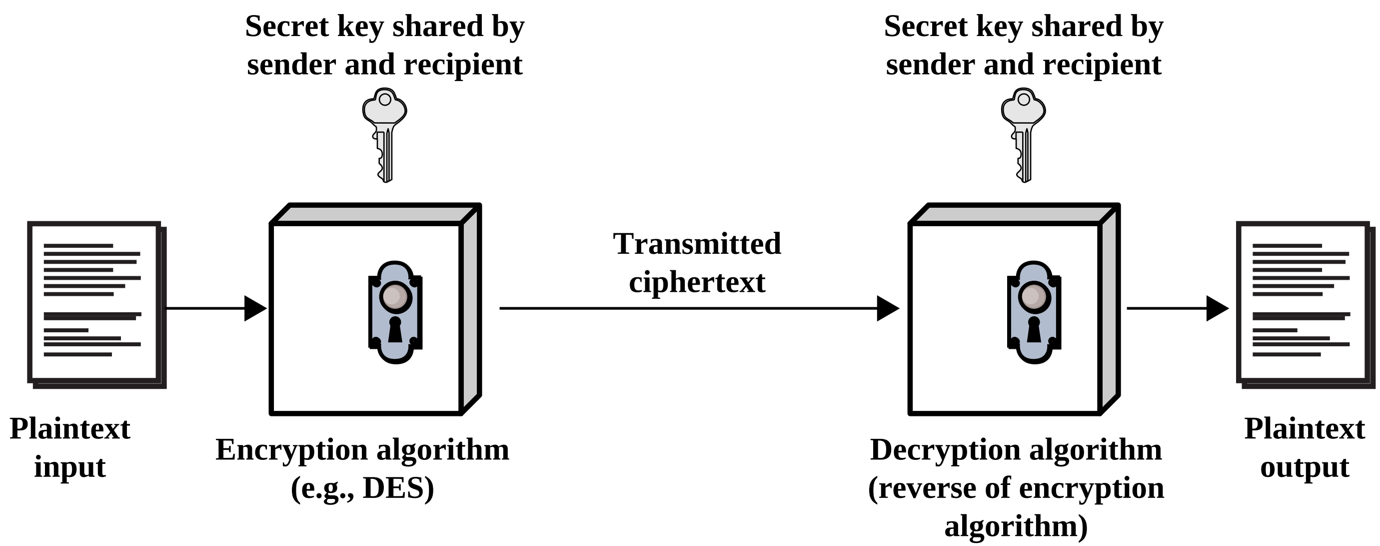


Figure 2.1 Simplified Model of Conventional Encryption

Cryptography

- Classified along three independent dimensions:
  - The type of operations used for transforming plaintext to ciphertext
  - The number of keys used
    - symmetric (single key)
    - asymmetric (two-keys, or public-key encryption)
  - The way in which the plaintext is processed

Average time required for exhaustive key search

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/µs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Feistel ciphers

- Block manipulation, with the block
  - Not too small – cipher would not be complicated
  - Not too big – permutations would be complicated
- Substitution performed on left half of data
  - Round function applied on the right half
  - XORing with the left half
- Permutation – exchange of the two halves

- Parameters: key size, block size, number of rounds

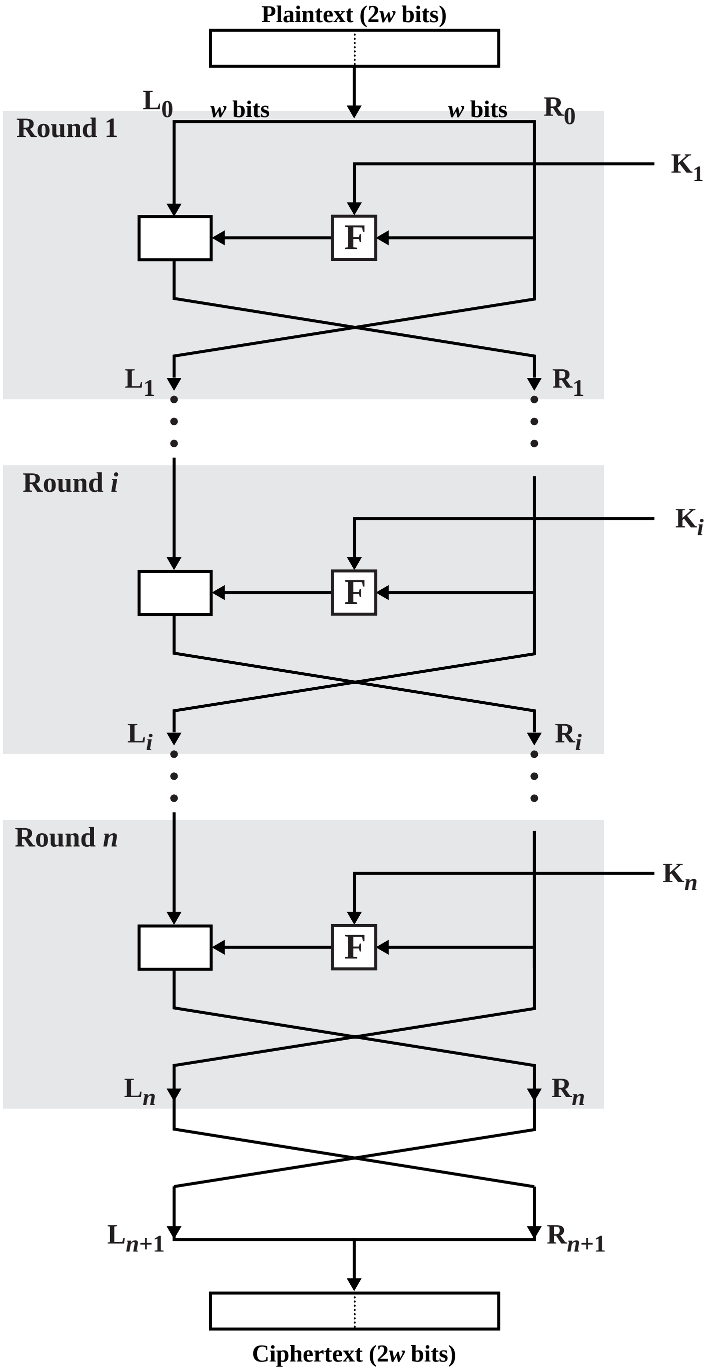


Figure 3.5 Classical Feistel Network

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - The algorithm is reffered to the Data Encryption Algorithm (DEA)
  - DES is a block cipher
  - The plaintext is processed in 64-bit blocks
  - The key is 56-bits in length

DES – Data Encryption Standard

- IBM cipher LUCIPHER, modified(!)
  - LUCIPHER – H. Feistel, project for Lloyd's Bank (UK)
  - 128bit key-length reduced to 56 bits
  - Design of S-boxes classified
- US standard in 1977, last renewal in 1994
  - NBS/NIST – FIPS PUB 46
- 64 bit blocks of input/output
- 56 bit key (64 with parity bits)
- Weak keys (4): $E_k(x) = x$
- Semi-weak keys (6 pairs): $E_{k_2}(E_{k_1}(x)) = x$

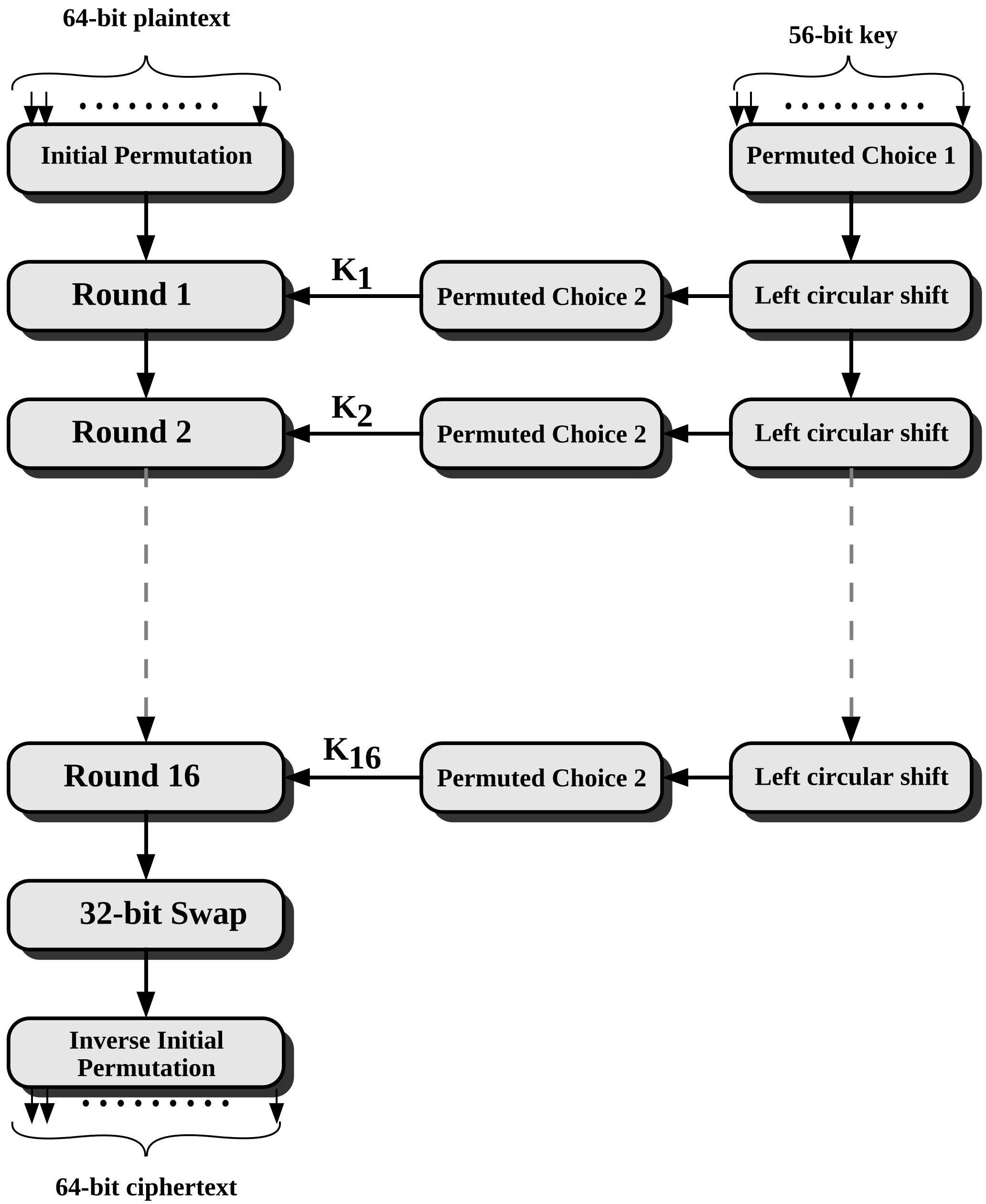


Figure 3.7 General Depiction of DES Encryption Algorithm

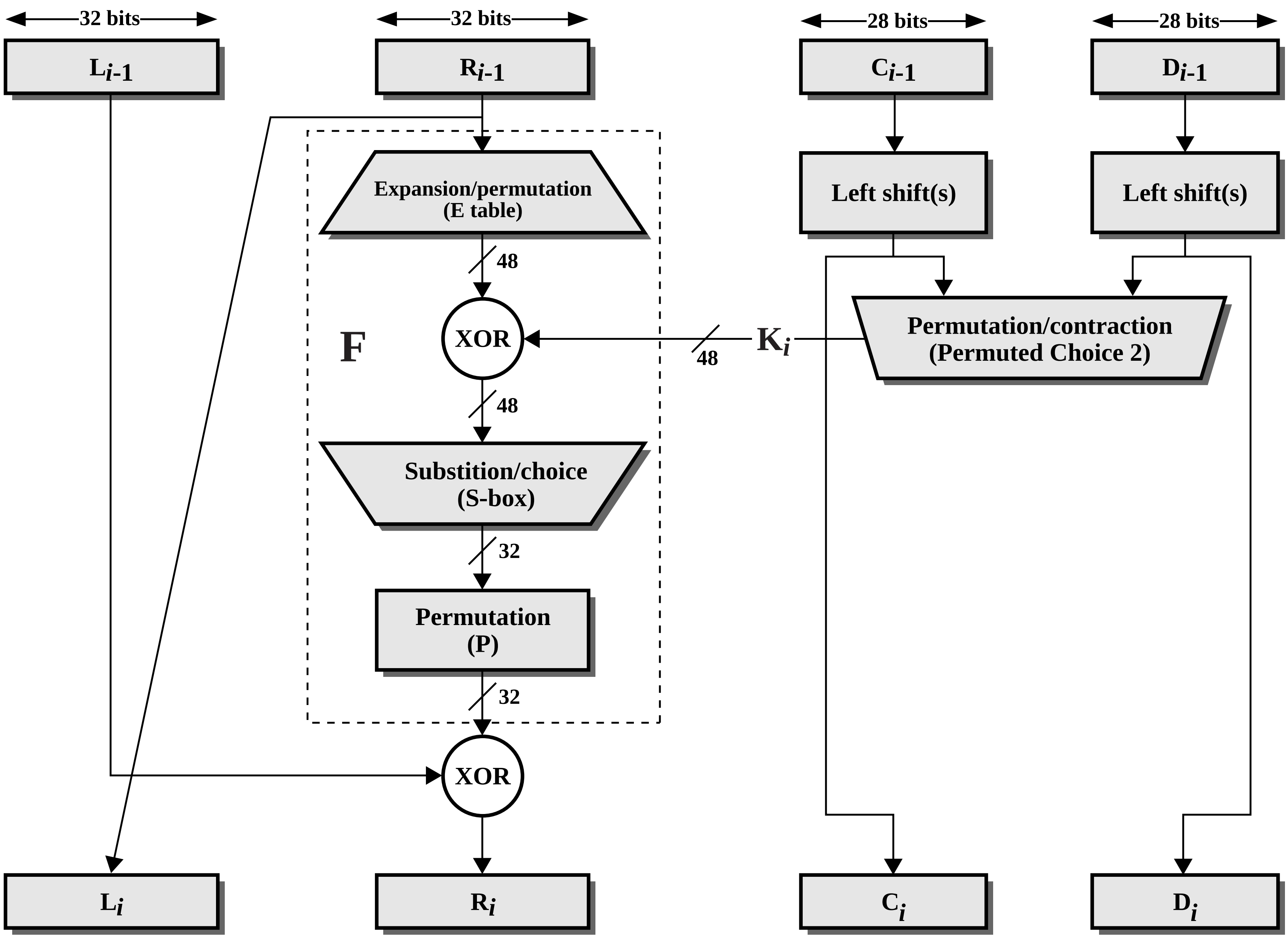
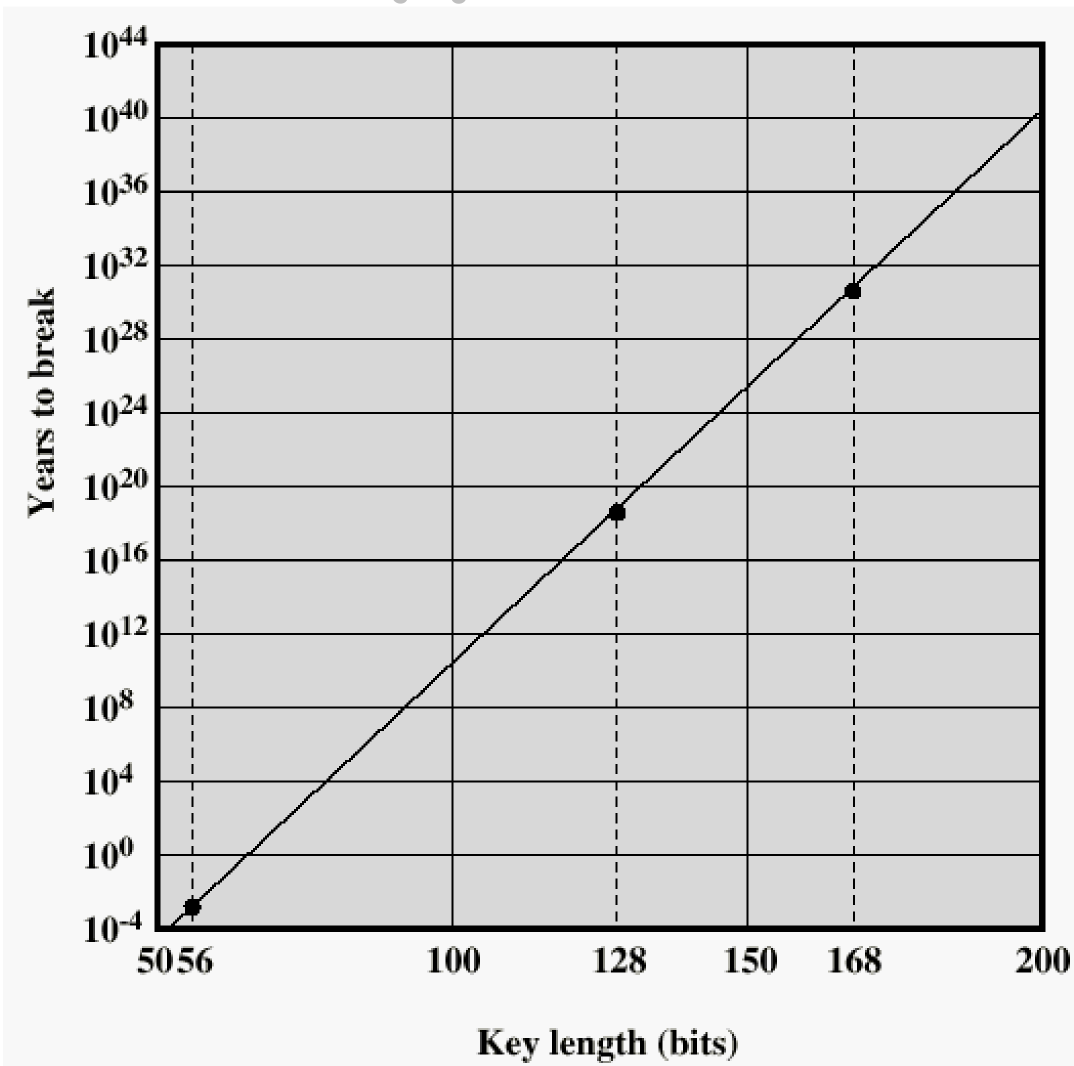


Figure 3.8 Single Round of DES Algorithm

DES

- **The overall processing at each iteration:**
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \otimes F(R_{i-1}, K_i)$
- Concerns about:
  - The algorithm and the key length (56-bits)

Time to break a code (10^6 decryptions/µs)



Breaking DES

- 1977 Diffie & Hellman – design ($20M)
- 1993 M. Wiener – chip design
  - $10M – 21 minutes
  - $1M – 3.5 hours
  - $100k – 35 hours
- 1997 DES-breaking, 70’000 systems, 96 days
- 1998 EFF DES-breaking machine built
  - Special circuits, PC-master
  - $200’000
  - Breaking keys in single hours

DES-based ciphers

- Double DES: $E_{k_2}(\ E_{k_1}(x))$
- Triple DES (3-DES-3):
  - Diffie-Hellman: $E_{k_3}(\ E_{k_2}(\ E_{k_1}(x)))$
  - <u>Merkle:</u> $E_{k_3}(\ D_{k_2}(\ E_{k_1}(x)))$
- **<u>Triple DES (3-DES-2):</u>** $\mathbf{E_{k_1}(\ D_{k_2}(\ E_{k_1}(x)))}$

DES cryptanalysis

- Linear cryptanalysis
  - Finding a linear approximation of DES transformation
  - Matsui, Eurocrypt'93
  - DES key can be found from 2^{47} known plaintexts
- Differential cryptanalysis
  - Starting with two plaintext with known XOR difference
  - Determining key bits one after another
  - Murphy ('90), Biham-Shamir (93)
  - Only successful against DES up to eight rounds (2^{14} chosen plaintexts then needed)
  - Standard DES – $O(2^{47})$, 2^{47} chosen plaintexts needed

Other block ciphers

- IDEA: 128bit key, blocks of 64 bit
- Blowfish: variable key-length up to 448 bits, 64bit blocks, fast, relatively compact (runs in less than 5K of memory)
- RC5: variable key-length up to 2040 bits, 32-,64-, 128-bit blocks, fast, simple
- CAST-128: variable key-length 40-128 bits (mult. 8), 64bit blocks
- RC2, GHOST, LOKI, FEAL,SQUARE

(DES) Modes of operation – Block Modes

- **Electronic Codebook Book (ECB)**
  - the message is broken into independent 64-bit blocks that are individually encrypted
  - $C_i = DES_{K1}(P_i)$

- **Cipher Block Chaining (CBC)**
  - the message is also broken into 64-bit blocks, but these are linked together in the encryption operation (starting with an initial vector/value IV)
  - $C_i = DES_{K1}(P_i \otimes C_{i-1})$, where $C_{-1} = IV$

(DES) Modes of operation – Stream Modes

- **Cipher FeedBack (CFB)**
  - the message is treated as a stream of bits, added to the output of the DES, with the result being fed back for the next stage
  - $C_i = P_i \otimes DES_{K1}(C_{i-1})$, where $C_{-1} = IV$

- **Output FeedBack (OFB)**
  - the message is also treated as a stream of bits, added to the message, but with the *feedback being independent of the message*
  - $C_i = P_i \otimes O_{i,}$ where $O_i = DES_K(O_{i-1})$, and $O_{-1} = IV$

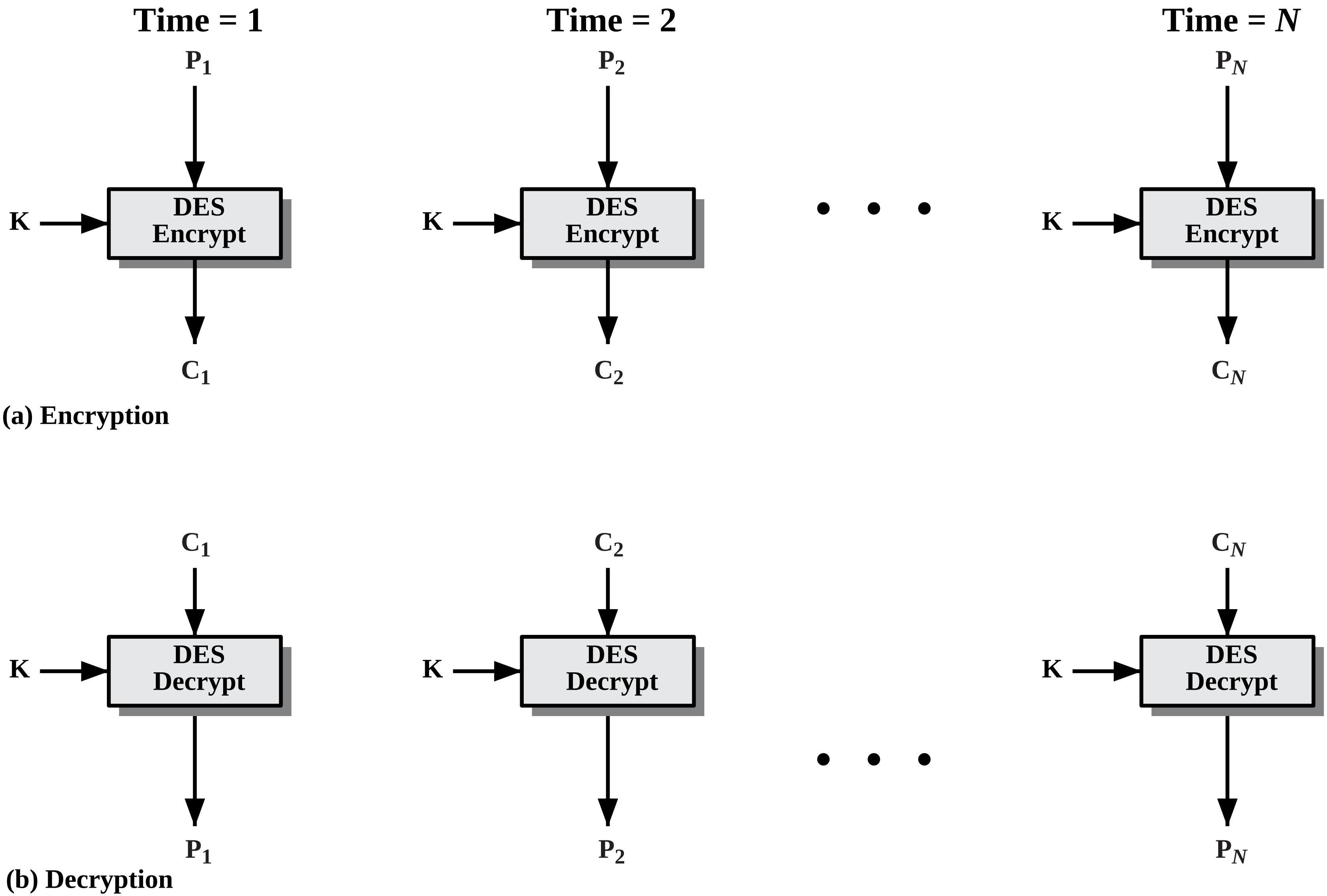


Figure3.11 Electronic Codebook (ECB) Mode

ECB issues

- Repetitions in message can be reflected in ciphertext!!!
  - E.g., with messages that change very little, which become a code-book analysis problem
- Reason – enciphered message blocks are independent of each other.

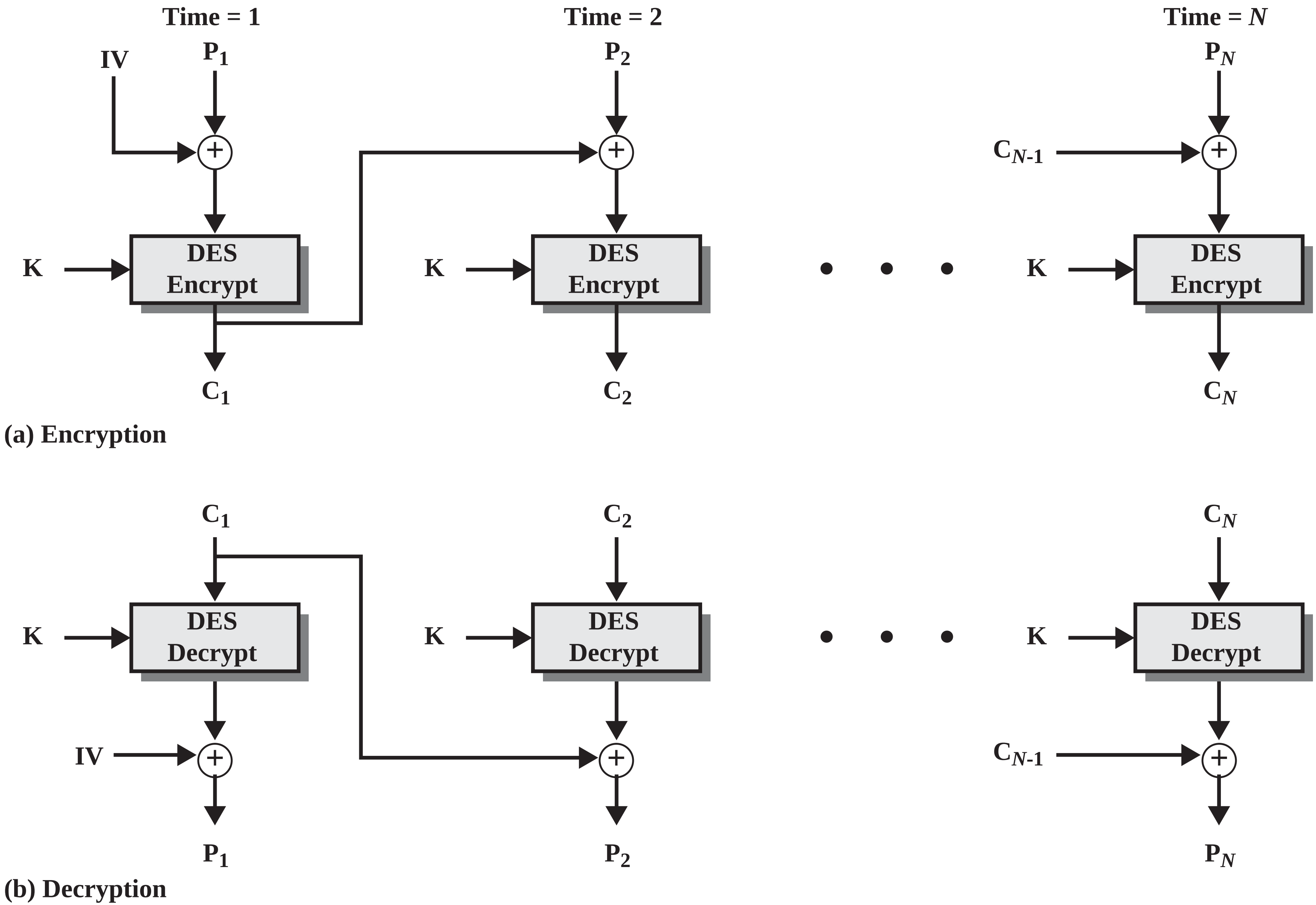


Figure 3.12 Cipher Block Chaining (CBC) Mode

CBC issues

- Each ciphertext block is dependent on *all* message blocks before it
  - I.e., a change in the message affects the ciphertext block after the change as well as the original block.
- *Initial Value* (IV) must be known by both sender and receiver!
  - IV cannot be sent in clear – must either be a fixed value or be sent encrypted in ECB mode before rest of message
- Caution – end of the message, have to handle a possible last “short” block – *padding*.

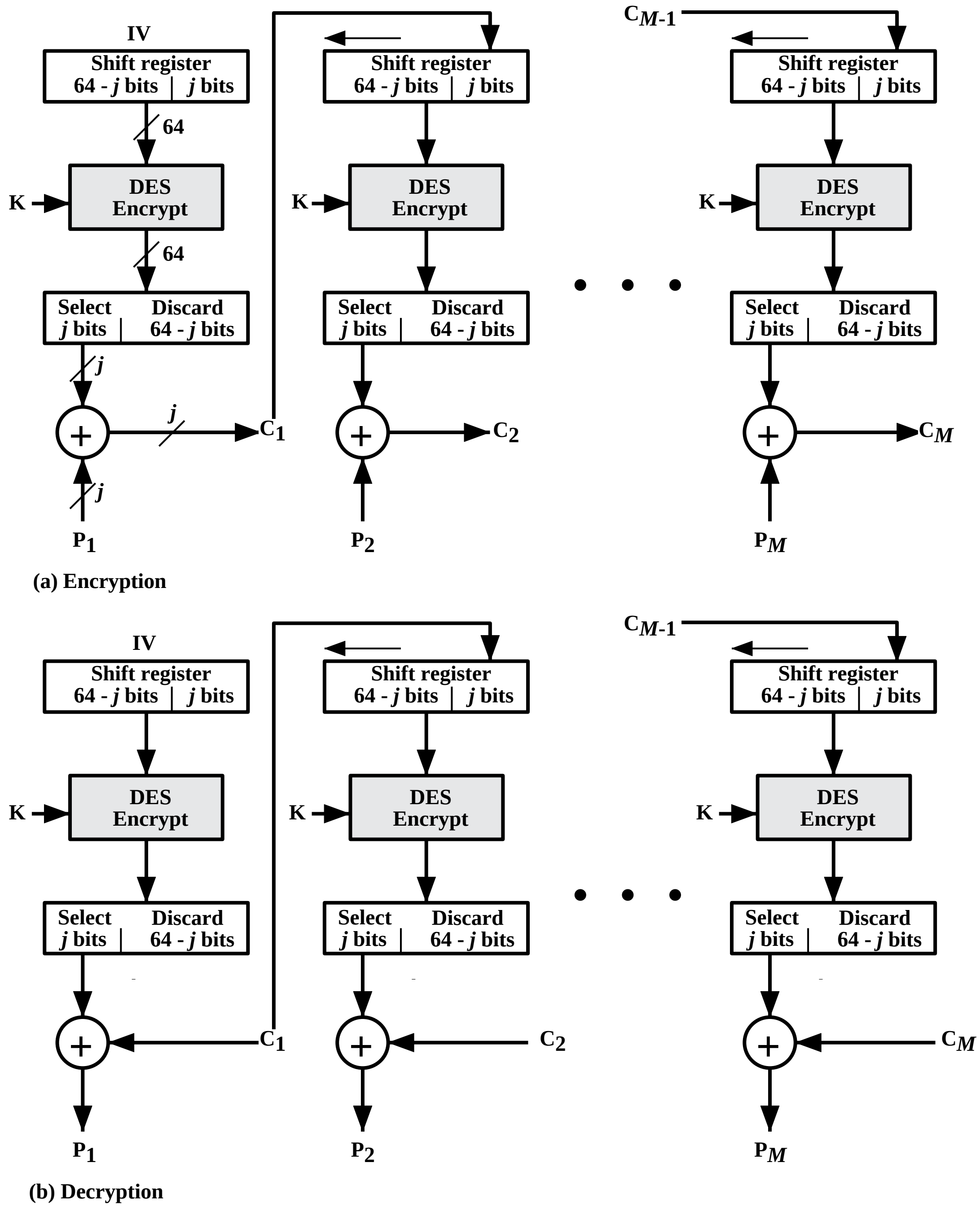


Figure 3.13 J-Bit Cipher Feedback (CFB) Mode

CFB issues

- Use when data is bit or byte oriented – a stream mode.
- The block cipher is use in *encryption mode at both ends*, with input being a feed-back copy of the ciphertext
- Can vary the number of bits fed back, trading off efficiency for ease of use.
- Errors also propagate for several blocks after the error (given by the size of feedback register and shift value).

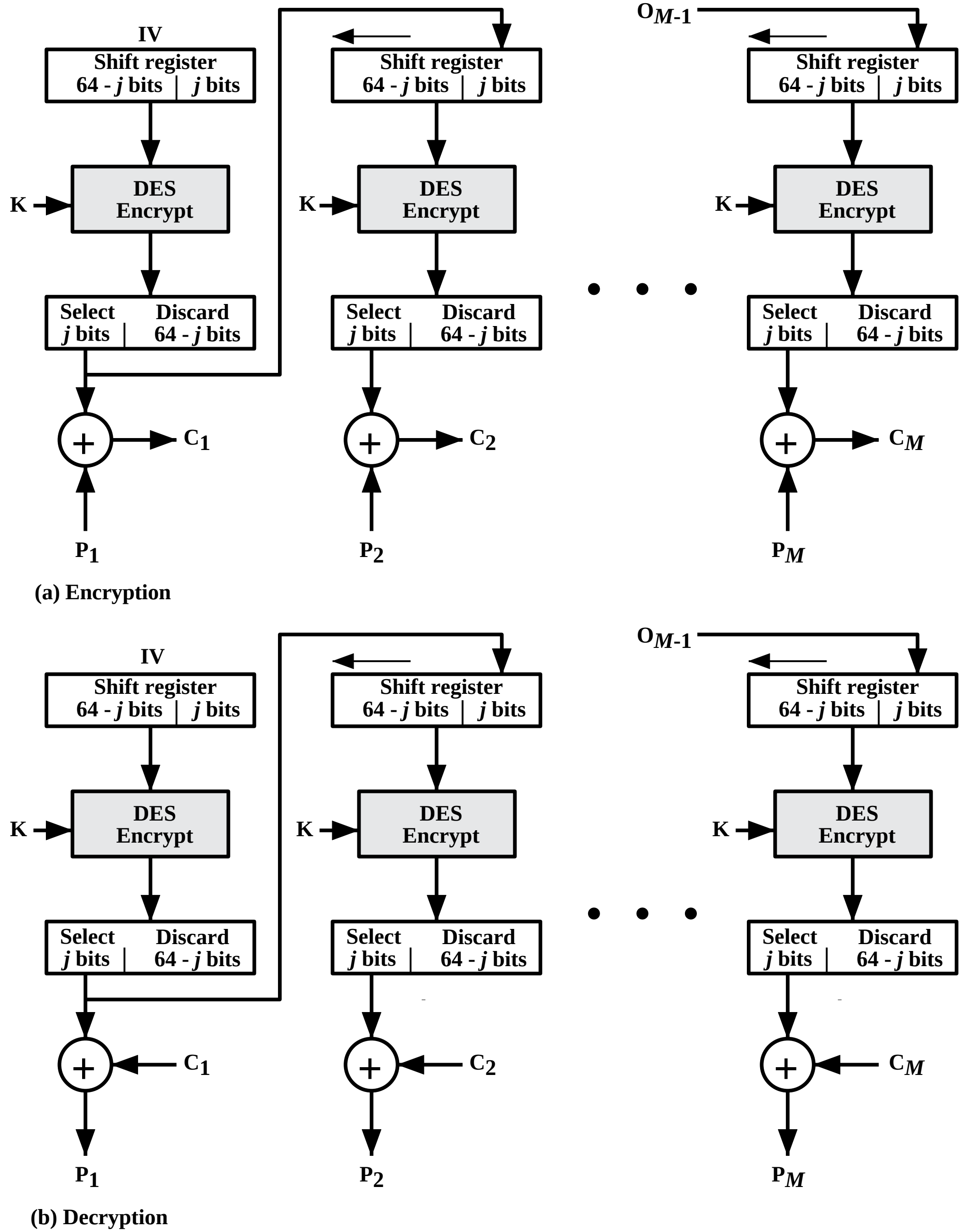


Figure 3.14 J-Bit Output Feedback (OFB) Mode

OFB issues

- Intended for use where the error feedback is a problem, or where the encryptions (expensive operations) should be done before the message is available.
- Difference from CFB: the feedback is from the output of the block cipher and is *independent of the message*, a variation of a Vernam cipher.
- Again, an IV is needed; and sender and receiver must remain in sync, and some recovery method is needed to ensure this occurs!!!

Advanced Encryption Standard Exercise

- Rumors from NIST in 1996
- January 1997 – Official announcement
- September 1997 – Call for Proposals
- August 1998 – 15 candidates announced
- August 1999 – 5 finalists
- 2 October 2000 – Choice of algorithm
- Late 2000, early 2001 – First implementations (PGP 7.0.3)
- Spring 2001 – Standard – FIPS

AES finalists

- MARS (IBM)
  - high security, large ROM req., no good HW impl.
- RC6 (RSA Labs)
  - adequate security, moderate ROM req., average HW impl.
- Rijndael (Rijmnen, Daemen – Belgium!)
  - adequate security, fast-SW, low memory req., fast-HW
- Serpent (Anderson, Biham, Knudsen)
  - high security, low memory req., slow-SW, fast-HW
- Twofish (Schneier et al.)
  - adequate security, high ROM req., average HW impl.

AES-Rijndael

- Input & Output: 128 bits
- Key: 128, 192 or 256 bits
- Processing by bytes – basic units
- Operations – addition (XOR), multiplication
- 10, 12 or 14 rounds (given by key length)
  - Initial Round Key addition
  - Last Round slightly different

AES-Rijndael (cont'd)

- PDF slides from the algorithm authors

http://csrc.nist.gov/CryptoToolkit/aes/rijndael/misc/nissc2.pdf

- Neat Rijndael animation…

http://www.esat.kuleuven.ac.be/~rijmen/rijndael/Rijndael_Anim.zip

Suggested reading

- A Performance Comparison of the Five AES Finalists – B Schneier, D Whiting
- http://csrc.nist.gov/CryptoToolkit/aes/round2/conf3/papers/17-bschneier.pdf