Symmetric Block Ciphers - Algorithm Overview

- Some popular algorithms:
  - Data Encryption Standard (DES)
  - Triple encryption with DES: Triple-DES
  - Advanced Encryption Standard (AES)
  - Twofish
  - Stream Cipher Algorithm RC4

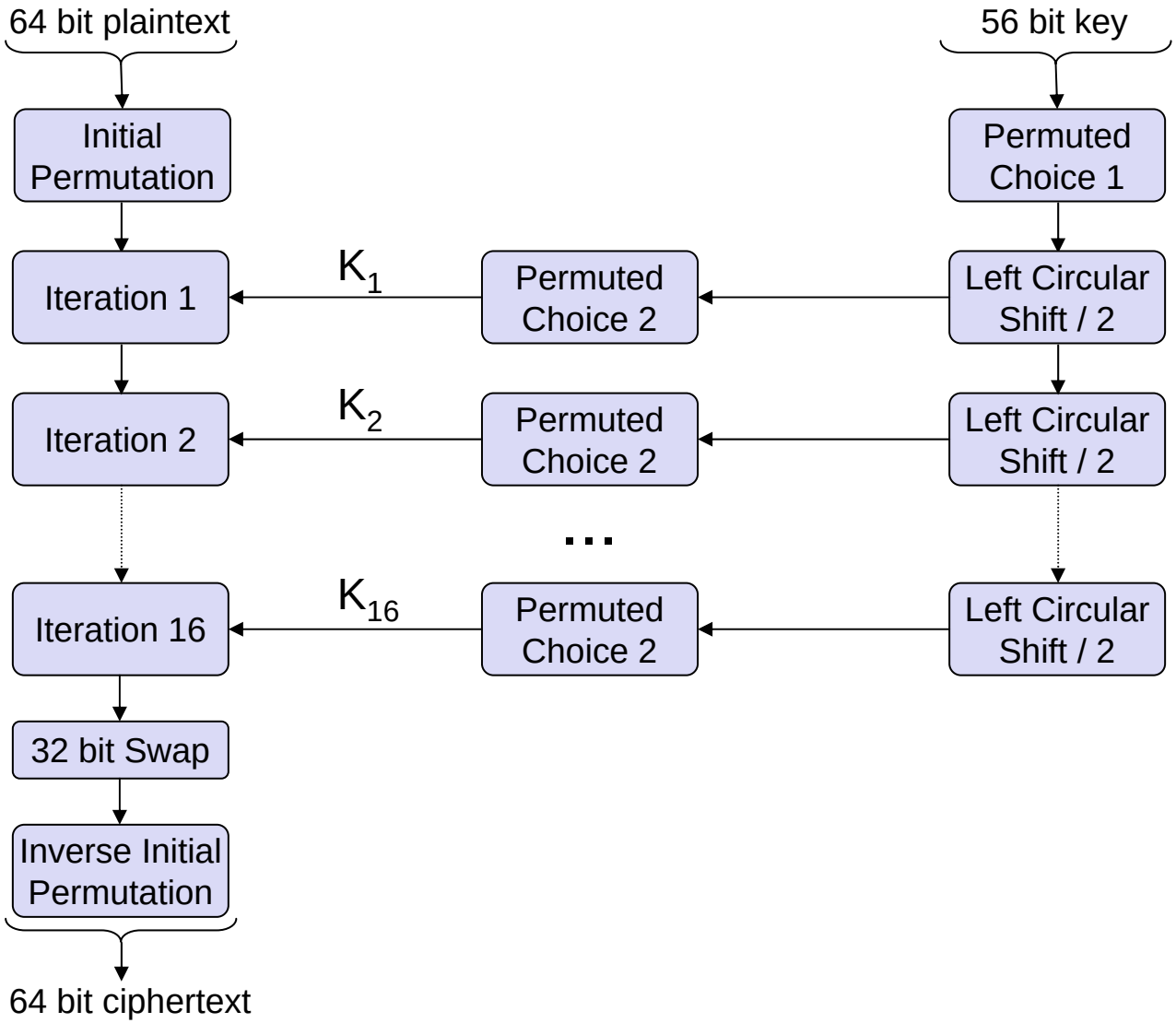
The Data Encryption Standard (DES) – History

- 1973 the National Bureau of Standards (NBS, now National Institute of Standards and Technology, NIST) issued a request for proposals for a national cipher standard, demanding the algorithm to:
  - provide a high level of security,
  - be completely specified and easy to understand,
  - provide security only by its key and not by its own secrecy,
  - be available to all users,
  - be adaptable for use in diverse applications,
  - be economically implementable in electronic devices,
  - be efficient to use,
  - be able to be validated, and
  - be exportable.
- None of the submissions to this first call came close to these criteria.
- In response to a second call, IBM submitted its' algorithm LUCIFER, a symmetric block cipher, which works on blocks of length 128 bit using keys of length 128 bit and that was the only promising candidate

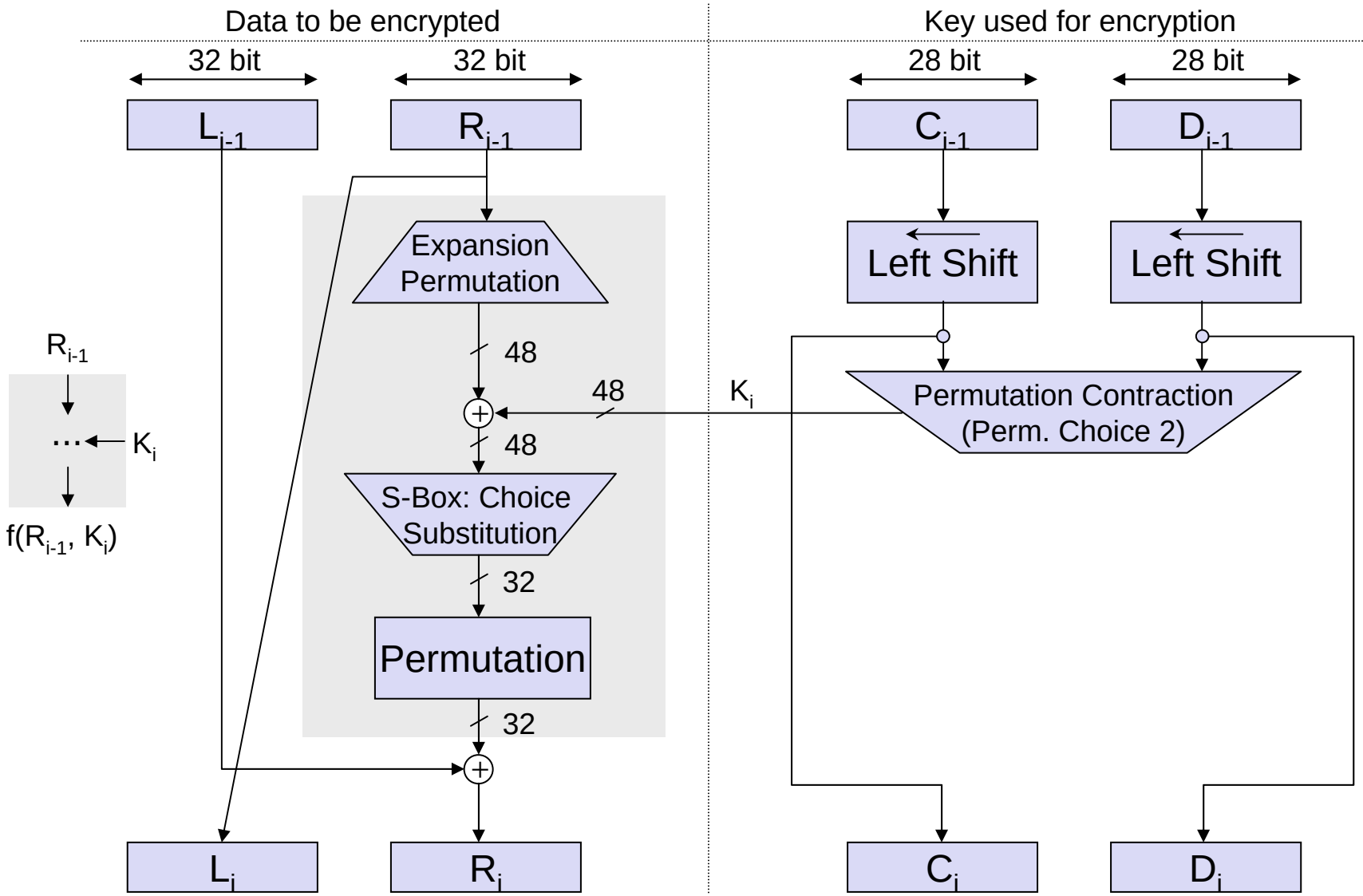
DES – History continued

- The NBS requested the help of the National Security Agency (NSA) in evaluating the algorithm's security:
  - The NSA reduced the block size to 64 bit, the size of the key to 56 bit and changed details in the algorithm's *substitution boxes.*
  - Many of the NSA's reasoning for these modifications became clear in the early 1990s, but raised great concern in the late 1970s.
- Despite all criticism the algorithm was adopted as "Data Encryption Standard" in the series of Federal Information Processing Standards in 1977 (FIPS PUB 46) and authorized for use on all unclassified government communications.
- DES was widely adopted in the years to follow

DES – Algorithm Outline



DES – Single Iteration



DES – Security

- Main weakness is the key length:
  - As a 56 bit key can be searched in 10.01 hours when being able to perform 10^6 encryptions / μs (which is feasible today), DES can no longer be considered as sufficiently secure
- *Differential cryptanalysis:*
  - In 1990 E. Biham and A. Shamir published a cryptoanalysis method for DES
  - It looks specifically for differences in ciphertexts whose plaintexts have particular differences and tries to guess the correct key
  - The basic approach needs **chosen plaintext** together with its **ciphertext**
  - DES with 16 rounds is immune against this attack, as the attack needs 2^{47} chosen plaintexts or (when “converted” to a known plaintext attack) 2^{55} known plaintexts.
  - The designers of DES told in the 1990s that they knew about this kind of attacks in the 1970’s and that the S-boxes were designed accordingly

Extending the Key-Length of DES by Multiple Encryption

- Triple encryption scheme, as proposed by W. Tuchman in 1979:
  - $C = E(K_3, D(K_2, E(K_1, P)))$
  - The use of the decryption function *D* in the middle allows to use triple encryption devices with peers that only own single encryption devices by setting $K_1 = K_2 = K_3$ (backwards compatibility with DES)
  - Triple encryption can be used with two (set $K_1 = K_3$) or three different keys
  - There are no known practical attacks against this scheme up to now
  - Drawback: the performance is only 1/3 of that of single encryption, so it should be a better idea to use a different cipher, which offers a bigger key-length right away
- Double encryption is not a feasible option – there is an attack against it (Meet-in-the-middle-attack)

The Advanced Encryption Standard AES (1)

- Jan. 1997: the *National Institute of Standards and Technology (NIST)* of the USA announces *the AES development* effort.
  - The overall goal is to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm(s) capable of protecting sensitive government information well into the next century.
  - The algorithm(s) is expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.
- Sep. 1997: formal *call for algorithms*, open to everyone
  - AES would specify an unclassified, publicly disclosed encryption algorithm(s), available royalty-free, worldwide.
  - The algorithm(s) must implement symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bits and key sizes of 128-, 192-, and 256-bits.
- Aug. 1998: first AES candidate conference
  - NIST announces the selection of 15 candidate algorithms
  - Demand for public comments

The Advanced Encryption Standard AES (2)

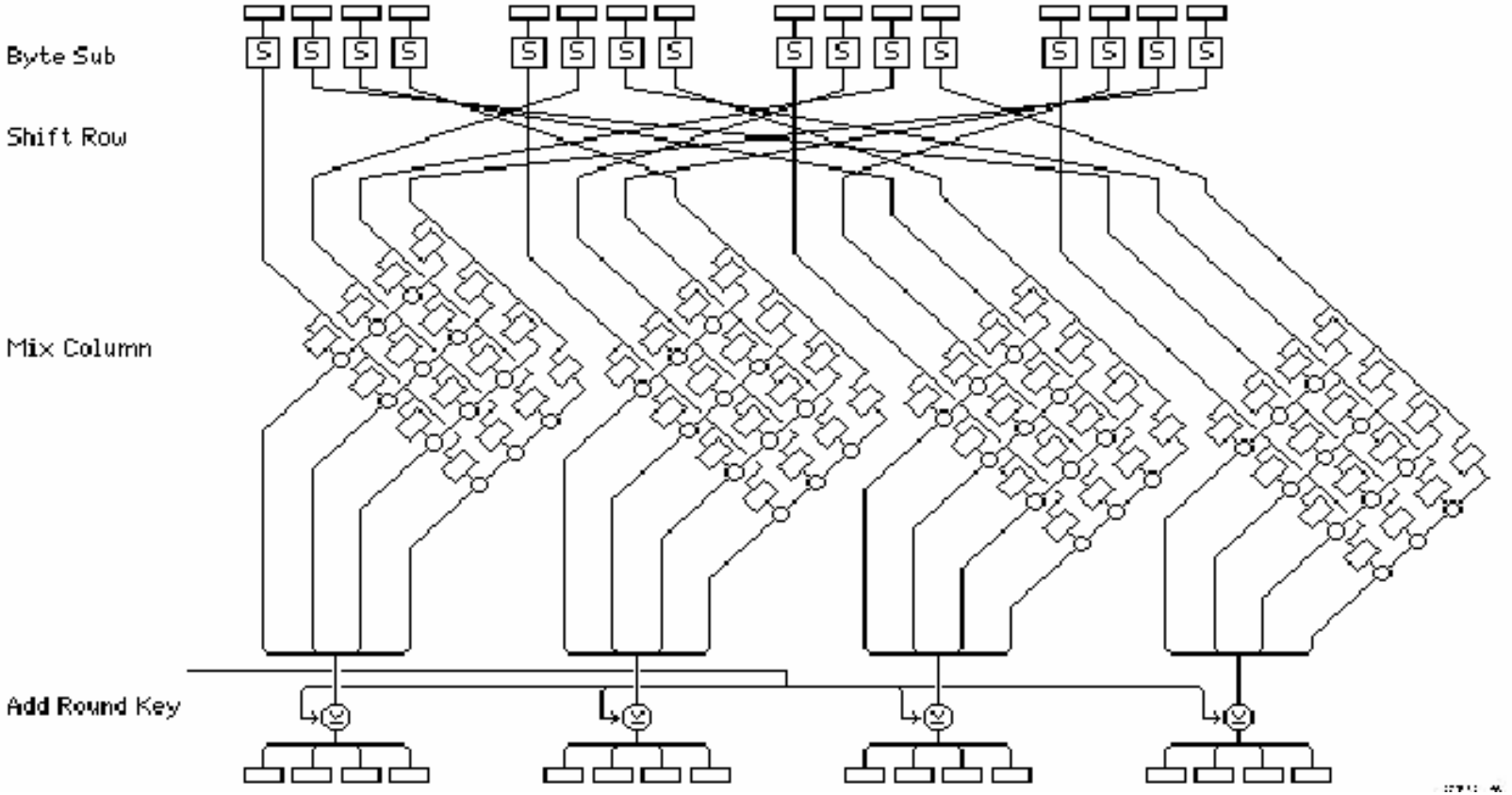
- Mar. 1999: second AES candidate conference
  - Discussion of results of the analysis conducted by the global cryptographic community on the candidate algorithms.
- April 1999:
  - Using the analyses and comments received, NIST selects five algorithms as finalist candidates: *MARS, RC6, Rijndael, Serpent,* and *Twofish*
  - Demand for public comments on any aspect of the finalists:
    - Cryptanalysis
    - Implementation issues
    - Intellectual property & Overall recommendations
- May 2000: third AES candidate conference
- October 2000: Rijndael is announced as NIST's proposal for AES
- 28. February 2001: draft FIPS standard is published [AES01a]
- 29. May 2001: comment period ends
- 26. November 2001: official announcement of the AES standard

The Advanced Encryption Standard AES (3)

- Key and block lengths:
  - Key Length: 128, 192, or 256 bit
  - Block Length: 128, 192, or 256 bit
  - In the following only 128 bit is considered
- Number of rounds: 10 (for block and key size of 128 bit)
  - Rounds 1 - 9 make use of four different operations:
    - ByteSub: a non-linear byte substitution (basically an s-box), specifically designed to work against differential and linear cryptanalysis
    - ShiftRow: the rows of the state are cyclically shifted by various offsets → aims to increase diffusion
    - MixColumn: an operation based on polynomial algebra → aims to increase diffusion
    - RoundKey: a round-key is XORed with the state
  - Round 10 does not make use of the MixColumn operation

The Advanced Encryption Standard AES (4)

Structure of one Round in Rijndael



(source: “Rijndael”, a presentation by J. Daemen and V. Rijmen)

Properties of AES

- Roughly 3 times the speed of DES (200 MBit/s vs. 80 MBit/s)
  - Speed was critical in the selection of Rijndael as AES
  - Other ciphers were considered stronger, but slower
  - Rijndael seemed to be the best overall choice
- Can be used in CBC or CTR modes in communication.
- Highly parallel architecture

- From the NIST report:
  - “Rijndael appears to offer an adequate security margin. [There is] some criticism on two grounds: that its security margin is on the low side […], and that its mathematical structure may lead to attacks. However, its structure is fairly simple.”
  - “Twofish appears to offer a high security margin. […] Twofish has received some criticism for its complexity.”

Properties of AES

- Currently still considered secure.
- Until about 2009, AES was considered very secure, but:
  - Its position has been somewhat weakened
    - Description of AES in 8,000 quadratic equations, sparse matrix
      → XSL attack: not workable as such, but has caused some concern
    - Related-key attack on 256 bit AES with 11 rounds
      (full AES has 14 rounds at 256 bit) → does not extend to AES 128 bit, but reduces safety margin
  - A major criticism is that the algebraic description, while elegant, is not well-understood → someone might come up with a linear description
  - Known good attacks are side-channel attacks (timing) – these do not attack the algorithm itself, and are usually impractical
- AES seems to be the best we have, and it is among the most researched algorithms.

Additional References

[AES01a] National Institute of Standards and Technology (NIST). *Specification for the Advanced Encryption Standard (AES).* Federal Information Processing Standards Publication, February 2001.

[DR97a] J. Daemen, V. Rijmen. *AES Proposal: Rijndael.* http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1997.

[FMS01a] S. Fluhrer, I. Mantin, A. Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4.* Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[Riv01a] R. Rivest. *RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4*. http://www.rsa.com/rsalabs/technotes/wep.html, 2001.

[SIR01a] A. Stubblefield, J. Ioannidis, A. D. Rubin. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.* AT&T Labs Technical Report TD-4ZCPZZ, August 2001.