

Cryptography

Symmetric Encryption

Prof. Dr. Heiko Knospe

TH Köln – University of Applied Sciences

April 11, 2025

Block Ciphers

Symmetric ciphers can be divided into *block ciphers* and *stream ciphers*. A *block cipher* encrypts a block of plaintext bits of fixed length l into a block of ciphertext bits, and vice versa:

$$E_k(m_1, m_2, \dots, m_l) = (c_1, c_2, \dots, c_l)$$

$$E_k^{-1}(c_1, c_2, \dots, c_l) = (m_1, m_2, \dots, m_l)$$

Block ciphers are designed to be pseudorandom functions (*prf*). Operations modes (such as ECB, CBC or CTR) then allow the encryption of plaintexts of arbitrary length.

Stream Ciphers

A *stream cipher* takes a key and often also an initialization vector, recursively updates a state and outputs *keystream* bits k_1, k_2, \dots

A plaintext m_1, m_2, \dots is encrypted by XORing with k_1, k_2, \dots

Decryption works similarly.

$$(m_1, m_2, \dots) \oplus (k_1, k_2, \dots) = (m_1 \oplus k_1, m_2 \oplus k_2, \dots) = (c_1, c_2, \dots)$$

$$(c_1, c_2, \dots) \oplus (k_1, k_2, \dots) = (m_1 \oplus k_1 \oplus k_1, m_2 \oplus k_2 \oplus k_2, \dots) = (m_1, m_2, \dots)$$

The keystream produced by a stream ciphers should be pseudorandom, i.e., polynomial-time adversaries should not be able to distinguish between the keystream and a truly random sequence.

CTR Mode

The CTR mode effectively transforms a block cipher into a stream cipher! The keystream is generated by encrypting a randomly chosen counter. By incrementing the counter (i.e., the state) the required number of keystream blocks can be generated.

$$\begin{aligned}ctr &\stackrel{\$}{\leftarrow} \{0, 1\}^I \\(k_1, \dots, k_l) &= E_k(ctr + 1) \\(k_{l+1}, \dots, k_{2l}) &= E_k(ctr + 2) \\&\dots\end{aligned}$$

Native Stream Ciphers

Stream ciphers have been used a lot in the past and they were often quite efficient. Examples include the A5 ciphers (for GSM encryption) and RC4 (previously used for network data encryption). However, these ciphers have cryptographic weaknesses and they are deprecated now.

A new generation of stream ciphers is under investigation, but new ciphers are not yet standardized. A promising candidate is the *Salsa20 family of stream ciphers*, in particular the high-speed cipher *ChaCha20* (see [RFC 7539](#)), which is already used in the network security protocols TLS, SSH and IPsec as an alternative to AES.

Block Ciphers

A block cipher is a *keyed family of permutations*, which is designed to behave like a pseudorandom permutation (*prp*). Block ciphers operate on a binary string of fixed length and depend on a key:

$$E : \{0, 1\}^n \times \{0, 1\}^l \rightarrow \{0, 1\}^l$$

Today, a block length of $l = 128$ bits and key lengths between $n = 128$ and $n = 256$ bits are used.

Design of Block Ciphers

The bijective encryption functions

$$E_k : \{0, 1\}^l \rightarrow \{0, 1\}^l$$

should be indistinguishable from a true random permutation if k is unknown. The construction of a secure block cipher (a *prp*) is a non-trivial task! *Diffusion* and *confusion* are important design goals of block ciphers.

- Diffusion: Small input changes, e.g., only one bit, result in large output changes (avalanche effect). Plaintext patterns are diffused in the ciphertext.
- Confusion: Complex and non-linear relationship between ciphertext and key, even if plaintext is known. This helps to protect the cipher and the key against cryptanalysis, e.g., by known plaintext attacks and linear approximations.

Confusion and Diffusion

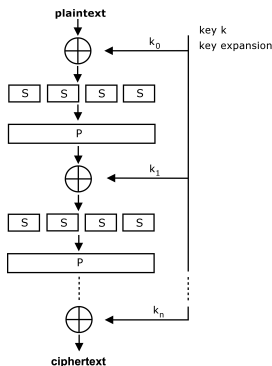
Confusion requires *non-linear* and *non-affine* maps (so-called S-Boxes). Since non-linear maps are difficult to describe on full blocks, S-Boxes usually operate only on small segments of a block and are applied in parallel, e.g., on 8-bit segments of a 128-bit block. In addition, *round keys* are mixed in.

Diffusion can be achieved by linear or affine mixing maps, e.g., using bit permutations, XOR and matrix operations. Such operations can have good diffusion properties and are very efficient. However, without confusion such operations can be easily reconstructed with linear algebra.

Modern block ciphers combine diffusion and confusion operations to obtain a key-dependent non-linear transformation.

Substitution-Permutation Networks

Substitution-Permutation Networks (SPN) implement the confusion-diffusion paradigm. In each round, a round key k_i is added, followed by a non-affine S-Box substitution S and an affine or linear permutation P .



AES Encryption

The block cipher *Rijndael* has been adopted as *Advanced Encryption Standard (AES)* and the cipher is widely used today. The standardized AES cipher has a block length of 128 bits and supports 128-, 192- and 256-bit key lengths. The Rijndael encryption function

$$E_k : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$$

is given by a SPN. The 128-bit *state* is arranged in a 4×4 matrix over $GF(256) = GF(2^8)$ by writing the bytes p_0, p_1, \dots, p_{15} into the columns.

$$\begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{pmatrix}$$

Each byte is interpreted as an element of the field

$$GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1).$$

High-level Description of AES

```
Rijndael(State, CipherKey)
{
    KeyExpansion(CipherKey, ExpandedKey) // Derive the round keys
    AddRoundKey(State, ExpandedKey[0])
    for(i = 1; i < Nr ; i++) {          // Nr is either 10, 12 or 14
        // Round i
        SubBytes(State)
        ShiftRows(State)
        MixColumns(State)
        AddRoundKey(State, ExpandedKey[i])
    }
    // Final Round
    SubBytes(State)
    ShiftRows(State)
    AddRoundKey(State, ExpandedKey[Nr])
}
```

AES S-Box

The AES S-Box `SubBytes` is the only non-affine component of AES.

The invertible S-Box function $S_{RD} : GF(2^8) \rightarrow GF(2^8)$ is applied to each byte of the state individually.

$$\begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{pmatrix} \xrightarrow{\text{SubBytes}} \begin{pmatrix} S_{RD}(p_0) & S_{RD}(p_4) & S_{RD}(p_8) & S_{RD}(p_{12}) \\ S_{RD}(p_1) & S_{RD}(p_5) & S_{RD}(p_9) & S_{RD}(p_{13}) \\ S_{RD}(p_2) & S_{RD}(p_6) & S_{RD}(p_{10}) & S_{RD}(p_{14}) \\ S_{RD}(p_3) & S_{RD}(p_7) & S_{RD}(p_{11}) & S_{RD}(p_{15}) \end{pmatrix}$$

S-Box Function S_{RD}

The definition

$$GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$$

gives a $GF(2)$ -linear isomorphism between $GF(2^8)$ and $GF(2)^8$. The invertible S-Box function is defined by a multiplicative inversion in $GF(2^8)^*$ (which is highly non-linear), followed by an affine map:

$$S_{RD} : GF(2^8) \rightarrow GF(2^8), S_{RD}(a) = \begin{cases} Aa^{-1} + b & \text{for } a \neq 0 \\ b & \text{for } a = 0 \end{cases}$$

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Implementing the S-Box S_{RD}

Lookup table are used for S_{RD} and S_{RD}^{-1} . The (hexadecimal) values of $S_{RD}(0), \dots, S_{RD}(255)$ are:

```
63 7C 77 7B F2 6B 6F C5 30 01 67 2B FE D7 AB 76 CA 82 C9 7D FA 59
47 F0 AD D4 A2 AF 9C A4 72 C0 B7 FD 93 26 36 3F F7 CC 34 A5 E5 F1
71 D8 31 15 04 C7 23 C3 18 96 05 9A 07 12 80 E2 EB 27 B2 75 09 83
2C 1A 1B 6E 5A A0 52 3B D6 B3 29 E3 2F 84 53 D1 00 ED 20 FC B1 5B
6A CB BE 39 4A 4C 58 CF D0 EF AA FB 43 4D 33 85 45 F9 02 7F 50 3C
9F A8 51 A3 40 8F 92 9D 38 F5 BC B6 DA 21 10 FF F3 D2 CD 0C 13 EC
5F 97 44 17 C4 A7 7E 3D 64 5D 19 73 60 81 4F DC 22 2A 90 88 46 EE
B8 14 DE 5E 0B DB E0 32 3A 0A 49 06 24 5C C2 D3 AC 62 91 95 E4 79
E7 C8 37 6D 8D D5 4E A9 6C 56 F4 EA 65 7A AE 08 BA 78 25 2E 1C A6
B4 C6 E8 DD 74 1F 4B BD 8B 8A 70 3E B5 66 48 03 F6 0E 61 35 57 B9
86 C1 1D 9E E1 F8 98 11 69 D9 8E 94 9B 1E 87 E9 CE 55 28 DF 8C A1
89 0D BF E6 42 68 41 99 2D 0F B0 54 BB 16
```

ShiftRows

ShiftRows is a bit-permutation and rotates the bytes in the second, third and fourth row to the left. The first row is left unchanged, the bytes in second row are rotated by one position, bytes in the third row are rotated by two positions and bytes in the fourth row are rotated by three positions. Obviously, *ShiftRows* is invertible.

$$\begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{pmatrix} \xrightarrow{\text{ShiftRows}} \begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_5 & p_9 & p_{13} & p_1 \\ p_{10} & p_{14} & p_2 & p_6 \\ p_{15} & p_3 & p_7 & p_{11} \end{pmatrix}$$

MixColumns

MixColumns transforms the columns of the state by a $GF(2^8)$ -linear map. The product of a constant 4×4 matrix M over $GF(2^8)$ with the current state matrix defines the new state, i.e., each column of the state is multiplied with M and gives the updated column. The matrix M is invertible over $GF(2^8)$.

$$\begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{pmatrix} \xrightarrow{\text{MixColumns}} \underbrace{\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}}_M \cdot \begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{pmatrix}$$

Key Scheduling

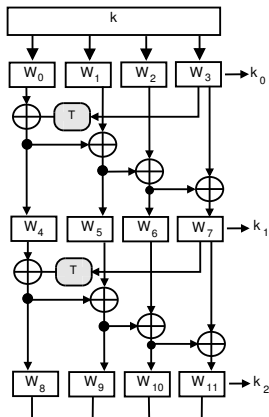
In the key expansion step, the 128-bit round keys k_0, k_1, \dots, k_{N_r} are derived from the AES key k . The round keys ensure that the transformation depends on the key. Note that confusion in the cipher protects the round keys against cryptanalysis.

The AES key scheduling is *non-linear*, which is intended to protect the cipher against *related key attacks*.

Suppose k is a 128-bit AES key. Then AES has ten rounds and eleven 128-bit round keys k_0, k_1, \dots, k_{10} are required. During key expansion, 44 words $W_0, W_1, \dots, W_{43} \in GF(2^8)^4$ of length 32 bits are computed. The round keys are given by

$$k_i = W_{4i} \parallel W_{4i+1} \parallel W_{4i+2} \parallel W_{4i+3} \text{ for } i = 0, 1, \dots, 10.$$

Key Scheduling for 128-bit AES keys



The first two rounds of 128-bit AES key scheduling (round keys k_0, k_1, k_2). T is defined by $T(W_{4i-1}) = \mathbf{S}(sh(W_{4i-1})) \oplus (RC_i, 0, 0, 0)$, where sh rotates the bytes to the left, $\mathbf{S} = S_{RD} \times S_{RD} \times S_{RD} \times S_{RD}$ and RC_i is a round constant.