

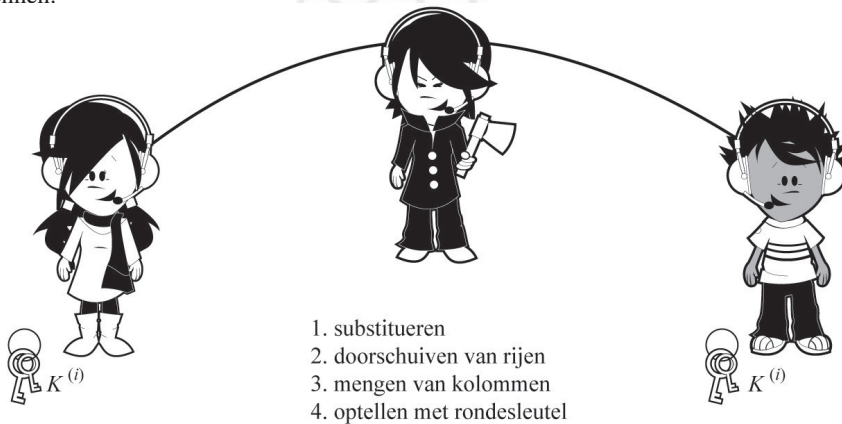
Voorbeeld: Ter illustratie blijkt onze laatste 2^{de} -graadsuitbreiding van het binair priemveld $(\mathbb{Z}_2, +, \cdot)$ bepaald door de irreducibele veelterm $P(x) = x^2 + x + 1 \pmod{2}$ een galoisveld $(\mathbb{F}_{2^2}, +, \cdot)$ te zijn. De vier elementen van dit galoisveld sommen we op als $\mathbb{F}_{2^2} = \{0, 1, x, x + 1\}$.

13.2 Advanced Encryption Standard

Wat Vincent Rijmen en Joan Daemen gemeenzaam ‘Rijndael’ noemen, overkoepelt op zich een ruim gamma varianten van hun symmetrisch versleutelingsalgoritme. Zoals reeds vermeld is ‘Rijndael’ ontworpen als een blokversleuteling die zijn gegevens afhandelt in n -bitblokken. De wereldstandaard ‘Advanced Encryption Standard’ of AES is een algoritme uit dit ‘Rijndael’-gamma met een populaire blok grootte van 128 bits. In dit boek kiezen we de sleutelruimte van onze AES eveneens 128 bits groot, daar waar in realiteit 192-bit- en 256-bitsleutels twee overige alternatieven bieden.

DE PUBLIEKE REKENOMGEVING

AES-cryptografie is zoals vermeld een symmetrisch schema waarin Alice en Bob over eenzelfde veilig uitgewisselde sleutel K beschikken, zoals we verderop stapsgewijze verkennen.



Figuur 13.1: Het symmetrisch schema van AES

Het AES-algoritme vindt plaats in het galoisveld $(\mathbb{F}_{2^8}, +, \cdot)$ bepaald door de irreducibele Rijndael-veelterm $P(x) = x^8 + x^4 + x^3 + x + 1 \pmod{2}$.

Hiertoe steunt de AES-versleuteling op een allocatie (zie paragraaf 12.4) van de veldelementen als dragers van de bytes, bytes die in dit boek worden in- en uitgevoerd volgens de (Windows)ANSI ASCII-tabel (zie bijlage B). Volledigheidshalve merken we op dat in realiteit dit laatste nog volgens allerlei andere tabellen kan (zoals die van Unicode bijvoorbeeld).

Qua interne allocatie stemmen alle 256 bytes als bitrijen overeen met de coëfficiënten van alle *aflopend gerangschikte* veldelementen.

$$a(x) = \begin{matrix} \alpha_7 x^7 + & \alpha_6 x^6 + & \alpha_5 x^5 + & \alpha_4 x^4 + & \alpha_3 x^3 + & \alpha_2 x^2 + & \alpha_1 x + & \alpha_0 \\ (\alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0)_b \end{matrix}$$

Op plaatsen waar het niet nuttig blijkt in veeltermen te noteren, geven we de aflopend gerangschikte coëfficiënten als bitrijen weer in zestiendelige cijfers (zie tabel 4.1 op pagina 79). Dergelijke bitrijen dienen *alle* voorkomende nulcoëfficiënten van de 7^{de}-graadsveeltermen te bevatten. We onderscheiden voor wat volgt algemene bitrijen in zestiendelige weergave via beneden-index ‘h’ expliciet van hexadecimale getallen (die beneden-index ‘hex’ of ‘16’ dragen), daar we de bitrijen interpreteren als veldelementen $a(x)$ en niet als getallen.

Voorbeelden: Ter illustratie tonen we de interne allocatie voor drie binaire galoisvelden. We letten erop de veldelementen als aflopend gerangschikte veeltermen te zetten en te **vervolledigen** met alle nulcoëfficiënten.

- ▷ Het galoisveld $(\mathbb{F}_{2^2}, +, \cdot)$ telt vier veldelementen:

$$\begin{aligned} \{0, 1, x, x+1\} &= \{0x+0, 0x+1, 1x+0, 1x+1\} \\ &= \{(00)_b, (01)_b, (10)_b, (11)_b\} \\ &= \{0_h, 1_h, 2_h, 3_h\}. \end{aligned}$$

- ▷ Een galoisveld $(\mathbb{F}_{2^4}, +, \cdot)$ telt zestien veldelementen.

$$\begin{aligned} &\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, \\ &x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\} \\ &= \{0x^3+0x^2+0x+0, 0x^3+0x^2+0x+1, 0x^3+0x^2+1x+0, 0x^3+0x^2+1x+1, \\ &0x^3+1x^2+0x+0, 0x^3+1x^2+0x+1, 0x^3+1x^2+1x+0, 0x^3+1x^2+1x+1, \\ &1x^3+0+0+0, 1x^3+0+0+1, 1x^3+0+1x+0, 1x^3+0+1x+1, \\ &1x^3+1x^2+0x+0, 1x^3+1x^2+0x+1, 1x^3+1x^2+1x+0, 1x^3+1x^2+1x+1\} \end{aligned}$$

$$\begin{aligned}
&= \{(0000)_b, (0001)_b, (0010)_b, (0011)_b, (0100)_b, (0101)_b, (0110)_b, (0111)_b, \\
&\quad (1000)_b, (1001)_b, (1010)_b, (1011)_b, (1100)_b, (1101)_b, (1110)_b, (1111)_b\} \\
&= \{0_h, 1_h, 2_h, 3_h, 4_h, 5_h, 6_h, 7_h, 8_h, 9_h, A_h, B_h, C_h, D_h, E_h, F_h\} \\
&\triangleright \text{Een galoisveld } (\mathbb{F}_{2^8}, +, \cdot) \text{ telt 256 veldelementen.} \\
&\quad \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, \dots, x^7+x^6+x^5+x^4+x^3+x^2+x+1\} \\
&= \{0x^7+0x^6+0x^5+0x^4+0x^3+0x^2+0x+0, \dots, 1x^7+1x^6+1x^5+1x^4+1x^3+1x^2+1x+1\} \\
&= \{(0000\ 0000)_b, (0000\ 0001)_b, (0000\ 0010)_b, (0000\ 0011)_b, (0000\ 0100)_b, \dots, (1111\ 1111)_b\} \\
&= \{(00)_h, (01)_h, (02)_h, (03)_h, (04)_h, (05)_h, (06)_h, (07)_h, (08)_h, (09)_h, (0A)_h, (0B)_h, \dots, (FF)_h\}
\end{aligned}$$

HET AES-VERSLEUTELINGSALGORITME

De interne rekenomgeving van AES is de vierkante matrixruimte $\mathbb{F}_{2^8}^{4 \times 4}$, met het galoisveld \mathbb{F}_{2^8} steunend op de Rijndael-veelterm $P(x) = x^8 + x^4 + x^3 + x + 1$ (die we hierna stilzwijgend veronderstellen voor de duur van dit hoofdstuk). Voor een eventuele introductie of herhaling van matrixrekenen verwijzen we de lezer naar de literatuur (zie *Wiskunde voor multimedia* [12]). Daar de rekenkundige (matrix)bewerkingen in het eindig galoisveld \mathbb{F}_{2^8} plaatsvinden, blijft de interne rekenomgeving hieronder gesloten.

Elke ingevoerde klare 128-bitblok

$$M = (m_0 m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8 m_9 m_{10} m_{11} m_{12} m_{13} m_{14} m_{15})_h$$

wordt van begin tot eind en byte na byte in de vier kolommen van een $\mathbb{F}_{2^8}^{4 \times 4}$ -matrix geplaatst:

$$\begin{pmatrix} m_0 & m_4 & m_8 & m_{12} \\ m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \end{pmatrix} = \begin{pmatrix} a(x)_{11} & a(x)_{12} & a(x)_{13} & a(x)_{14} \\ a(x)_{21} & a(x)_{22} & a(x)_{23} & a(x)_{24} \\ a(x)_{31} & a(x)_{32} & a(x)_{33} & a(x)_{34} \\ a(x)_{41} & a(x)_{42} & a(x)_{43} & a(x)_{44} \end{pmatrix} = A.$$

Alle matricelementen $a(x)_{ik}$ van de **klare matrix** A zijn (via de interne allocatie) aflopend gerangschikte veldelementen $a(x)_{ik} \in \mathbb{F}_{2^8}$.

We definiëren een **AES-toestand** als elke tussentijdse $\mathbb{F}_{2^8}^{4 \times 4}$ -matrix (verschillend van de sleutel), die we in het AES of AES⁻¹-algoritme ontmoeten. De initiële 4×4 matrix A die de klare 128-bitboodschap in zijn kolommen bevat, is hiervan een voorbeeld.

Ook de symmetrische 128bit-sleutel

$$K = (k_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10} k_{11} k_{12} k_{13} k_{14} k_{15})_h$$