This page deals only with Rijndael with block length 128 and key length 128.

Bytes. A *bit* is an element of $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. Eight bits form one *byte*. The space $\mathbf{F}_2^8$ of all bytes is identified with $\{f \in \mathbf{F}_2[X] : \deg f < 8\}$ by $(b_7b_6b_5b_4b_3b_2b_1b_0) = \sum_{h=0}^{7} b_h X^h$. Define the affine map $\lambda: \mathbf{F}_2^8 \to \mathbf{F}_2^8$ by $\lambda(f) \equiv (X^4+X^3+X^2+X+1)\cdot f + X^6+X^5+X+1 \bmod (X^8+1)$. The inverse $\lambda^{-1} = \lambda^3$ is given by $\lambda^{-1}(f) \equiv (X^6+X^3+X)\cdot f + X^2+1 \bmod (X^8+1)$. All other operations on $\{f \in \mathbf{F}_2[X] : \deg f < 8\}$ will be done not mod X^8+1 but mod $m = X^8+X^4+X^3+X+1$, so that $\mathbf{F}_2^8$ becomes identified with the field $\mathbf{F}_{256} = \mathbf{F}_2[X]/(m)$. Define the map $\sigma: \mathbf{F}_{256} \to \mathbf{F}_{256}$ by $\sigma(a) = \lambda(a^{254})$; here $a^{254} = a^{-1}$ for $a \neq 0$. The cycle lengths of σ are 2, 27, 59, 81, and 87, and $\sigma^{-1} = \sigma^{277181}$ is given by $\sigma^{-1}(a) = (\lambda^{-1}(a))^{254}$.

Words. Four bytes form one *word*. The map from the space $\mathbf{F}_{256}^4$ $(= \mathbf{F}_2^{32})$ of all words to itself sending $(a_i)_{i=0}^3$ to $(\sigma(a_i))_{i=0}^3$ is again denoted by σ. The map $\xi: \mathbf{F}_{256}^4 \to \mathbf{F}_{256}^4$ is defined by $\xi((a_i)_{i=0}^3) = (\sigma(a_{i+1}))_{i=0}^3$ (indices mod 4). Write $c = (X, 1, 1, X+1)$ and $d = (X^3+X^2+X, X^3+1, X^3+X^2+1, X^3+X+1)$, and identify $\mathbf{F}_{256}^4$ with $\{g \in \mathbf{F}_{256}[Y] : \deg g < 4\}$ by $(a_0, a_1, a_2, a_3) = \sum_{i=0}^{3} a_i Y^i$. Define μ, $\nu: \mathbf{F}_{256}^4 \to \mathbf{F}_{256}^4$ by $\mu(g) \equiv c \cdot g \bmod (Y^4+1)$ and $\nu(g) \equiv d\cdot g \bmod (Y^4+1)$. One has $\nu = \mu^{-1} = \mu^3$.

States. Four words form one *state*. The maps from the space $\mathcal{S} = (\mathbf{F}_{256}^4)^4$ $(= \mathbf{F}_2^{128})$ of all states to itself sending $(w_j)_{j=0}^3$ to $(\mu(w_j))_{j=0}^3$, to $(\nu(w_j))_{j=0}^3$, and to $(\sigma(w_j))_{j=0}^3$ are again denoted by μ, ν, and σ, respectively. Define $\rho: \mathcal{S} \to \mathcal{S}$ by $\rho(((a_{i,j})_{i=0}^3)_{j=0}^3) = ((a_{i,i+j})_{i=0}^3)_{j=0}^3$ (indices mod 4). If a state is written as a 4×4-matrix, each column being a word, then ρ shifts the entries in row i cyclically i places to the left $(0 \le i \le 3)$; similarly, $\rho^{-1} = \rho^3$ shifts row i cyclically i places to the right. One has $\rho\sigma = \sigma\rho$. For $s \in \mathcal{S}$, the map $\tau_s: \mathcal{S} \to \mathcal{S}$ is defined by $\tau_s(x) = x + s$; one has $\tau_s^{-1} = \tau_s$ and $\mu\tau_s = \tau_{\mu(s)}\mu$.

Key expansion. The *key* space $\mathcal{K}$ equals $\mathcal{S}$. For fixed $k = (w_j)_{j=0}^3 \in \mathcal{K}$, define inductively $w_4, w_5, \ldots, w_{43} \in \mathbf{F}_{256}^4$ by $w_j = w_{j-1} + w_{j-4}$ if $j \not\equiv 0 \bmod 4$ and $w_j = \xi(w_{j-1}) + w_{j-4} + (X^{(j-4)/4}, 0, 0, 0)$ if $j \equiv 0 \bmod 4$, and put $k_l = (w_{4l}, w_{4l+1}, w_{4l+2}, w_{4l+3}) \in \mathcal{S}$ for $0 \le l \le 10$.

Encryption and decryption. Messages are divided in blocks of 128 bits each. Each block belongs to $\mathcal{S}$. Given a key $k \in \mathcal{K}$, a block is encrypted by means of the encryption function $\varepsilon_k: \mathcal{S} \to \mathcal{S}$ defined by

$$\varepsilon_k = \tau_{k_{10}}\rho\sigma\tau_{k_9}\mu\rho\sigma\tau_{k_8}\mu\rho\sigma\tau_{k_7}\mu\rho\sigma\tau_{k_6}\mu\rho\sigma\tau_{k_5}\mu\rho\sigma\tau_{k_4}\mu\rho\sigma\tau_{k_3}\mu\rho\sigma\tau_{k_2}\mu\rho\sigma\tau_{k_1}\mu\rho\sigma\tau_{k_0}$$

(nine μ's, ten ρ's, ten σ's, and eleven τ's; composition is from right to left). The corresponding decryption function $\delta_k = \varepsilon_k^{-1}$ is given by

$$\delta_k = \tau_{k_0}\rho^{-1}\sigma^{-1}\tau_{\nu(k_1)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_2)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_3)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_4)}\nu\rho^{-1}\sigma^{-1} \circ$$
$$\circ\, \tau_{\nu(k_5)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_6)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_7)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_8)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_9)}\nu\rho^{-1}\sigma^{-1}\tau_{k_{10}}.$$

Twenty-five Rijndaels. Let $\mathbf{b}$, $\mathbf{k} \in \{4,5,6,7,8\}$. This page describes Rijndael with block length $32\mathbf{b}$ and key length $32\mathbf{k}$. Bits, bytes, and words are as before, and so are the function σ defined on bytes and the functions μ, ν, ξ, and σ defined on words.

States. One *state* is formed by $\mathbf{b}$ words. The space $\mathcal{S}$ of all states equals $(\mathbf{F}_{256}^4)^{\mathbf{b}}$ $(= \mathbf{F}_2^{32\mathbf{b}})$. The maps μ, ν, $\sigma: \mathcal{S} \to \mathcal{S}$ send $(w_j)_{j=0}^{\mathbf{b}-1}$ to $(\mu(w_j))_{j=0}^{\mathbf{b}-1}$, to $(\nu(w_j))_{j=0}^{\mathbf{b}-1}$, and to $(\sigma(w_j))_{j=0}^{\mathbf{b}-1}$, respectively. Define $\rho: \mathcal{S} \to \mathcal{S}$ by $\rho(((a_{i,j})_{i=0}^{3})_{j=0}^{\mathbf{b}-1}) = ((a_{i,e(i)+j})_{i=0}^{3})_{j=0}^{\mathbf{b}-1}$ (addition of indices mod $\mathbf{b}$); here $e(i) = i$ if $\mathbf{b} + i \le 9$, and $e(i) = i + 1$ if $\mathbf{b} + i > 9$. If a state is written as a $4 \times \mathbf{b}$-matrix with entries from $\mathbf{F}_{256}$, then ρ and ρ^{-1} shift the entries in row i cyclically $e(i)$ places to the left and right, respectively $(0 \le i \le 3)$. One has $\rho\sigma = \sigma\rho$. For $s \in \mathcal{S}$, the map $\tau_s: \mathcal{S} \to \mathcal{S}$ is defined by $\tau_s(x) = x + s$; one has $\tau_s^{-1} = \tau_s$ and $\mu\tau_s = \tau_{\mu(s)}\mu$.

Key expansion. One *key* is formed by $\mathbf{k}$ words. The key space $\mathcal{K}$ equals $(\mathbf{F}_{256}^4)^{\mathbf{k}}$ $(= \mathbf{F}_2^{32\mathbf{k}})$. Write $\mathbf{r} = 6 + \max\{\mathbf{b}, \mathbf{k}\}$. For fixed $k = (w_j)_{j=0}^{\mathbf{k}-1} \in \mathcal{K}$, define inductively $w_{\mathbf{k}}$, $w_{\mathbf{k}+1}$, $\ldots$, $w_{\mathbf{br}+\mathbf{b}-1} \in \mathbf{F}_{256}^4$ as follows. If $\mathbf{k} \le 6$, then put $w_j = w_{j-1} + w_{j-\mathbf{k}}$ if $j \not\equiv 0 \bmod \mathbf{k}$ and $w_j = \xi(w_{j-1}) + w_{j-\mathbf{k}} + (X^{(j-\mathbf{k})/\mathbf{k}}, 0, 0, 0)$ if $j \equiv 0 \bmod \mathbf{k}$. If $\mathbf{k} > 6$, then the same formulas are used, except if $j \equiv 4 \bmod \mathbf{k}$, in which case one takes $w_j = \sigma(w_{j-1}) + w_{j-\mathbf{k}}$. In all cases, put $k_l = (w_{\mathbf{b}l+j})_{j=0}^{\mathbf{b}-1} \in \mathcal{S}$ for $0 \le l \le \mathbf{r}$.

Encryption and decryption. Messages are divided in blocks of $32\mathbf{b}$ bits each. Each block belongs to $\mathcal{S}$. Given a key $k \in \mathcal{K}$, a block is encrypted by means of the encryption function $\varepsilon_k: \mathcal{S} \to \mathcal{S}$ defined by

$$\varepsilon_k = \tau_{k_{\mathbf{r}}}\rho\sigma\tau_{k_{\mathbf{r}-1}}\mu\rho\sigma\tau_{k_{\mathbf{r}-2}}\mu\rho\sigma\tau_{k_{\mathbf{r}-3}}\mu\cdots\rho\sigma\tau_{k_2}\mu\rho\sigma\tau_{k_1}\mu\rho\sigma\tau_{k_0}$$

($\mathbf{r} - 1$ μ's, $\mathbf{r}$ ρ's, $\mathbf{r}$ σ's, and $\mathbf{r} + 1$ τ's). The corresponding decryption function $\delta_k = \varepsilon_k^{-1}$ is given by

$$\delta_k = \tau_{k_0}\rho^{-1}\sigma^{-1}\tau_{\nu(k_1)}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_2)}\nu\rho^{-1}\sigma^{-1}\cdots\tau_{\nu(k_{\mathbf{r}-2})}\nu\rho^{-1}\sigma^{-1}\tau_{\nu(k_{\mathbf{r}-1})}\nu\rho^{-1}\sigma^{-1}\tau_{k_{\mathbf{r}}}.$$

Dictionary. Here are the names used for some of Rijndael's ingredients.
AddRoundKey: one of the maps τ_{k_l}.
MixColumns: the map μ defined on $\mathcal{S}$.
Round constant: one of the elements $X^{(j-\mathbf{k})/\mathbf{k}}$ of $\mathbf{F}_{256}$ used in the key expansion.
Round key: one of the elements k_l of $\mathcal{S}$.
Round transformation: one of the maps $\tau_{k_l}\mu\rho\sigma$, with μ left out if $l = \mathbf{r}$.
S-box: the map σ defined on $\mathbf{F}_{256}$.
Shift offset: one of the numbers $e(i)$.
ShiftRows: the map ρ.
SubBytes: the map σ defined on $\mathcal{S}$.

Reference. Joan Daemen, Vincent Rijmen, *The design of Rijndael*, Springer, Berlin, 2002.
The present document can be found on ⟨http://www.math.berkeley.edu/∼hwl/⟩.