AES variation (AES-V)

Parameters of the cipher:
prime number p, fixed numbers a, b, 2×2 matrix $T = [t_{11}, t_{12}, t_{21}, t_{22}]$.
The message block $M = [m_{11}, m_{12}, m_{21}, m_{22}]$,
and the key $K = [k_{11}, k_{12}, k_{21}, k_{22}]$.

Three iterations are used with the subkeys $K_1 = K, K_2, K_3$. The subkeys K_2 and K_3 are derived from K according to the key schedule.

The structure of an iteration:

Step 1. Substitution of bytes

$$M = \begin{vmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{vmatrix} \to \begin{vmatrix} m^1_{11} & m^1_{12} \\ m^1_{21} & m^1_{22} \end{vmatrix}, \quad m^1_{ij} = (am^{-1}_{ij}+b) \pmod p \text{ if } m_{ij} \neq 0.$$

If $m_{ij} = 0$, then $m^1_{ij} = b$.

Step 2. Shift of rows

$$\begin{vmatrix} m^1_{11} & m^1_{12} \\ m^1_{21} & m^1_{22} \end{vmatrix} \to \begin{vmatrix} m^2_{11} & m^2_{12} \\ m^2_{21} & m^2_{22} \end{vmatrix} = \begin{vmatrix} m^1_{11} & m^1_{12} \\ m^1_{22} & m^1_{21} \end{vmatrix}.$$

Step 3. Mix of columns

$$\begin{vmatrix} m^2_{11} & m^2_{12} \\ m^2_{21} & m^2_{22} \end{vmatrix} \to \begin{vmatrix} m^3_{11} & m^3_{12} \\ m^3_{21} & m^3_{22} \end{vmatrix}, \quad \begin{pmatrix} m^3_{1i} \\ m^3_{2i} \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} m^2_{1i} \\ m^2_{2i} \end{pmatrix}, \quad i = 1, 2.$$

Step 4. Addition with the round key

$$\begin{vmatrix} m^4_{11} & m^4_{12} \\ m^4_{21} & m^4_{22} \end{vmatrix} = \begin{vmatrix} m^3_{11} & m^3_{12} \\ m^3_{21} & m^3_{22} \end{vmatrix} + \begin{vmatrix} k^i_{11} & k^i_{12} \\ k^i_{21} & k^i_{22} \end{vmatrix} \pmod p,$$

here

$$K_i = \begin{vmatrix} k^i_{11} & k^i_{12} \\ k^i_{21} & k^i_{22} \end{vmatrix}$$

is the subkey of the i-th iteration.

For decryption, all transformations should be inverted and keys used in reverse order.

The inverse of a matrix:

$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}, \quad T^{-1} = (\det T)^{-1} \begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix} \pmod{p}.$$

Generation of the subkeys:

If $K_i = [k_{11}^i, k_{12}^i, k_{21}^i, k_{22}^i]$ is the subkey of the i-th iteration, then the subkey of the $(i+1)$-th iteration $K_{i+1} = [k_{11}^{i+1}, k_{12}^{i+1}, k_{21}^{i+1}, k_{22}^{i+1}]$ can be obtained this way:

$$k_{11}^{i+1} = \begin{cases} k_{11}^i + (a/k_{22}^i + b) \pmod{p}, & \text{if } k_{22}^i \neq 0, \\ k_{11}^i + b \pmod{p}, & \text{otherwise.} \end{cases}$$

$$k_{12}^{i+1} = k_{12}^i + k_{11}^{i+1} \pmod{p},$$

$$k_{21}^{i+1} = k_{21}^i + k_{12}^{i+1} \pmod{p},$$

$$k_{22}^{i+1} = k_{22}^i + k_{21}^{i+1} \pmod{p}.$$