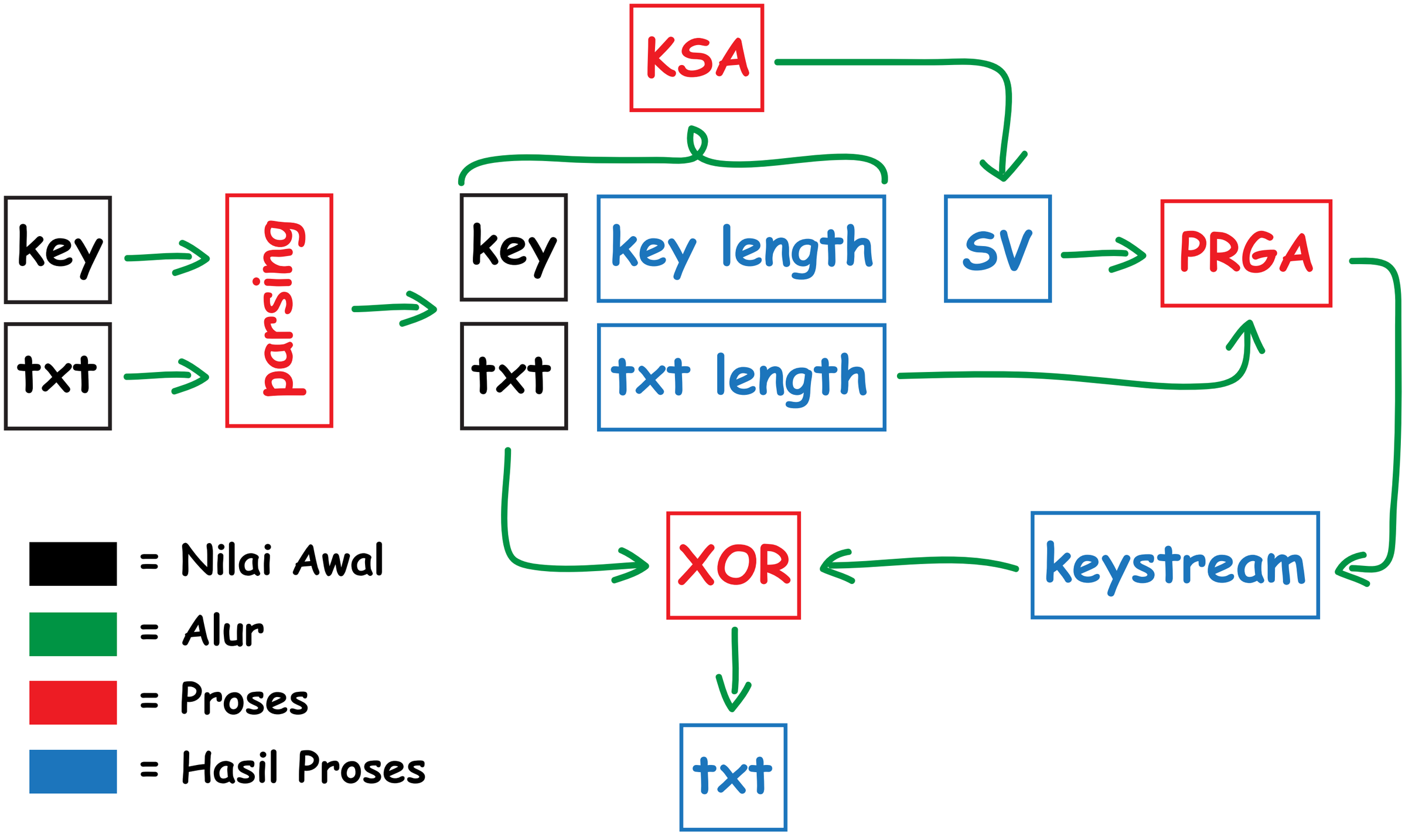
RC4 Algorithm (Stream Cipher)



Key Scheduling Algorithm (KSA)

karakter di ubah
ke ASCII Code
(misal: A=65, Z=90)

J = 0

SV = {SV[I]=I | I=0,1,...256-1}

$$SV = \sum_{I=0}^{256-1} \{$$

J=(J+SV[I]+key[I % key_length]) % 256

SV[I],SV[J] = SV[J],SV[I]

SV adalah State Vector

---

kenapa 256 ?.

1 byte = 8 bits ⟶ 2^8 = 256

range dari
00000000(2) = 0(10)
sampai
11111111(2) = 255(10)

Pseudo-random Generation Algorithm (PRGA)

J = 0; X = 0;

K adalah Keystream

$$K = \sum_{I=0}^{txt\_length-1} \begin{cases} X=(X + 1) \% 256 \\ J=(J + SV[X]) \% 256 \\ SV[X],SV[J] = SV[J],SV[X] \\ K[I] = SV[SV[X] + SV[J] \% 256] \end{cases}$$

langkah terakhir -nya

$$result = \sum_{I=0}^{txt\_length-1} \{ result[I] = (txt[I] \text{ xor } K[I])$$

karakter di ubah
ke ASCII Code
(misal: A=65, Z=90)