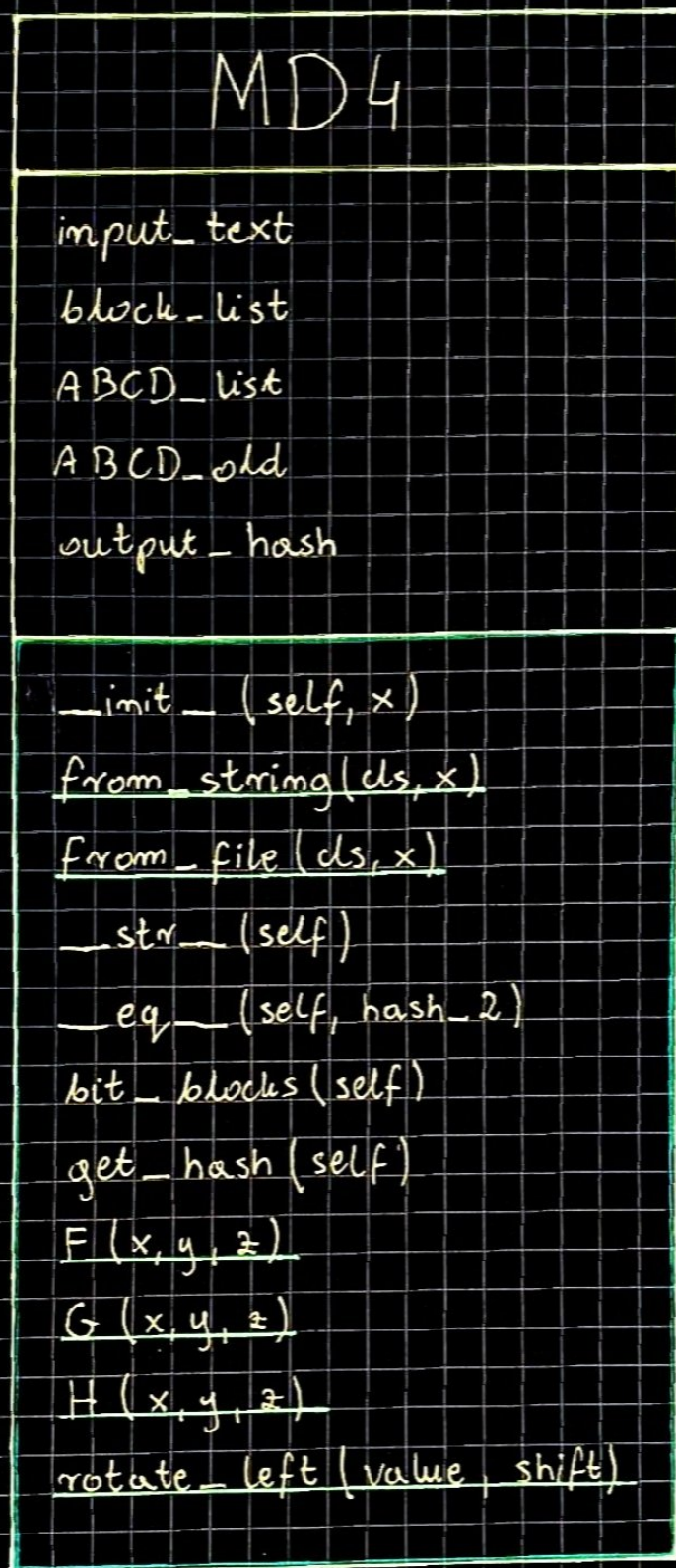


# DIAGRAM UML



## Legenda atrybutów i metod:

- podkreślenie - metody klasy lub statyczne
- `input_text` - przechowuje podany przez użytkownika tekst dziedziczący z klasy bytes do zakodowania (w konstruktorze jego oznaczenie to `x`)
- `block_list` - lista dzieląca wiadomości na bloki po 512 bitów



- `ABCD_list` - lista czterech stałych wartości dla algorytmu MD4.
  - `ABCD_old` - kopia listy `ABCD_list`
  - `output_hash` - kod końcowy przechowywany jako liczba całkowita
  - `__init__(self, x)` - konstruktor zawierający atrybuty i sprawdzający czy podane przez użytkownika wartości jest klasy bytes
  - `from_string(cls, x)` - metoda konwertująca podany przez użytkownika tekst z str do bytes
  - `from_file(cls, x)` - tworzy instancję klasy MD4 z pliku, odczytując jego zawartość jako bajty
  - `__str__(self)` - zwraca kod końcowy jako liczbę w systemie szesnastkowym
  - `__eq__(self)` - zwraca wartość logiczną wynikającą z porównania szesnastkowej wartości końcowego kodu z kodem oznaczonym jako `hash-2`
  - `bit_blocks(self)` - zwraca listę bloków bitów pochodzących z `block_list`
  - `get_hash(self)` - zwraca kod końcowy jako liczbę całkowitą po trzech rundach zapisywania stałych
  - $F(x, y, z)$
  - $G(x, y, z)$
  - $H(x, y, z)$
- Funkcje pomocnicze wykorzystywane do stworzenia trzech rund w MD4. Każda z nich przyjmuje trzy 32-bitowe liczby całkowite jako argumenty i zwraca jedną 32-bitową liczbę całkowitą.
- `rotate_left(value, shift)` - funkcja definiująca obrót ( $a \ll b$  to przesunięcie liczby  $a$  w zapisie binarnym o  $b$  miejsc w lewo z obrotem)