```
MODULE pbkdf2
EXTENDS Integers, Sequences, TLC, Bitwise

Password ≜ ⟨32, 12, 45, 67, 78, 43, 21, 19⟩
Salt ≜ ⟨16, 12, 34, 45⟩
Iterations ≜ 5
OutputLength ≜ 16
BlockIndex ≜ ⟨4, 2, 1, 0⟩

VARIABLES U, F, DerivedKey

HMAC(password, data) ≜ data ∘ Password

U1 ≜ HMAC(Password, Append(Salt, BlockIndex))

ModAdd(x, y) ≜ ((x + y)%(2^8))
ModSub(x, y) ≜ ((x − y)%(2^8))
ModMul(x, y) ≜ ((x ∗ y)%(2 ^8))

Init ≜
    ∧ U = [i ∈ 1 . . Iterations ↦ IF i = 1 THEN U1 ELSE ⟨⟩]
    ∧ F = U1
    ∧ DerivedKey = ⟨⟩

GenNextU(i) ≜ U[i] = HMAC(Password, U[i − 1])

UpdateF(i) ≜ F′ = F^^U[i]

FinalizeDerivedKey ≜
    ∧ DerivedKey′ = Append(DerivedKey, F)
    ∧ UNCHANGED ⟨U, F⟩

Next ≜
    ∨ ∃ i ∈ 2 . . Iterations :
        ∧ GenNextU(i)
        ∧ UpdateF(i)
        ∧ UNCHANGED ⟨DerivedKey⟩
    ∨ FinalizeDerivedKey

Spec ≜
    ∧ Init
    ∧ □[Next]_⟨U, F, DerivedKey⟩
```