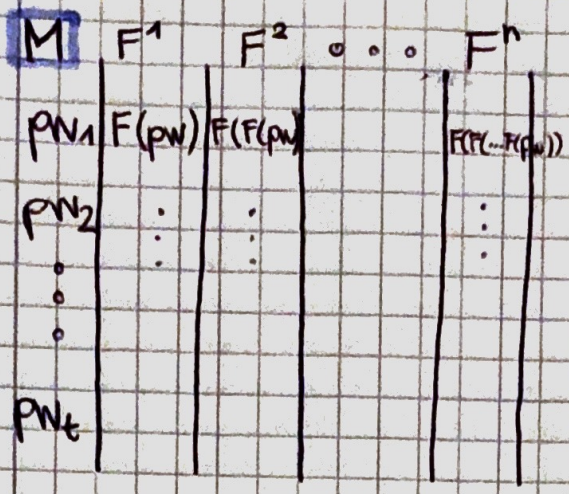
Exercise 10.3 (Rainbow Tables)



T $(pw_i, y_i) = (pw_i, F^n(pw_i))$

(1.)

Initialization:

1. $y_1 = g(\underbrace{f(pw)}_{\text{input}})$
2. if y_1 is in T in row r
   → output is pw_r

Algorithm:

1. Compute $y_{i+1} = F(y_i)$
2. Search in T for y_{i+1}
   - 2.1 if found on row r
     → output $F^{n-i-1}(pw_r)$
   - 2.2 if not found, go to 1.

→ terminate after n iterations with no output

(2.) $n + (n-1)$ times while computing the result
→ from n outer iterations of the given hash

(3.) If not all y_i's are distinct, then you might end up with several passwords ((pw)'s), so the result is also not distinct.