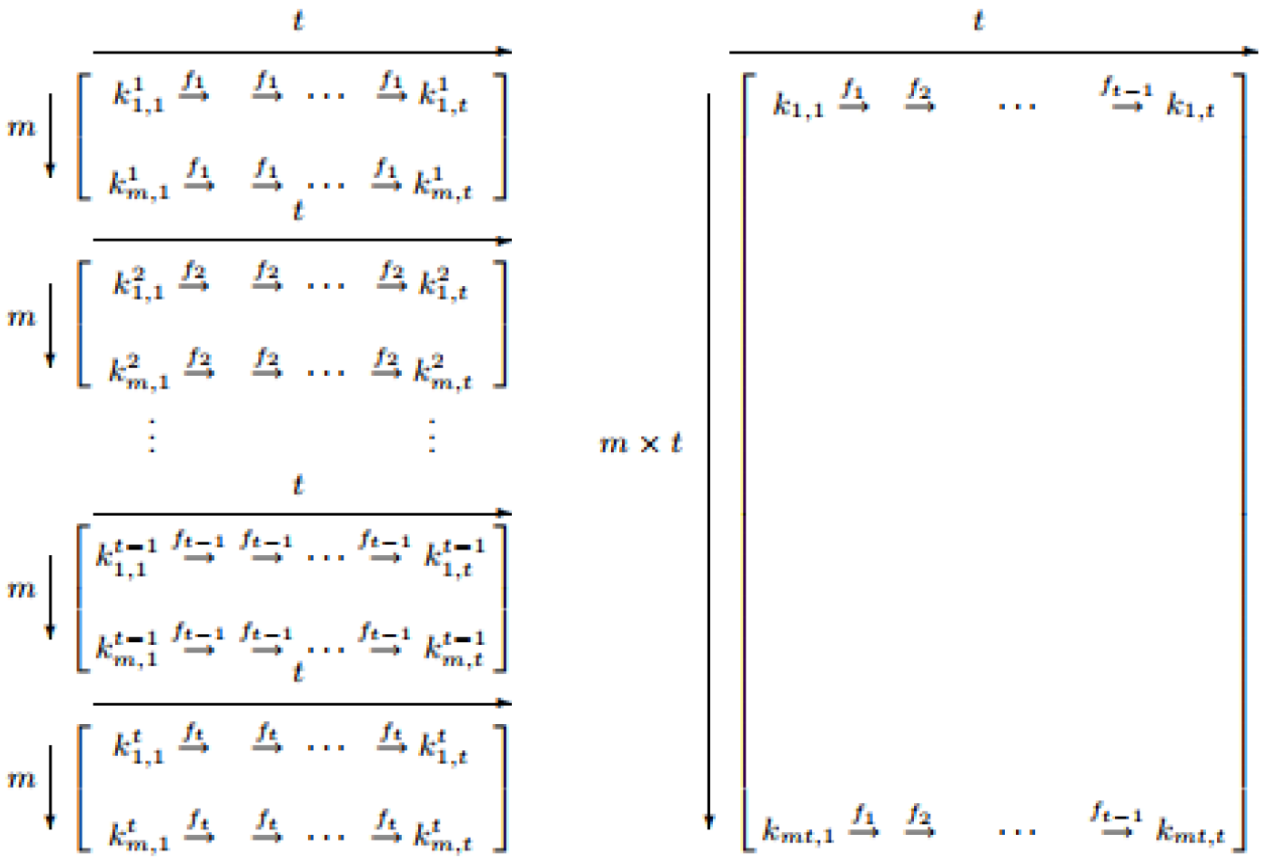
Solutions

ENEE 457
Hellman/Rainbow Table Class Exercise



1. Given a hash value $\mathrm{H}(pass)$, explain how to do a table look-up to determine $pass$ in Hellman's table on the left.

   For the i-th table do the following: Compute k_1 = R_i(H(pass)) and check if the value matches any of the EP by doing a table lookup. Assume it matches EP^i_j, then start from SP^i_j and compute forward to find pass. Otherwise, compute k_2 = f_i(k_1) and check again. Repeat until pass is found.
   Total number of hash evaluations t^2
   Total number of table lookups t^2

1. Given a hash value $\mathrm{H}(pass)$, explain how to do a table look-up to determine $pass$ in the Rainbow table on the right.

   Compute k_1 = R_{t-1}(H(pass)) and check if the value matches any of the EP by doing a table lookup. Assume it matches EP_{i,j}, then start from SP_{i,j} and compute forward to find pass. Otherwise, compute k_2 = f_{t-1}(R_{t-2}(H(pass))) and check again. Repeat until pass is found.
   Total number of hash evaluations: 1 + 2 +... + t ~ t^2/2
   Total number of table lookups: t