ENEE 457
Hellman/Rainbow Table Class Exercise

$$\begin{array}{c} m \downarrow \end{array} \begin{bmatrix} k_{1,1}^1 \xrightarrow{f_1} \xrightarrow{f_1} \cdots \xrightarrow{f_1} k_{1,t}^1 \\ \\ k_{m,1}^1 \xrightarrow{f_1} \xrightarrow{f_1} \cdots \xrightarrow{f_1} k_{m,t}^1 \end{bmatrix}$$

$$\begin{array}{c} m \downarrow \end{array} \begin{bmatrix} k_{1,1}^2 \xrightarrow{f_2} \xrightarrow{f_2} \cdots \xrightarrow{f_2} k_{1,t}^2 \\ \\ k_{m,1}^2 \xrightarrow{f_2} \xrightarrow{f_2} \cdots \xrightarrow{f_2} k_{m,t}^2 \end{bmatrix}$$

$$\vdots \qquad \qquad \vdots$$

$$\begin{array}{c} m \downarrow \end{array} \begin{bmatrix} k_{1,1}^{t-1} \xrightarrow{f_{t-1}} \xrightarrow{f_{t-1}} \cdots \xrightarrow{f_{t-1}} k_{1,t}^{t-1} \\ \\ k_{m,1}^{t-1} \xrightarrow{f_{t-1}} \xrightarrow{f_{t-1}} \cdots \xrightarrow{f_{t-1}} k_{m,t}^{t-1} \end{bmatrix}$$

$$\begin{array}{c} m \downarrow \end{array} \begin{bmatrix} k_{1,1}^t \xrightarrow{f_t} \xrightarrow{f_t} \cdots \xrightarrow{f_t} k_{1,t}^t \\ \\ k_{m,1}^t \xrightarrow{f_t} \xrightarrow{f_t} \cdots \xrightarrow{f_t} k_{m,t}^t \end{bmatrix}$$

$$m \times t \qquad \begin{bmatrix} k_{1,1} \xrightarrow{f_1} \xrightarrow{f_2} \cdots \xrightarrow{f_{t-1}} k_{1,t} \\ \\ \\ \\ \\ \\ \\ \\ k_{mt,1} \xrightarrow{f_1} \xrightarrow{f_2} \cdots \xrightarrow{f_{t-1}} k_{mt,t} \end{bmatrix}$$
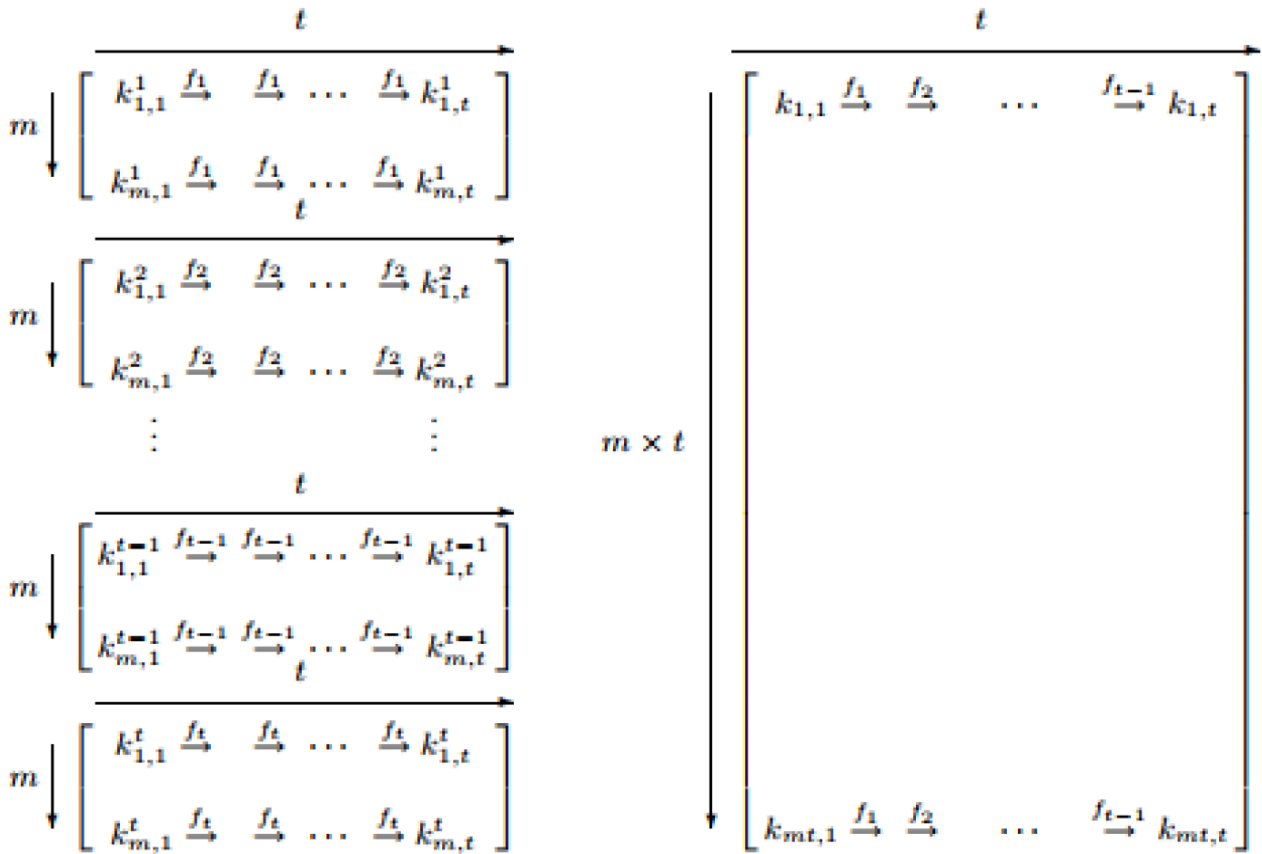
1. Given a hash value $H(pass)$, explain how to do a table look-up to determine $pass$ in Hellman's table on the left.

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