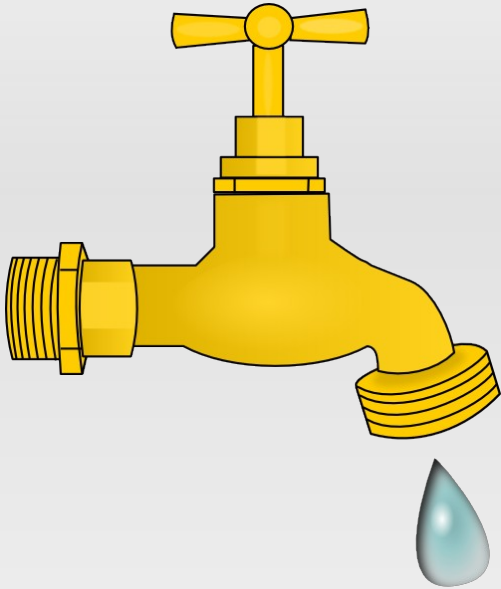


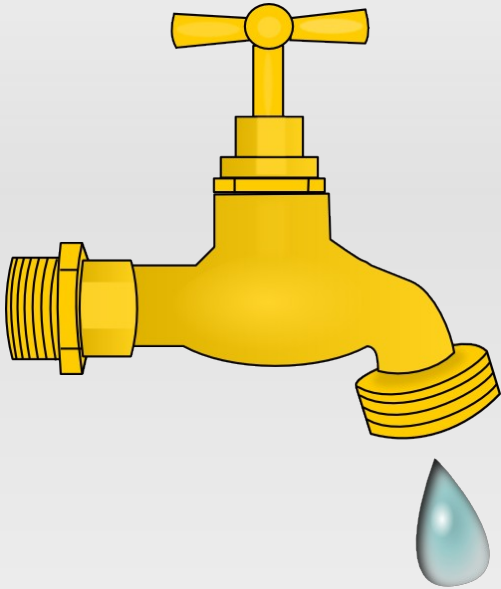
Leakage

Leakage



Leakage

Leakage

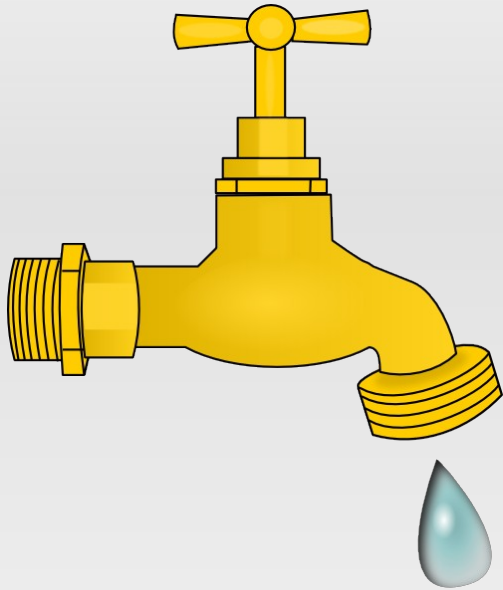


Leakage

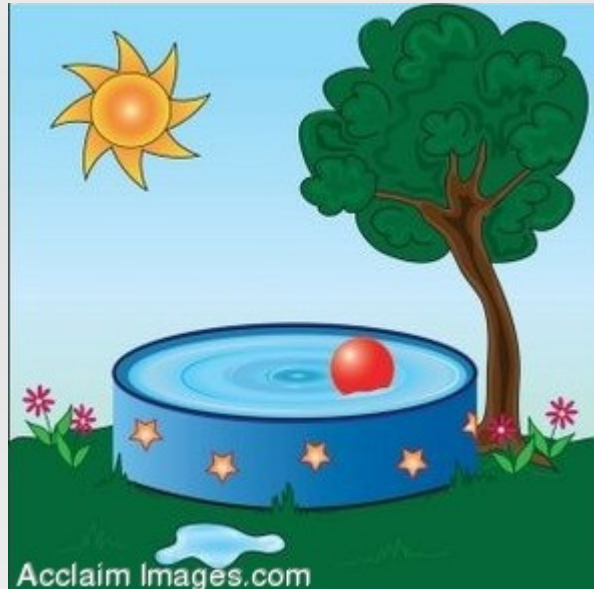


Leakage
Leakage

Leakage



Leakage



Leakage
Leakage



"Leakage"
Leakage

- Leakage leakage leakage [LEAKAGE09]
- Leakage leakage leakage leakage [LeaKage10]

Leakage leakage leakage

$$PK = h = g_1^{x_1} \cdot g_2^{x_2},$$
$$SK = (x_1, x_2)$$



$$a = g_1^{r_1} \cdot g_2^{r_2}$$



$$c$$



$$z_1 = r_1 - c \cdot x_1, z_2 = r_2 - c \cdot x_2$$

PK



- Leakage leakage leakage leakage leakage leakage?
- Leakage leakage leakage "leakage leakage" leakage!

