DZ1

1.a) $k = 77, 69, 39, 70, 6, 8, 40, 89, 49, 15$

$m = 19$

$h(77) = 77 \bmod 19 = 1$
$h(69) = 69 \bmod 19 = 12$
$h(39) = 39 \bmod 19 = 1$
$h(70) = 70 \bmod 19 = 13$
$h(6) = 6 \bmod 19 = 6$
$h(8) = 8 \bmod 19 = 8$
$h(40) = 40 \bmod 19 = 2$
$h(89) = 89 \bmod 19 = 13$
$h(49) = 49 \bmod 19 = 11$
$h(15) = 15 \bmod 19 = 15$

0	/
1	→ 77 → 39 /
2	→ 40 /
3	/
4	/
5	/
6	→ 6 /
7	/
8	→ 8 /
9	/
10	/
11	→ 49 /
12	→ 69 /
13	→ 70 → 89 /
14	/
15	→ 15 /
16	/
17	/
18	/

a

1.b)

$h_1(77) = 1$	$h_2(77) = 6$	$h(77,0) = 1$
$h_1(69) = 12$	$h_2(69) = 16$	$h(69,0) = 12$
$h_1(39) = 1$	$h_2(39) = 4$	$h(39,0) = 5$
$h_1(70) = 13$	$h_2(70) = 17$	$h(70,0) = 13$
$h_1(6) = 6$	$h_2(6) = 7$	$h(6,0) = 6$
$h_1(8) = 8$	$h_2(8) = 9$	$h(8,0) = 8$
$h_1(40) = 2$	$h_2(40) = 5$	$h(40,0) = 2$
$h_1(89) = 13$	$h_2(89) = 18$	$h(89,2) = 1$
$h_1(49) = 11$	$h_2(49) = 14$	$h(49,3) = 15$
$h_1(15) = 15$	$h_2(15) = 16$	$h(15,2) = 9$

0	
1	77
2	40
3	
4	
5	39
6	6
7	
8	8
9	15
10	
11	89
12	69
13	70
14	
15	49
16	
17	
18	

1.2. $f(x)$ je univerzalna ako je definirana za sve moguće ulaze x, vrijednosti joj moraju biti cijeli brojevi i vjerojatnost kolizije mora biti 1/br. mogućih izlaza fje

$$f(x) = \sum_{i=1}^{n} a_i x_i \pmod 8$$

želimo pokazati da je $f(x) = f(y) \leq \frac{1}{8}$

za npr. $x=0,\ y=3$; $a_0 = 1$

$$\Rightarrow f(0) = 0$$
$$f(3) = 0$$

2. Pod pretpostavkom uniformnog raspršenja, vjerojatnost da 2 različita ključa imaju istu vrijednost hash fje je $\frac{1}{m}$, jer postoji ukupno m mogućih vrij. hash fje, a svaki ključ se raspoređuje uniformno na te vrijednosti.

T.d. je očekivani broj kolizija za n ključeva je brojnih mogućih parova ključeva $\frac{n(n-1)}{2}$ pomnožen s vjer. da se ti ključevi sudare t.d.

$$E\{k, l\} = \frac{n(n-1)}{2} \cdot \frac{1}{m}$$

3.2 $Pr\{n_{2\lg n} \geq k\} \leq 2^{-2\lg n} = 2^{\lg n^{-2}} = \frac{1}{n^2}$

$$\Rightarrow O\left(\frac{1}{n^2}\right)$$

3. $Pr\{x_1 \geq 2\lg n\} + Pr\{x_2 \geq 2\lg n\} + \dots + Pr\{x_n \geq 2\lg n\} =$
$= \sum_{i=1}^{n} Pr\{x_i \geq 2\lg n\} \leq \sum_{i=1}^{n} \frac{1}{n^2} = n \cdot \frac{1}{n^2} \Rightarrow O\left(\frac{1}{n}\right)$

4. $E[x] \leq Pr\{x \leq 2\lg n\} \cdot 2\lg n + Pr\{x > \lg n\} \cdot n =$
$= \frac{n-1}{2} \cdot 2\lg(n) + \frac{1}{n} \cdot n = 2\lg n + 1 - 2\frac{\lg(n)}{n}$
$\Rightarrow O(\lg n)$