Question 1

Prove that the family of functions $\mathrm{H} = \mathrm{h_a} : \mathrm{X} \rightarrow \mathrm{Y} : \mathrm{a} \in \mathrm{A}\}$ is 2-universal if and only if it is universal and independent.

As we know that H is k-universal for every fixed sequence of k distinct keys and for any h chosen at random from H, the sequence is likely to be any of the $|\mathrm{Y}|^{\mathrm{k}}$ pairs. We can look at the definitions for universal and 2-universal :

$$\mathrm{Pr_{a \leftarrow A}}[\mathrm{h_a}(\mathrm{x}) = \mathrm{h_a}(\mathrm{x}')] = \frac{1}{|\mathrm{Y}|} \qquad \text{universal}$$

$$\mathrm{Pr_{a \leftarrow A}}[(\mathrm{h_a}(\mathrm{x}) = \mathrm{y}) \wedge \mathrm{h_a}(\mathrm{x}') = \mathrm{y}')] = \frac{1}{|\mathrm{Y}|^2} \qquad \text{2-universal}$$

So, if H is 2-universal then our $\mathrm{k} = 2$, and for every pair of keys x and x', where $x \neq x'$, their fixed sequence is as likely to be any of the $|\mathrm{Y}|^2$ pairs, so for every $\mathrm{i} \in |\mathrm{Y}|$, we get that there $\frac{1}{|\mathrm{Y}|}$ collisions as $\frac{|Y|}{|Y|^2}$ so by definition it is universal:

$$\mathrm{Pr_{a \leftarrow A}}[\mathrm{h_a}(\mathrm{x}) = \mathrm{h_a}(\mathrm{x}')] = \sum_{\mathrm{i}=0}^{|\mathrm{Y}|-1}(\mathrm{Pr_{a \leftarrow A}}[< \mathrm{h_a}(\mathrm{x}), \mathrm{h_a}(\mathrm{x}') >=< \mathrm{i}, \mathrm{i} >]) = \frac{|\mathrm{Y}|}{|\mathrm{Y}|^2} = \frac{1}{|\mathrm{Y}|}$$

Question 2

Suggest a family $\mathrm{H} = \{\mathrm{h_a} : \mathrm{X} \rightarrow \mathrm{Y} : \mathrm{a} \in \mathrm{A}\}$ that is universal but not 2-universal. Justify your answer and try to make $|\mathrm{H}|$, $|\mathrm{X}|$, and $|\mathrm{Y}|$ as small as possible.

A family that is universal but not 2- universal is when $|H| = |X| = |Y| = 2$. For some pair $\{x, x'\}$, in the family if we choose at random a hash function then the probability of a collision is the same as the probability of picking some $h \in |H|$ is the same as picking $\frac{1}{|Y|}$ so $|H|$ is universal. But for a 2- universal family, when you pick at random a hash function, then all the pairs are equally likely but some pairs are not possible so H is not 2-universal.

Question 3

Let $\mathrm{H} = \{\mathrm{h_a} : \mathrm{X} \rightarrow \mathrm{Y} : \mathrm{a} \in \mathrm{A}\}$ be a universal family. A rival learns the value of $\mathrm{h_a}(x)$ for $\mathrm{x} \in \mathrm{X}$ that he chooses and for an $\mathrm{a} \in \mathrm{A}$ that was selected at random but he is not aware of. Can the rival find a collision (that is to say a value $\mathrm{x} \neq \mathrm{x}'$ such that $\mathrm{h_a}(\mathrm{x}) = \mathrm{h_a}(\mathrm{x}')$) with a probability greater than $\frac{1}{|\mathrm{Y}|}$?

We can add an extra key, so our rival can cause a collision. For example, for keys a, b, c we can force a collision with probability of $\frac{1}{2}$ for a and b, as well as for $a$and c, and we can have b and c collide with a probability of less than $\frac{1}{2}$, for example 0. The rival can determine which hash function we have selected by picking for example a, if we return a 0 then he can pick b, if we return 1, then we picked a different hash function and he can select c.

Question 4

As in the question above, but suppose that $\mathrm{H} = \{\mathrm{h_a} : \mathrm{X} \to \mathrm{Y} : \mathrm{a} \in \mathrm{A}\}$ is 2-universal.

With an H that is 2-universal, the rival cannot cause a collision with probability better than $\frac{1}{|\mathrm{Y}|}$. Since knowing $\mathrm{h_a(x)}$ does not give them any information about $\mathrm{h_a(x')}$ for any $\mathrm{x'}$ where $\mathrm{x} \neq \mathrm{x'}$. So if our rival learns that for $\mathrm{h_a(x)}$ we have C, that is to say that for some x, $\mathrm{h_a(x)} = \mathrm{C}$ then by the definition of 2-universality we have:

$$\mathrm{Pr_{a \leftarrow A}[h_a(x) = h_a(x') | h_a(x) = C]} = \frac{\mathrm{Pr_{a \leftarrow A}[h_a(x) = h_a(x') | h_a(x) = C]}}{\mathrm{Pr_{a \leftarrow A}[h_a(x) = C]}} = \frac{\frac{1}{|\mathrm{Y}|^2}}{\frac{1}{|\mathrm{Y}|}} = \frac{1}{|\mathrm{Y}|}$$