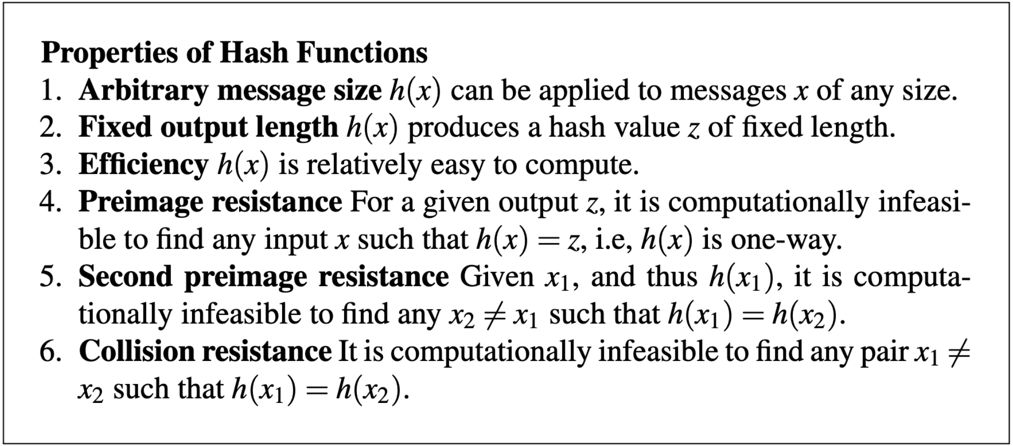
From pg. 345 of the text



Properties of Hash Functions

1. **Arbitrary message size** $h(x)$ can be applied to messages x of any size.
2. **Fixed output length** $h(x)$ produces a hash value z of fixed length.
3. **Efficiency** $h(x)$ is relatively easy to compute.
4. **Preimage resistance** For a given output z, it is computationally infeasible to find any input x such that $h(x) = z$, i.e, $h(x)$ is one-way.
5. **Second preimage resistance** Given x_1, and thus $h(x_1)$, it is computationally infeasible to find any $x_2 \neq x_1$ such that $h(x_1) = h(x_2)$.
6. **Collision resistance** It is computationally infeasible to find any pair $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$.