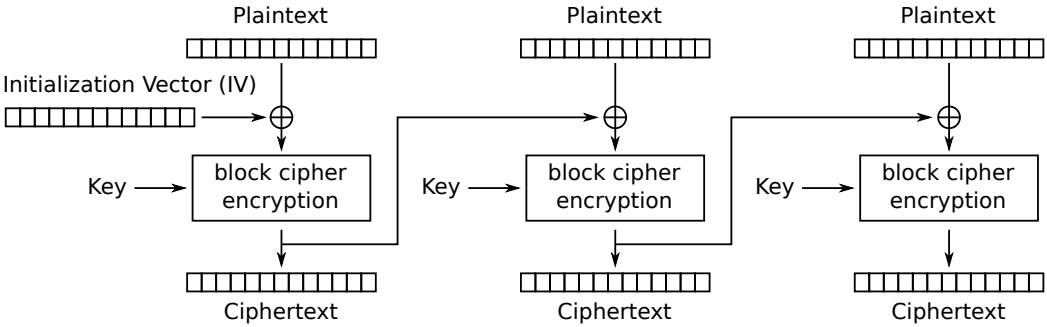
Some desirable features of hash functions $h(x)$

1. h can handle messages of any size
2. The output of h is a fixed size
3. $h(x)$ is relatively easy to compute
4. **Preimage resistance:**
   Given any output z, it is impossible to find an x such that $h(x) = z$
5. **Second preimage resistance:**
   Given any x_1, it is computationally infeasible to find an x_2 such that $h(x_1) = h(x_2)$
6. **Collision resistance:**
   It is computationally infeasible to find any pairs $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$



Cipher Block Chaining (CBC) mode encryption