birthday attack against HMAC

- suppose there is an oracle computing $\text{HMAC}_K(m)$ for any given message m by using key K
- if size of HMAC_K is n, then after $2^{n/2}$ different messages we expect a collision with probability 0.5; let be m_1 and m_2 such colliding messages
- now randomly choose string x e ask oracle to compute $t = \text{HMAC}_K(m_1 | x)$
  - overall we asked oracle for $2^{n/2}+1$ computations
- with "good" probability it holds $\text{HMAC}_K(m_2 | x) = t$
  - if hash function used by HMAC_K is iterated by Merkle-Damgård construction (SHA-1, SHA-2, not SHA-3)
  - m_1 and m_2 should end on some block boundary
  - thus the authentication tag of $m_2 | x$ has been found (with good probability) without asking the oracle for a further computation