

SPAB assignment 04

Task 2

$$n = 100 \cdot 100 \cdot 230 \cdot 15 = 3,45 \cdot 10^7 \text{ number of commits}$$

$$m = 2^{160} \text{ number of possible commit hashes}$$

→ 2 commits with same hash is a birthday problem (2 people with same birthday)

$$\rightarrow p = \prod_{i=0}^{n-1} \frac{m-i}{m} = \frac{m^n}{m^n} \approx \exp\left(-\frac{n^2}{2m}\right) = \exp\left(-\frac{(3,45 \cdot 10^7)^2}{2 \cdot 2^{160}}\right)$$

↑
approximation
for large m and
small n

$$= \exp\left(-\frac{(3,45 \cdot 10^7)^2}{2^{161}}\right) \approx 1$$

$$n = 1000 \cdot 1000 \cdot 365 \cdot 100 = 3,65 \cdot 10^{10} \text{ number of commits}$$

$$p = \prod_{i=0}^{n-1} \frac{m-i}{m} = \frac{m^n}{m^n} \approx \exp\left(-\frac{n^2}{2m}\right) = \exp\left(-\frac{(3,65 \cdot 10^{10})^2}{2^{161}}\right) \approx 1$$