Birthday Attack

Question: There are n people (n is given) in a room, what is the probability that at least two people share the same birthday?



is the probability that all n people have different birthdays







Python Code:

图形用户界面, 文本, 应用程序

描述已自动生成



Therefore, in general:



d is the space of hash

Normally, a hash contains lower and upper case of letters and digits (26+26+10=62 different available characters). In SHA256, the hash string has 64 characters in hex (0-9 and a-f, 16 characters).

The total space of SHA256 hash (d) is .

Finding how many hashing operations will result in a collision with Python:

Suppose the hash has 8 hex characters, 1000 different messages are hashed

文本

中度可信度描述已自动生成