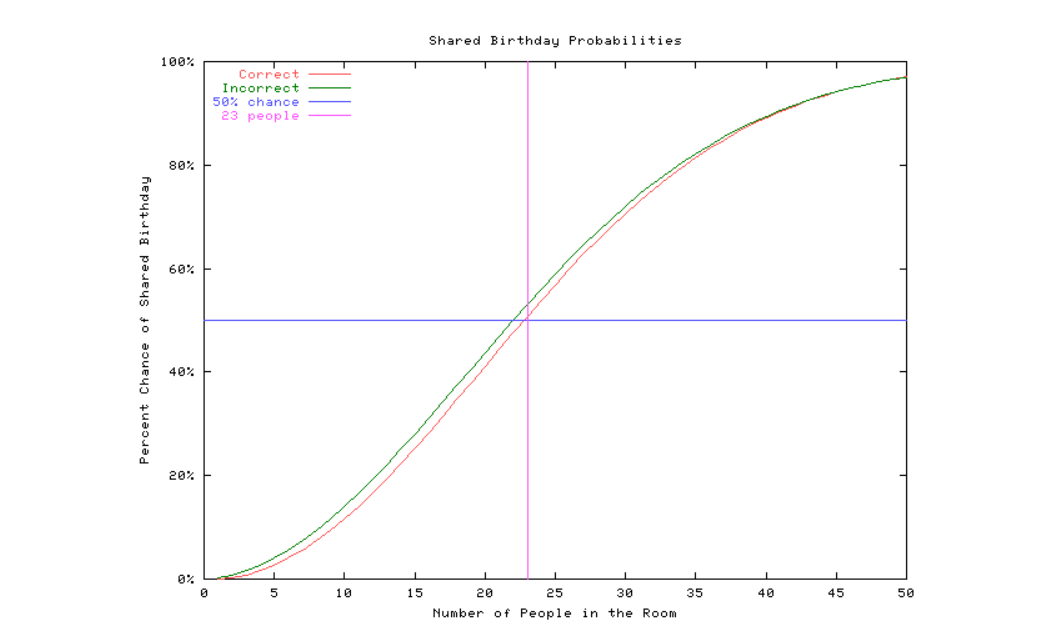
**Aria Javani**

**9725303**

**1:**



**2:**

:

64-bit :

128-bit :

160-bit :

:

64-bit :

128-bit :

160-bit :

**3.1:**

Depending on how great P is, it can be collision resistant or not.

**3.2:**

Since there is no straight and feasible way to compute input having he output, we have to check every number to invert an ouput thus this function is considered as a one way function.

**4:**

**4.1:**

Since the attacker knows and is also available, he can easily reverse the sum by this property: and thus find the key. After acquiring the key he can easily encrypt his own text().

With OTP is the find the key too, though he has to do it every time.

**4.2:**

It’s not possible. We can’t compute the without knowing its key, so we can’t neither find the whole key(unless the random generator of key stream is too short) nor encrypt our text.

**5:**

**6.1:**

It’s a reasonable amount of data to store.

**6.2:**

so in order to prevent the attacker from complete decryption before one month we have to use this many key in the duration of the movie(2h)

**7:**