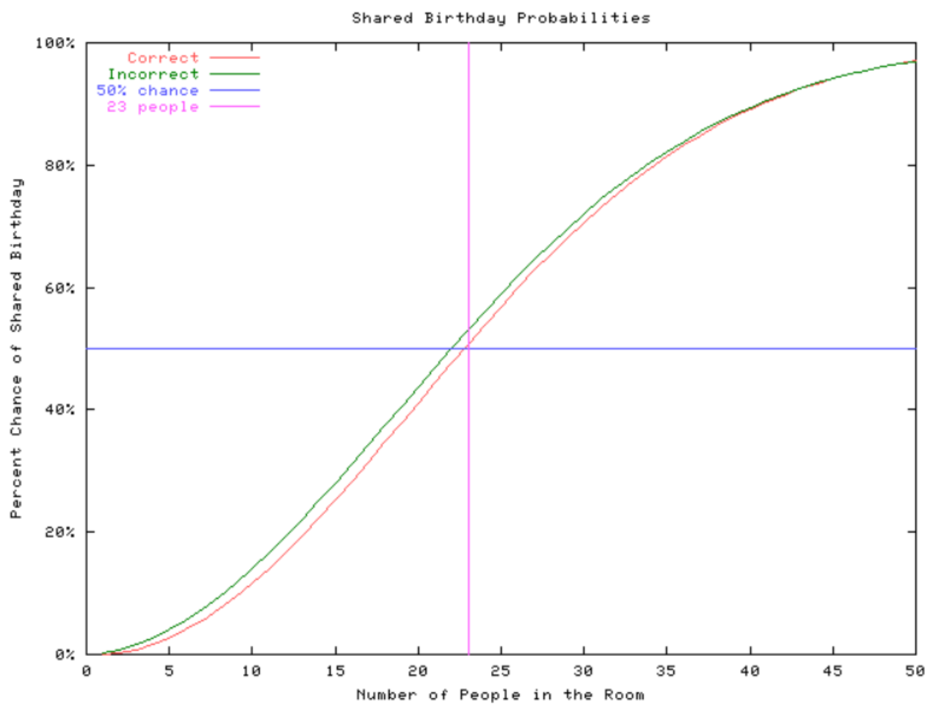
**Aria Javani**

**9725303**

**1:**

a) $0.5 \leq 1 - \left(\frac{365-1}{365}\right)\left(\frac{365-2}{365}\right) \ldots \left(\frac{365-n}{365}\right) \rightarrow n = 23 \rightarrow$ $number\ of\ students = 24$




b) $P(at\ least\ one\ collision) = 1 - \left(\frac{N-1}{N}\right)\left(\frac{N-2}{N}\right) \ldots \left(\frac{N-K+1}{N}\right)$

c) $P(at\ least\ one\ collision) = 1 - \left(\frac{2^n-1}{2^n}\right)\left(\frac{2^n-2}{2^n}\right) \ldots \left(\frac{2^n-r}{2^n}\right) = 1 - \left(1 - \frac{1}{2^n}\right)\left(1 - \frac{2}{2^n}\right) \ldots \left(1 - \frac{r}{2^n}\right) \approx 1 - \left(e^{-\frac{1}{2^n}}\right)\left(e^{-\frac{2}{2^n}}\right) \ldots \left(e^{-\frac{r}{2^n}}\right) = 1 - e^{-\frac{1+2+\cdots+r}{2^n}} = 1 - e^{-\frac{r(r+1)}{2^{n+1}}} \rightarrow 0.5 = e^{-\frac{r(r+1)}{2^{n+1}}} \rightarrow \ln(2) = \frac{r(r+1)}{2^{n+1}} \rightarrow r^2 + r - \ln(2) \,.\, 2^{n+1} = 0 \rightarrow (random\ numbers - 1)^2 + (random\ numbers) -$

1) $-\ln(2) . 2^{n+1} = 0 \rightarrow random\ numbers = \frac{-1 \pm \sqrt{1+\ln(2)2^{n+3}}}{2} + 1 = \frac{1+\sqrt{1+\ln(2)2^{n+3}}}{2}$

**2:**

$\epsilon = 0.5$ :

64-bit : $\frac{1+\sqrt{1+\ln(2)2^{64+3}}}{2} \approx 2^{32}. 2\ln(2)$

128-bit : $\frac{1+\sqrt{1+\ln(2)2^{128+3}}}{2} \approx 2^{65}. 2\ln(2)$

160-bit : $\frac{1+\sqrt{1+\ln(2)2^{160+3}}}{2} \approx 2^{80}. 2\ln(2)$

$\epsilon = 0.1$ :

64-bit : $\frac{1+\sqrt{1+\ln\left(\frac{10}{9}\right)2^{64+3}}}{2} \approx 2^{32}. 2\ln(\frac{10}{9})$

128-bit : $\frac{1+\sqrt{1+\ln\left(\frac{10}{9}\right)2^{128+3}}}{2} \approx 2^{65}. 2\ln(\frac{10}{9})$

160-bit : $\frac{1+\sqrt{1+\ln\left(\frac{10}{9}\right)2^{160+3}}}{2} 2^{80}. 2\ln(\frac{10}{9})$

**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 $x$ and $H(x)$ is also available, he can easily reverse the sum by this property:$a = b \oplus c \rightarrow c = a \oplus b$ and thus find the key. After acquiring the key he can easily encrypt his own text($x'$).

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 $MAC_{k_2}$ 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:**

total data $= 10^6 \frac{bit}{s}.(2h \times 60min \times 60s)s = 72 \times 10^8 bit = 0.9Gbyte$

It's a reasonable amount of data to store.

**6.2:**

total count of keys attacker can find in a month $= 30 \times 24 \times \frac{60}{10} = 4320$

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)

$$key\ generation\ rate = \frac{4320}{2\times60\times60} = 0.6\frac{key}{s} \rightarrow one\ key\ every\ 1.6s$$

**7:**