Birthday Bound

Problem Statement

How many people must there be in a room before there is a 50% chance that two of them were boron on the same day of the year ?

Let us assume # of days is n.

- If $N = n + 1$, probability of collision is 1 (Pigeonhole Principle)
- To ensure probability $\frac{1}{2}$, is the number $n/2$?
- The real answer is surprisingly small. Its about $\Omega(\sqrt{n})$

Q. (i) How many people must there be in a room before there is a 75% chance that two of them were born on the same day of the year ?
(ii) How many people must there be in a room before there is a 99% chance that two of them were born on the same day of the year ?

Are these constructions secure PRF ?

Secure PRF ?/ Secure MAC ?

Let f, g be two random functions and h be a hash function. We ask the following :

- $F_f(r, m) = f(r) \oplus m$
- $F_{f,g}(r, m) = f(r) \oplus g(m)$
- $F_{f,h}(r, m) = f(r) \oplus h(m)$
- $F_{f,g,h}(r, m) = f(r) \oplus g(h(m))$
- $F_{f,g}(r, m) = f(r) \oplus g(r \oplus m)$
- $F_{f,g,h}(r, m) = f(r) \oplus g(r \oplus h(m))$.

Let H be a Merkle-Damgard Iterated Hash Function. We define a MAC $S(k, m) = H(k||m)$. Is $S(k, m)$ a valid MAC (Check the Consistency / Correctness Condition of MAC) ? Is the MAC secure ? If secure, derive the security bound. If not, state the forgery attack.