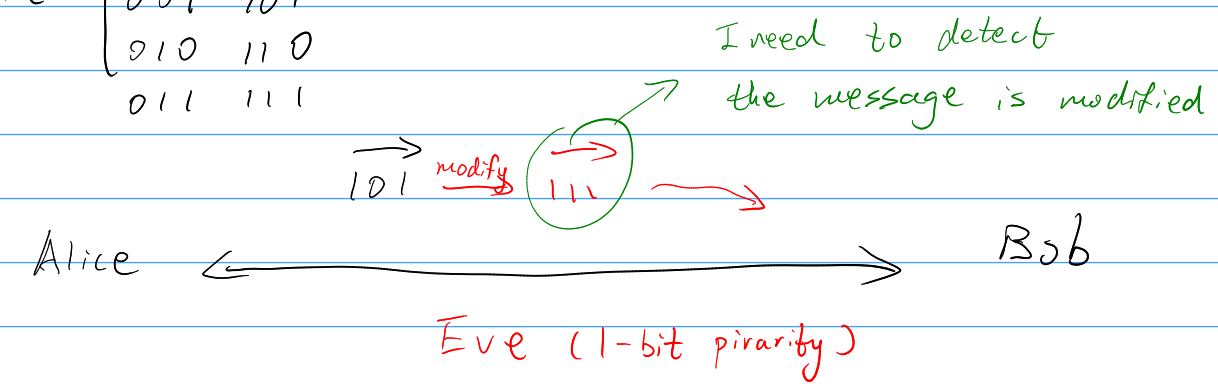
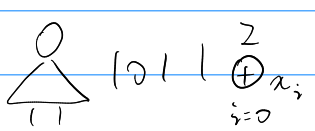
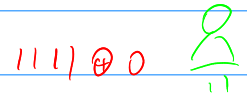
$M = \{ 000\ 100,\ 001\ 101,\ 010\ 110,\ 011\ 111 \}$



Solution!

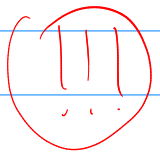
101 □ → tag checksum 111 → [X] It is not correct.





$100 \to 1 \to 101 \to 0$

$1 \oplus 1 \oplus 1 \to 1 \neq 0$ ✗



Eve could change the check sum.!

Uni → asks for bids.

$S_1 \xrightarrow{1000}$ 竞拍最低价

$S_2 \xrightarrow{1050} \to 900$ 如果别人价格泄漏

$S_3 \xrightarrow{950}$ 别人就会调低价格.

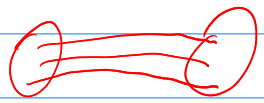
hash function 谁拿到 key 都会泄漏

↑

S_1 $H(1000) = y_1$ $\quad f \xrightarrow{map} 1000 \to y_1$

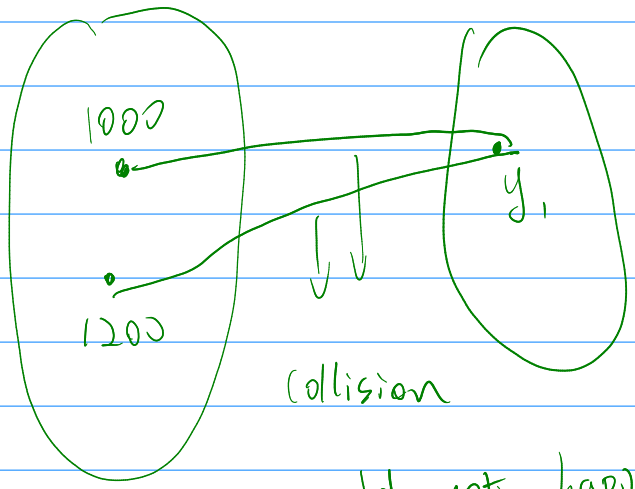
S_2 $H(1050) = y_2$

S_3 $H(950) = y_3$

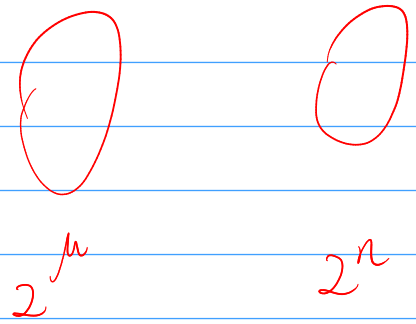


finding x

from $H(x)$ is hard!



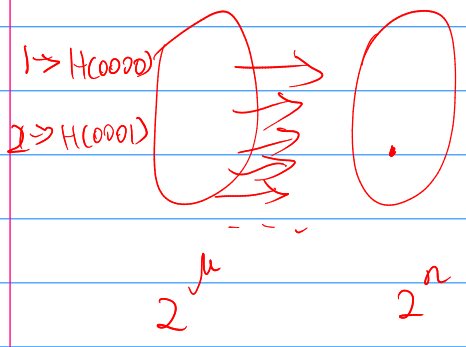
∴ could not happen like this!



$\mu >> n$

much larger than

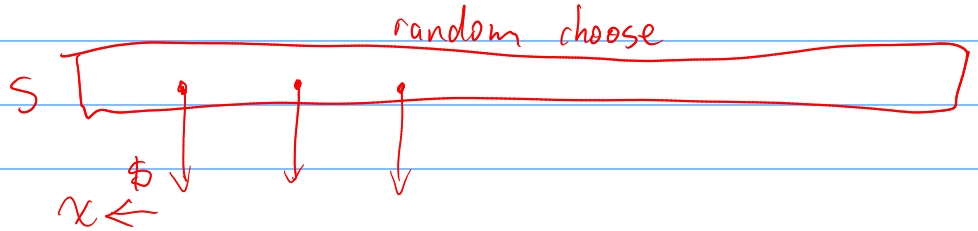
Hardness Collision Attack



Sufficient try 2^{n} times

collision may happen after $2^{\frac{n}{2}}$ time.

Set $N = 2^{n}$



for ($i = 1$ to q)
compute $H(i)$

? For what q, there will be a repetation?

$i = 1$ $i = 2$ $i = 3$ ... $i = q$

$p = 0$ $p = \frac{1}{N}$ $p = \frac{2}{N}$ $p = \frac{q-1}{N}$

No collision

$P = (1 - \frac{1}{N})\ P = (1 - \frac{2}{N})$ .. $P = 1 - \frac{q-1}{N}$

No collision

$P[\text{coll}_2] \times P[\text{coll}_3] \cdots$

$= \left(1 - \frac{1}{N}\right) \times \left(1 - \frac{2}{N}\right) \times \cdots \left(1 - \frac{q}{N}\right)$

$\approx \prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right) = \left(1 - \frac{\sum_{i=1}^{q-1} i}{N}\right)$

$= 1 - \frac{q^2}{2^{n+1}}$

2^n $\quad \frac{(q-1)\cdot q}{2} \quad \frac{2^n}{2^{n+1}}$

$1+2+\cdots+N$

$= \frac{N(N+1)}{2}$

$1+2+\cdots+(q-1) \quad \frac{(q-1)\cdot(q-1+1)}{2}$

$= \frac{(q-1)\cdot q}{2}$

$1 - \left(1 - \frac{q^2}{2^{n+1}}\right)$

$\frac{q^2}{2^{n+1}}$