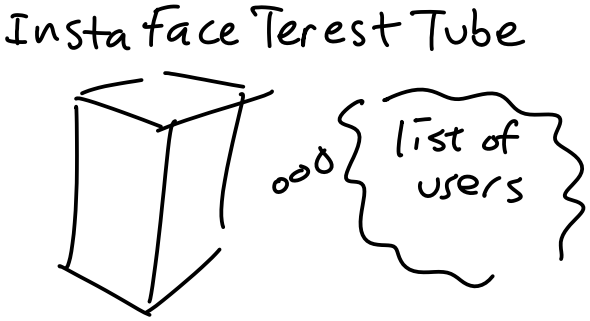
# Some Fun Stuff

Final exam Thursday @ 12

What does Mike do all day?

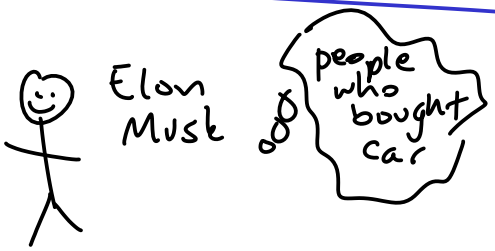



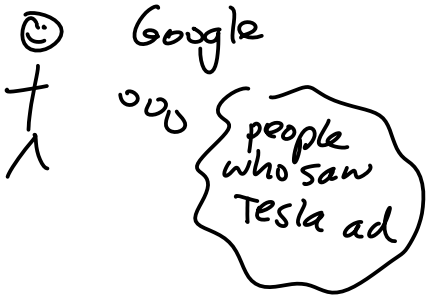

Alice wants to learn which friends use this site

Alice doesn't want site to learn her address book

site doesn't want Alice to learn anything <u>else</u> about its users

---




Want to learn: how many people saw ad AND bought car?

Don't learn anything else

---

## Private Set Intersection (PSI)

Alice has set of items $X$

Bob has $Y$

learn <u>only</u> $X \cap Y$ (or something related, like $|X \cap Y|$)

## Reasonable Idea that doesn't work:

Alice $X = \{x_1, \ldots, x_n\}$

Bob $Y = \{y_1 \ldots y_n\}$

for each $x_i$ is $H(x_i)$ included ? if so, $x_i$ in $X \cap Y$

$\xleftarrow{H(y_1),\ H(y_2),\ \ldots}$

**Idea:** If $H$ is collision-resistant, can assume

$$H(x_i) = H(y_j) \iff x_i = y_j \qquad \text{(correctness)}$$

If $H$ is hard to invert, then hard to compute $y_j$'s given $H(y_j)$'s

**Problem:** Suppose $X, Y \subseteq \{\text{phone numbers}\}$

only ~ billions of phone numbers

$\Rightarrow$ dictionary attack: compute $H(x)$ for every possible phone number $x$

Alice can figure out Bob's entire input $Y$ !!

---

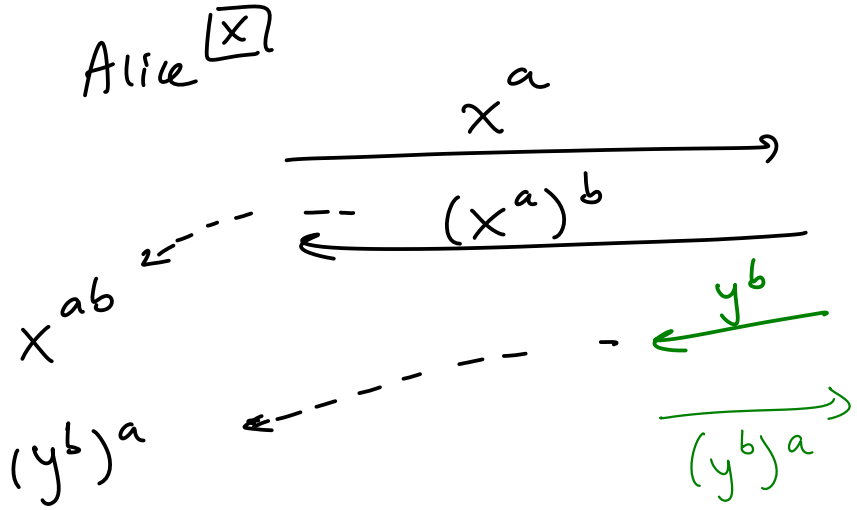
## Better Idea:

Simple case: each person has 1 item

Alice $(x)$ Bob $(y)$

want to learn "does $x = y$?"

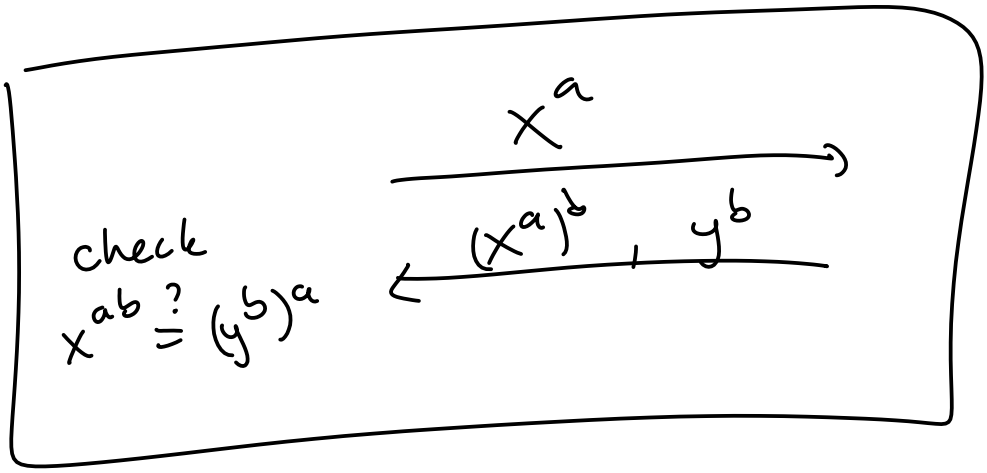
In case of $x \neq y$, don't learn <u>anything</u> about other person's input




Obs: $x = y \iff x^{ab} = y^{ab}$

what Alice wants to learn

something she can test




Let's say $x \neq y$, Alice tries to do dictionary attack

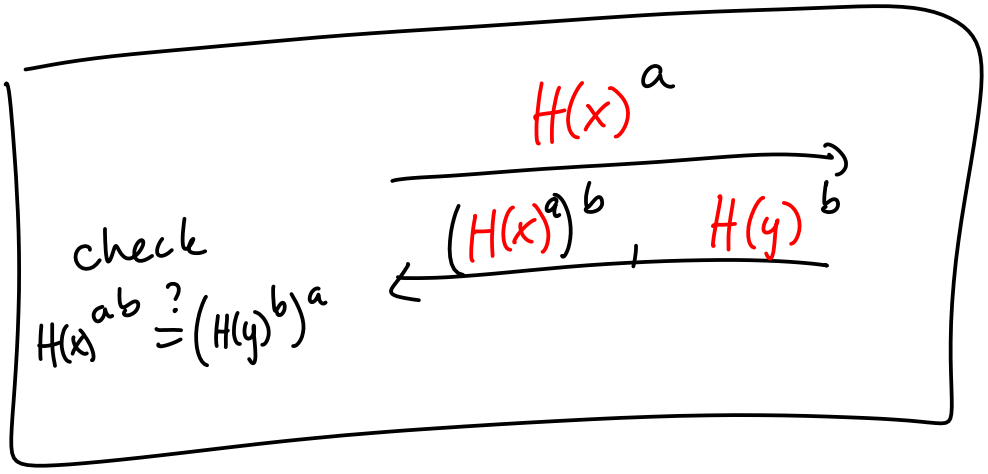
Alice knows $x^{ab}$, $y^{ab}$ (but not b)

can she compute $z^{ab}$ for other z values?

- $1^{ab}$
- $(x^{ab})^2 = (x^2)^{ab}$

If Alice can guess that $y = x^2$ then she can verify that guess by testing $(x^{ab})^2 \stackrel{?}{=} y^{ab}$

Fix:



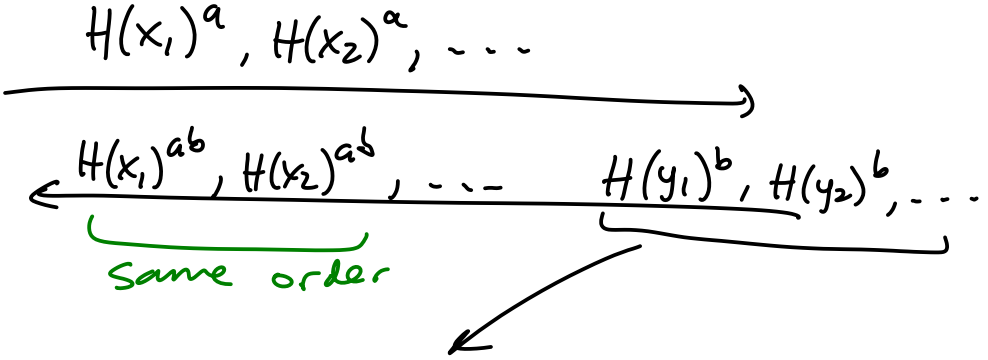

Idea: $H(x)$, $H(y)$ are "unrelated" even if $x$, $y$ are related (like $y = x^c$ for some known $c$)

---

Hard to find $c$: $H(x) = H(y)^c$

# Full-fledged PSI:

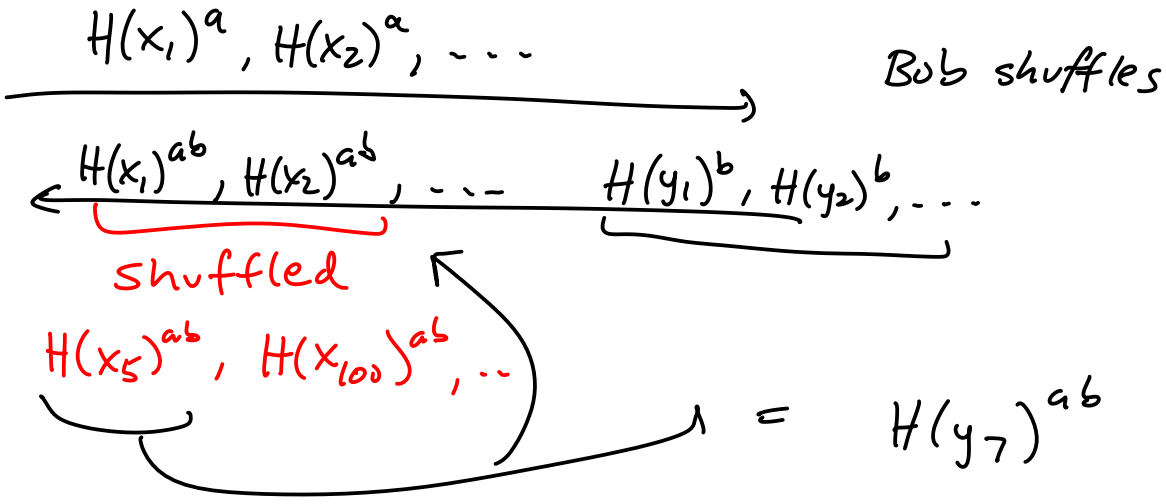
$X = \{x_1 \cdots x_n\}$ $\quad$ $Y = \{y_1 \cdots y_n\}$




for each $x_i$
check $H(x_i)^{ab} \in \{(H(y_i)^b)^a\}$

## Hide contents of intersection, reveal only size

$X = \{x_1 \cdots x_n\}$ $\quad$ $Y = \{y_1 \cdots y_n\}$




Alice doesn't know which $x_i$ corresponds to 1st item in