Intro to Privacy (& Security)

What do we mean by "privacy"?

- control of access
- control of use
- knowledge of over-use
- ownership of data
  opt-in vs opt-out
- "anonymity"

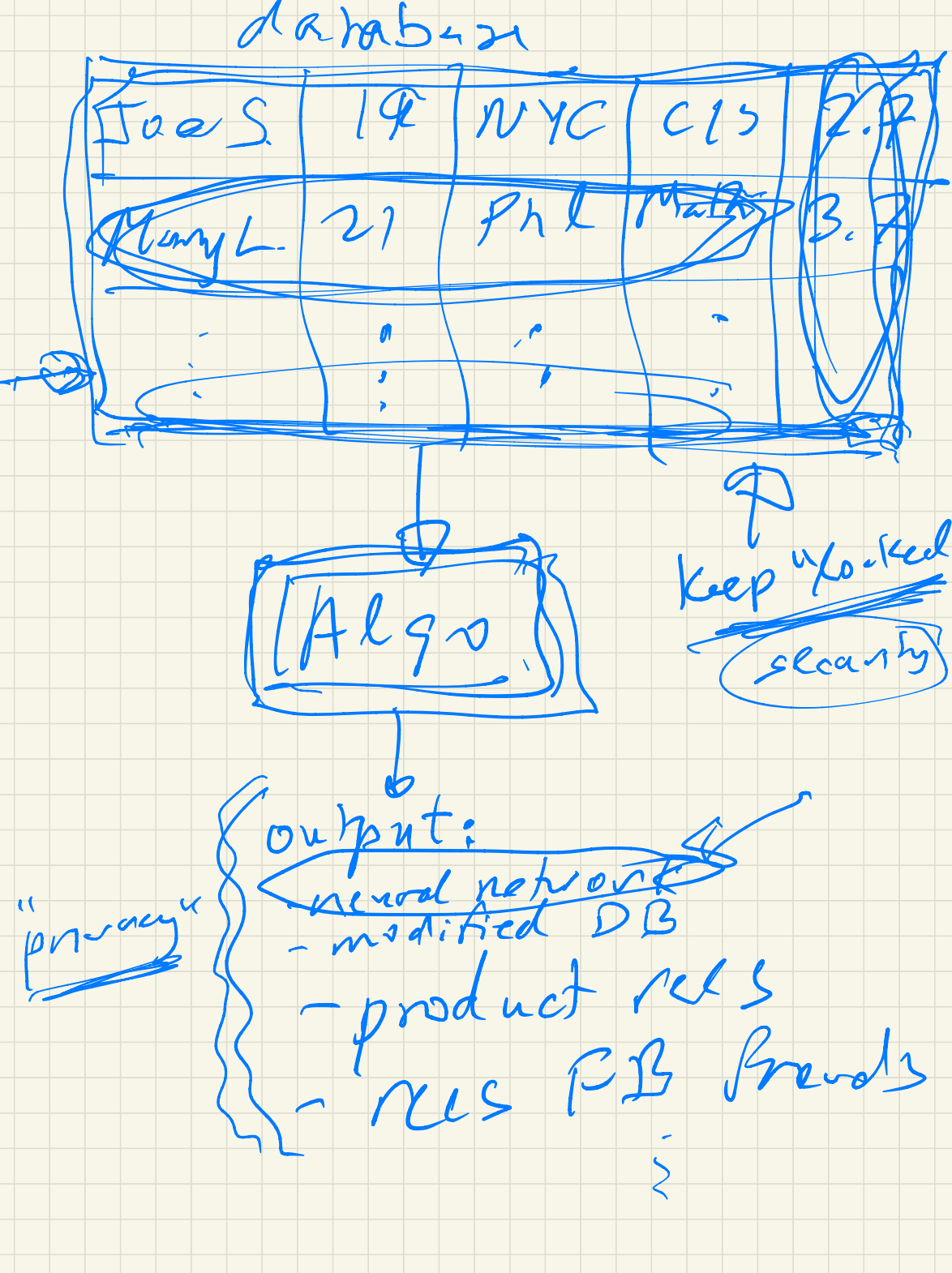
⋮

Key distinction:

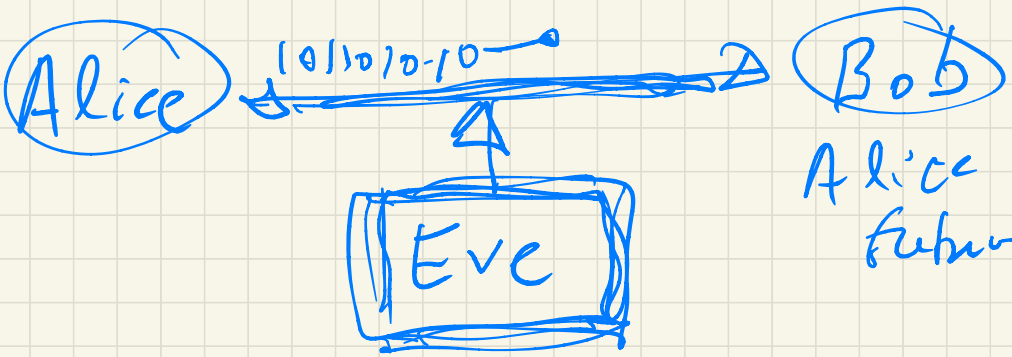
control of access ↗ security & crypto

vs.

control of inferences ↘ privacy


database
Algo
keep "worked"
security
output:
neural network
- modified DB
- product recs
- recs PB
"privacy"

A very short crypto primer



"one-time pad"

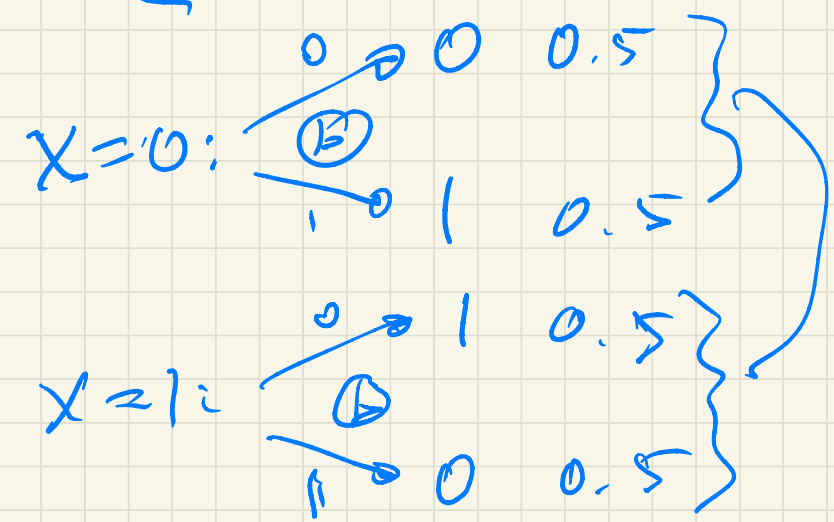
- Alice wants to send a single bit $x \in \{0,1\}$ to Bob
- Alice & Bob get together, generate a random bit $b \in \{0,1\}$
- Later, what should Alice send to Bob?

Idea: Alice sends to Bob

the bit $x \oplus b$

$$x \oplus b \triangleq \begin{cases} 0 & \text{if } x = b \\ 1 & \text{otherwise} \end{cases}$$

Eve



Decryption by Bob:

$y_1 y_2 \ldots$

$(x \oplus b) \oplus b = x \oplus (b \oplus b)$

$x_1 x_2 x_3 \ldots$

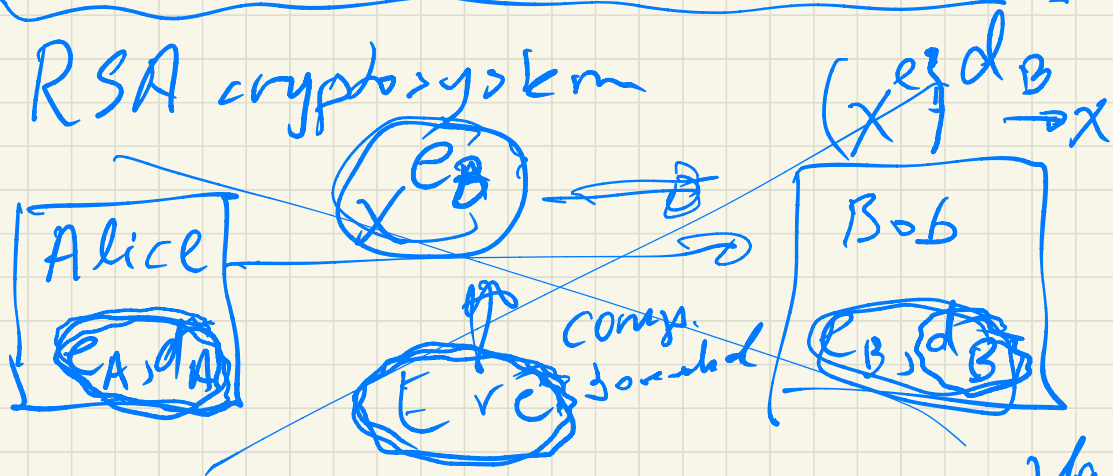
$\oplus \; \oplus \; \oplus$

$b_1 b_2 b_3 \ldots\ldots b_n = x$

0

Public-Key Cryptography (1970s)

- RSA cryptosystem



directory: Alice: e_A, Bob: e_B } public keys

e.g. RSA is "as secure" as factoring integers is computationally hard

i.e. I give you $N = p \cdot q$

→ {2, 3, 4, 5, 7, 11, 13, 17, ...} prime # · p

If N is a K-digit #,