Translate the paint-mixing Trick into numbers

So that Computers can do the trick through math

Why we start with the paint then?

One-way action

Can be done

"mixing the paint"

But can't be Undone

"unmix"

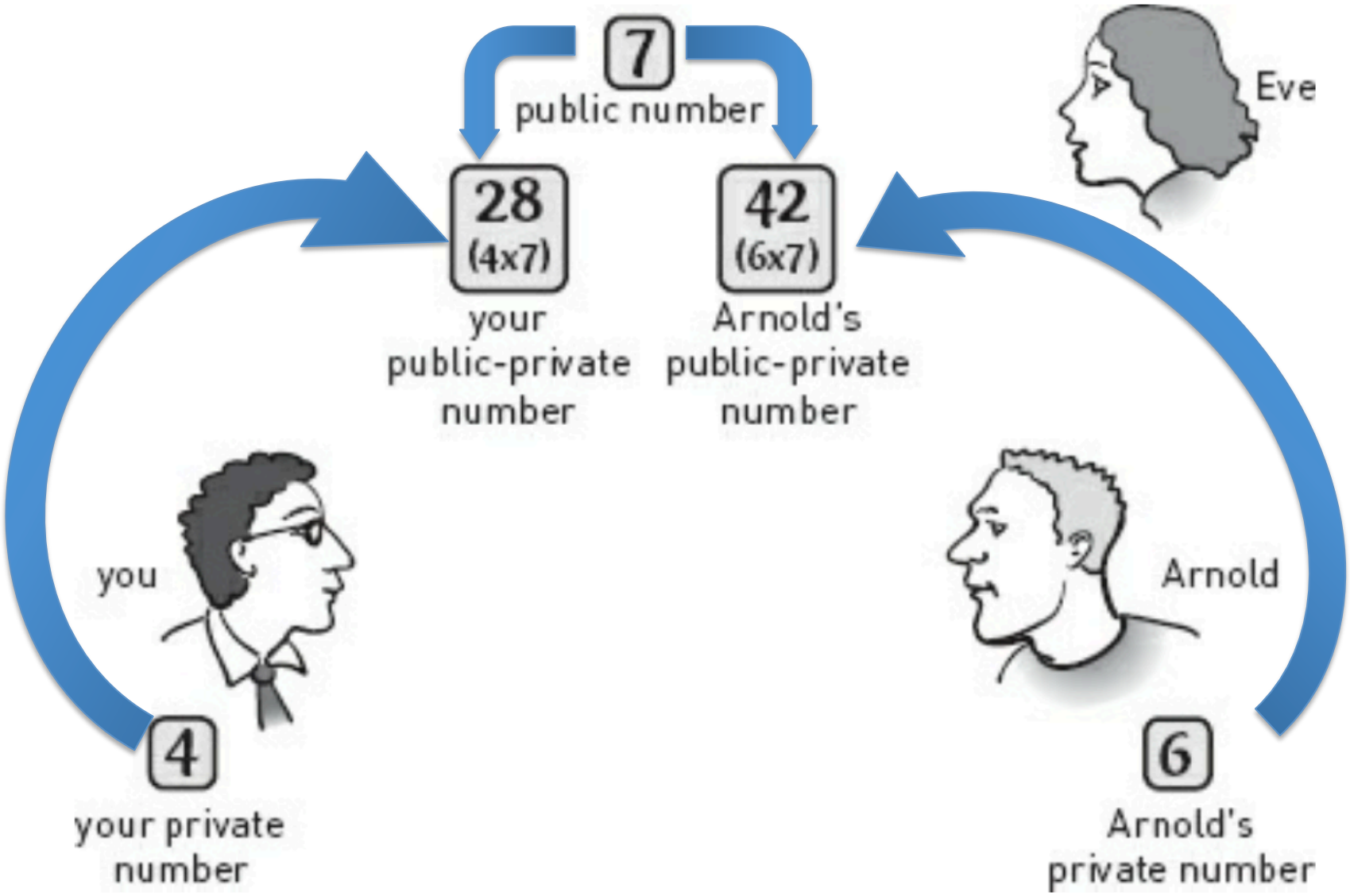
Pretend math: multiply✓

❄❄❖❄❄❄✕

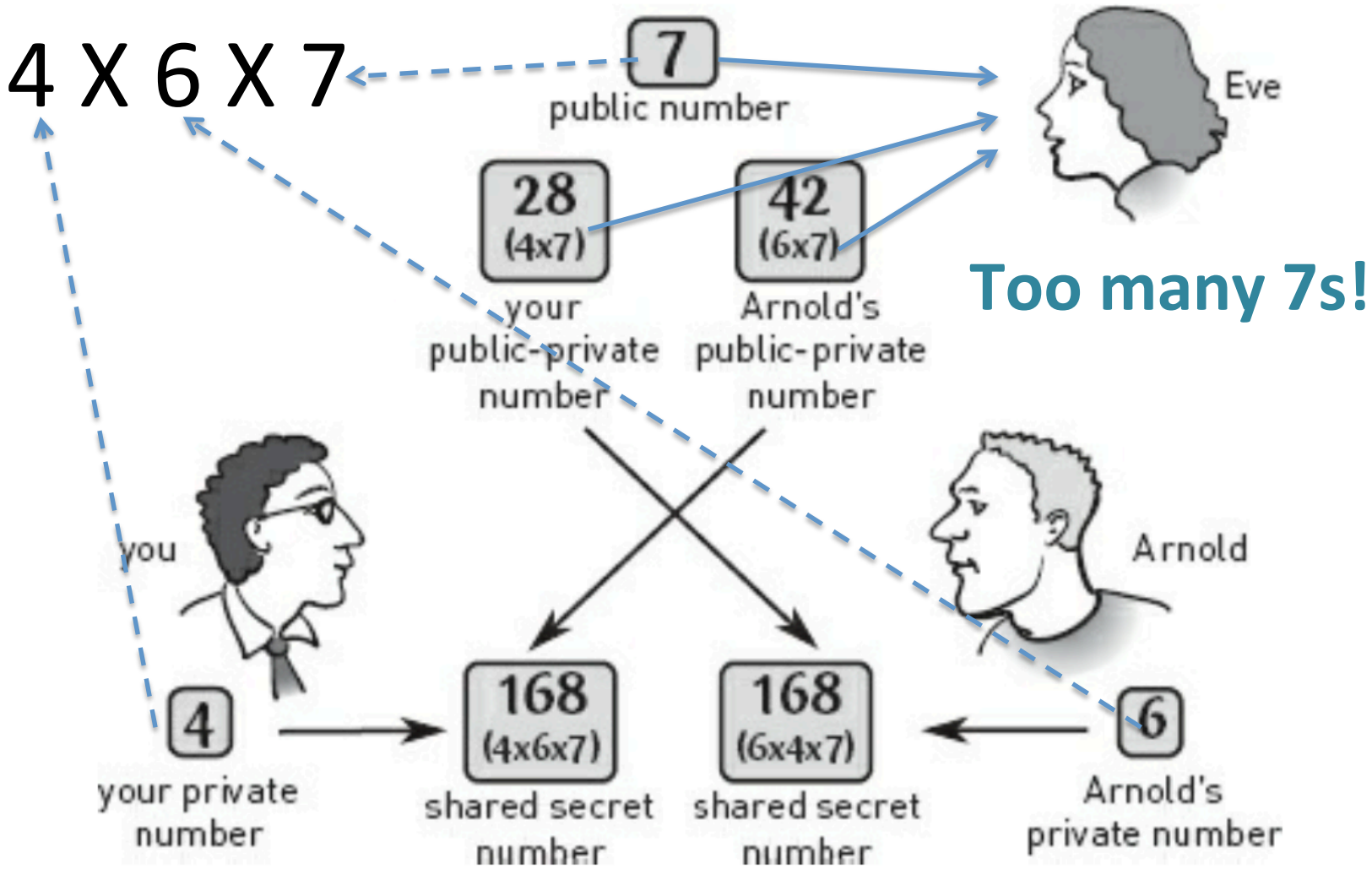
Same question here:
establish shared secret with Arnold
without letting Eve know.
All communications are public.

Start the same way:
Step 1 - choosing a private number
4 → you, 6 → Arnold
Step 2 - agree on a public number
7

Public-private mixture (number)



Get Shared Secret!



Real life: discrete exponentiation✓

❄⁜▲❋❒❄▼❄ ●❑⁕❁❒⁜▼⁕❍✕

1st: Clock arithmetic: 10 + 4 = 2

10am + 4h = 2pm

Slightly different from a clock

– size doesn't have to be 12

– Start from 0 rather than 1

Use 11 as an example clock size

– 7 + 8 + 9 = 24 = 2

– 8 X 7 = 56 = 1

2nd : power notation: 6 X 6 X 6 X 6 = 6

Step 1 - choosing a private number

8 → you, 9 → Arnold

Step 2 - agree on a **clock size(11)**

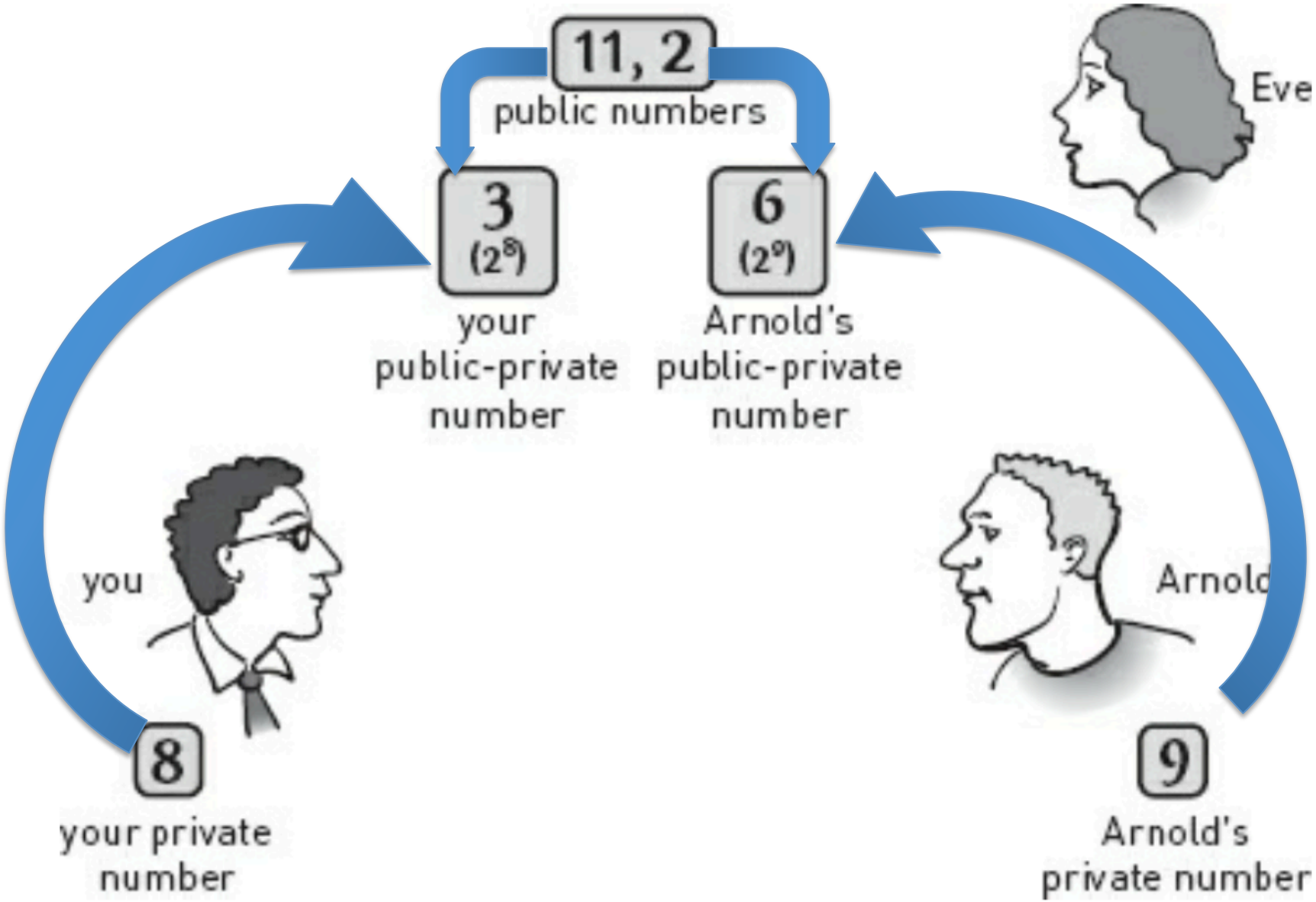
and a **base number(2)**

public- private number(PPN)

= base$^{\text{private number}}$(clock size)

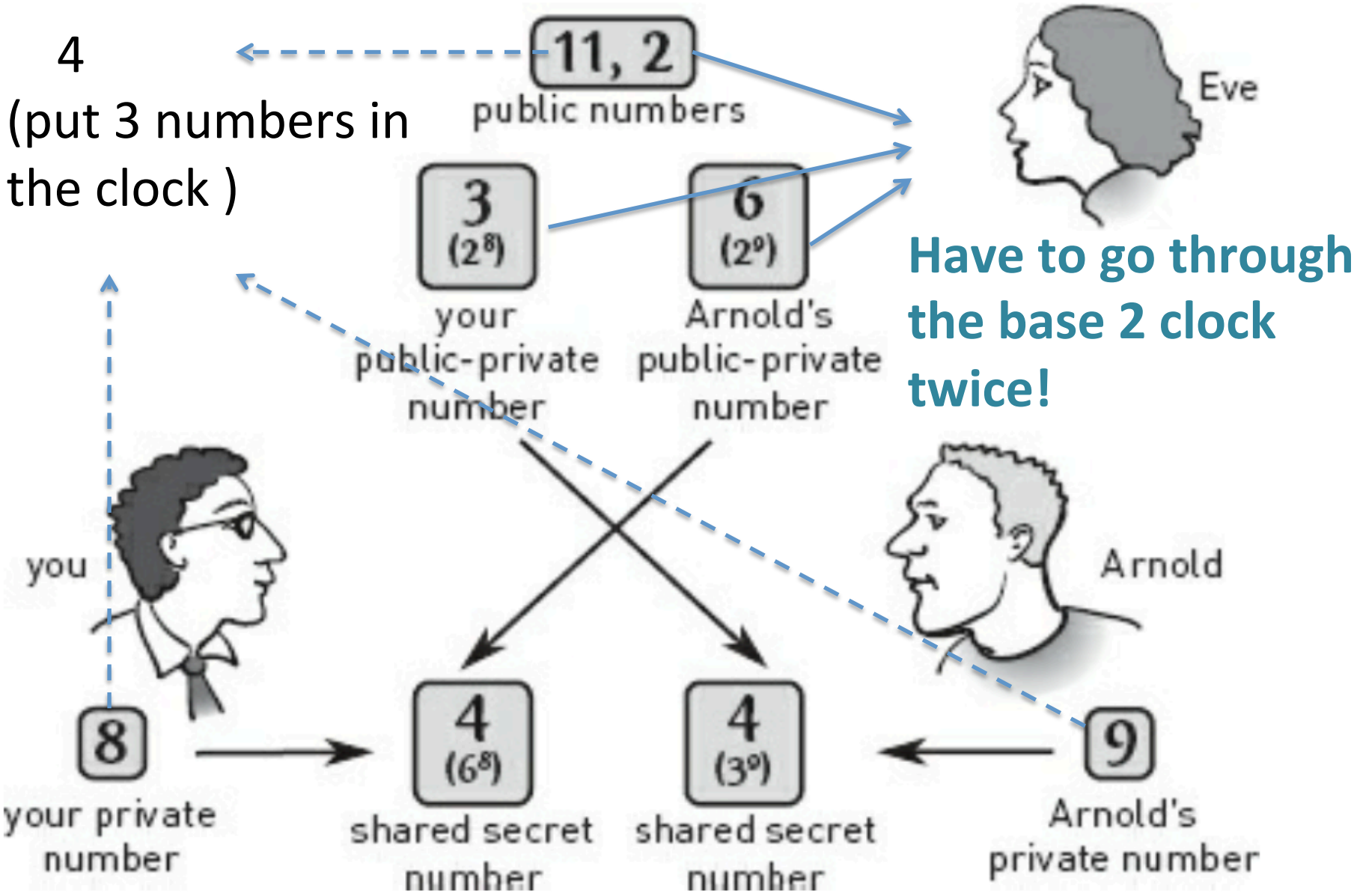
your PPN = 2^8 = 3

Arnold's PPN = 2^9 = 6


11, 2
public numbers
Eve
3
(2^8)
your
public-private
number
6
(2^9)
Arnold's
public-private
number
you
Arnold
8
your private
number
9
Arnold's
private number

4

(put 3 numbers in the clock)



Diffie-Hellman key exchange protocol

- Named after Whitfield Diffie and Martin Hellman, who published the algorithm in 1976

- Whenever using “https:” instead of “http:” your computer and the web server are communicating with a shared secret

- Difference with our algorithm
  - Way larger clock (more possible private numbers)
  - Usually a few hundreds digits

There are other public key algorithms get the message directly from intended recipient

But doing additional tricks with public information preferable under most circumstances, as it requires less computation