*aka end-to-end encryption

A SHALLOW DIVE ON E2EE

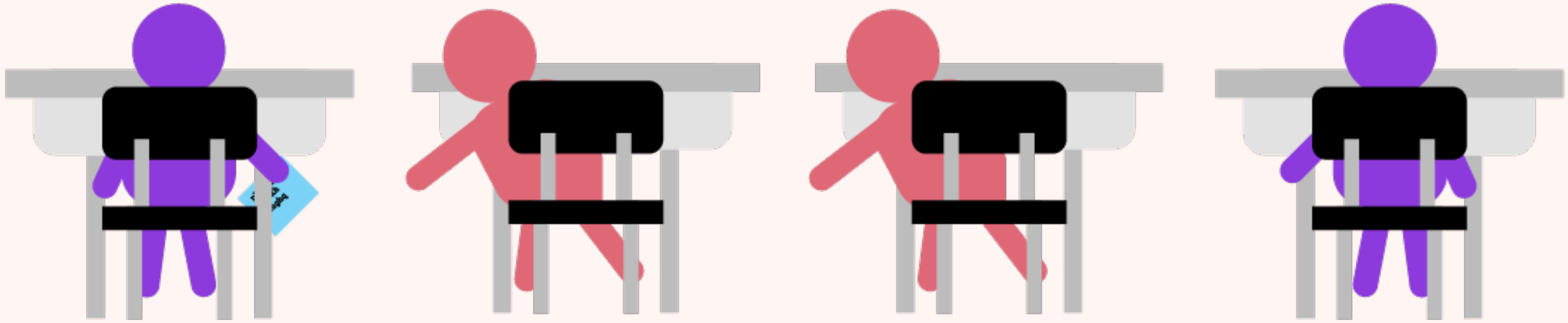
Zepto 5 Feb 2021

DISCLAIMER

- End-to-end encryption is strictly limited for personal use in mainland China.
- For instance, IM tools are not allowed to offer this level of encryption due to the supervision requirement.
- You might face legal issues if you get too creative with this technique.
- By giving out this talk, we are not encouraging you to violate regulations in any means.

HOW TO PASS A NOTE IN CLASS

- Say Alice wants to tell Bob to “meet me in the garden after class”.



- But she wants the meeting to be private, in other words, classmates should not understand the note.
- What to do?

HOW TO PASS A NOTE IN CLASS

- Easy!
- Alice could simply “shift the characters”.

meet me in the garden after class

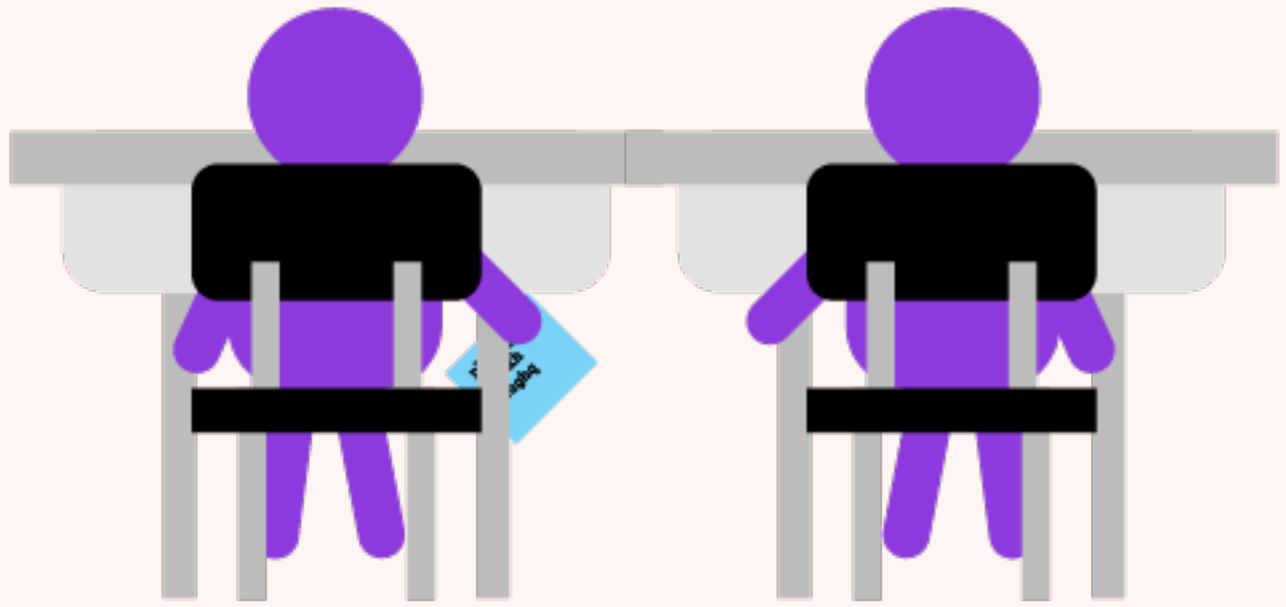
HOW TO PASS A NOTE IN CLASS

- **Other classmates will be totally confused as she uses an American keyboard to achieve this.**
- **And Bob will decrypt the message easily *if he knows what technique Alice is using*.**

nwwr nw ub rgw fleswb ldrwe xklaa

THIS TECHNIQUE WORKS ONLY IF

- Alice and Bob exchange the key idea beforehand using a safe method.
- And we know the safest method to communicate is....
- Find a quiet place ~~and enjoy themselves.~~
- Which brings us downsides of this way...



- Sender and receiver will have to find a way to exchange the “shifting method”, aka the key, in advance.

- Since they both hold the same key, the possibility of a key leakage doubles 😢

- For the same reason, the technique is named *symmetric encryption*.

ANY FIX?

IDEAL SITUATION

- We want to find a solution that
  - It’s safe to distribute remotely over a possibly insecure network.
  - Even someone else manages to hijack the transmission, they will not be able to understand the content, even they have “the key”.
  - Consumes reasonable computing power/time.
- Sounds too picky?

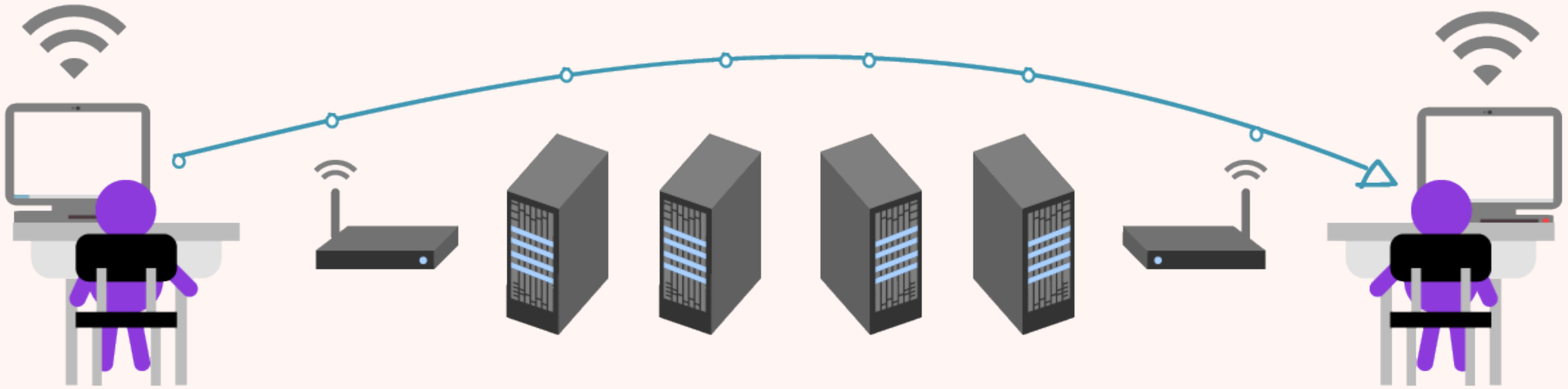
INTRODUCING RSA

RSA COULD HELP US ACHIEVE E2EE

- The method enables us to
  - Make sure only the sender and intended recipient can understand the message.
  - Anyone else, even the server, have no access to the original data.
  - Exchange keys (sort of) over an insecure network, and remain safe.
- How does it actually work?

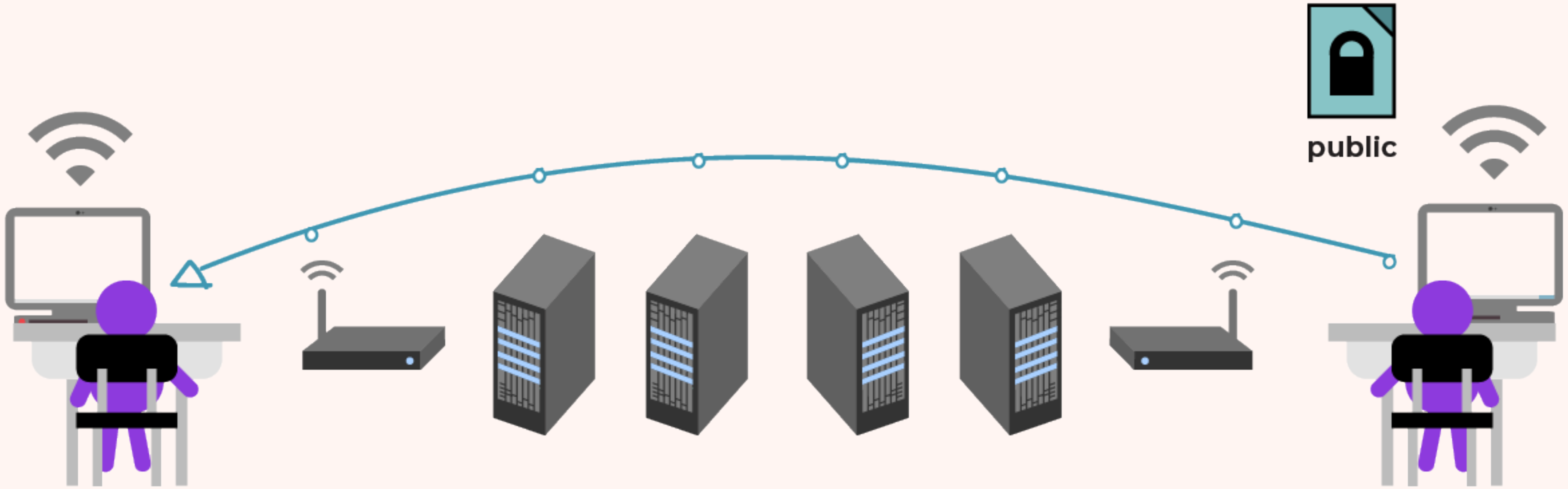
HOW DOES IT WORK

- Say Alice wants to tell Bob to “meet me in the garden after class”.
- But this time, through an insecure network, such that the server may leak the message or the wireless connection may be eavesdropped.
- *They use internet since they are both Zoom University students, just like us.



HOW DOES IT WORK

- Naturally, they have to use some kind of “key” to encrypt the message.
- The speciality comes here. RSA uses a set of two keys to achieve that.
- First, Bob will give Alice a “public key”, that is, could be publicly transported.



HOW DOES IT WORK

- **The public key looks like this:**

```
-----BEGIN PUBLIC KEY-----
MFswDQYJKoZIhvcNAQEBBQA
DSgAwRwJARe5nf//
9ZwklzyIaNC8SWG9EanVB2Yi
4
fy0b1aUHArIxp6yplLHFK1Q/
AdfQ3IJrVE3hIg7akkitG6liP+h
dnwIDAQAB
-----END PUBLIC KEY-----
```

- **Using this key, Alice encrypts the message, and that’s what Bob receives:**

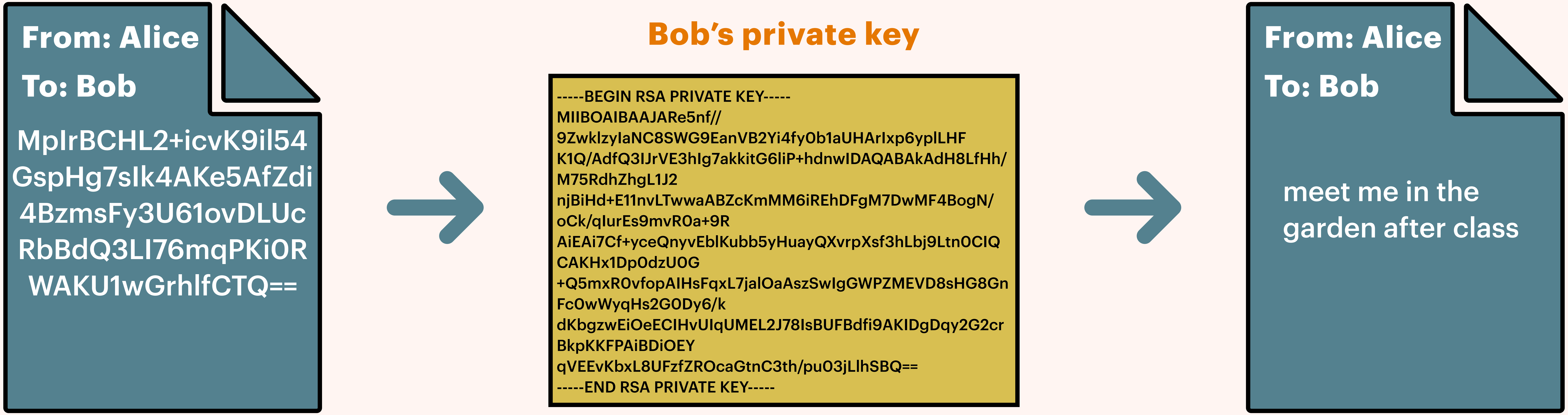
From: Alice

To: Bob

```
MpIrBCHL2+icvK9il54
GspHg7sIk4AKe5AfZdi
4BzmsFy3U61ovDLUc
RbBdQ3LI76mqPKi0R
WAKU1wGrhlfCTQ==
```

HOW DOES IT WORK

- The message is human-unreadable, and with the public key we can’t convert it back to the original text. (We will explain the reason later).



From: Alice

To: Bob

MpIrBCHL2+icvK9il54
GspHg7sIk4AKe5AfZdi
4BzmsFy3U61ovDLUc
RbBdQ3LI76mqPKi0R
WAKU1wGrhlfCTQ==

Bob’s private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOAIBAAJARe5nf//
9ZwklzyIaNC8SWG9EanVB2Yi4fy0b1aUHArIxp6yplLHF
K1Q/AdfQ3IJrVE3hIg7akkitG6liP+hdnwIDAQABAkAdH8LfHh/
M75RdhZhgL1J2
njBiHd+E11nvLTwwaABZcKmMM6iREhDFgM7DwMF4BogN/
oCk/qIurEs9mvR0a+9R
AiEAi7Cf+yceQnyvEblKubb5yHuayQXvrpXsf3hLbj9Ltn0CIQ
CAKHx1Dp0dzU0G
+Q5mxR0vfopAIHsFqxL7jalOaAszSwIgGWPZMEVD8sHG8Gn
Fc0wWyqHs2G0Dy6/k
dKbgzwEiOeECIHvUIqUMEL2J78IsBUFBdfi9AKIDgDqy2G2cr
BkpKKFPAiBDiOEY
qVEEvKbxL8UFzfZROcaGtnC3th/pu03jLlhSBQ==
-----END RSA PRIVATE KEY-----
```

From: Alice

To: Bob

meet me in the
garden after class

- However, with a “private key” that only himself knows, Bob could decrypt the text.

SUMMARY

- The Recipient shares the “public key” publicly so that the sender could use it to encrypt his words and send it out using even insecure network.
- After receiving the message, the recipient decrypt it using the corresponding private key WHICH THEY WON’T LET ANYONE ELSE KNOW (or it will no longer be private), and they will see the intact message.
- Others, including the sender, cannot decrypt the message easily with a public key.
- The server knows the metadata (encrypted text) but cannot understand it without the private key.
- Since the keys used for encrypting and decrypting are different, RSA is an asymmetric encryption method.

⚠️WARNING: BORING MATHS

WHY DOES IT WORK

- * I’m not a cryptography professional, please correct me if there’s anything wrong.
- First, we have a simple fact.
  - It easy to multiple some large prime numbers, whilst it not that easy to find the factors of a large composite number.
  - By now, the only way to factorise huge composite number is by brute force.

WHY DOES IT WORK

- **Based on this fact, Ron Rivest, Adi Shamir and Leonard Adleman invented the following algorithm.**
  - **Choose two arbitrary, distinct prime numbers p, q, and let $n = p \times q$.**
  - **Hence, we have $\varphi(n) = (p-1)(q-1)$.**
    - ***Euler's totient function, written as $\varphi(n)$, counts the positive integers up to a given integer n that are relatively prime to n, and it's a multiplicative function.**
  - **Choose a arbitrary integer e such that it's relatively prime to $\varphi(n)$, and satisfies $1 < e < \varphi(n)$.**

WHY DOES IT WORK

- **Choose two arbitrary, distinct prime numbers p, q, and let $n = p \times q$.**
- **Hence, we have $\varphi(n) = (p-1)(q-1)$.**
- **Choose a arbitrary integer e such that it's relatively prime to $\varphi(n)$, and satisfies $1 < e < \varphi(n)$.**
- **Let d be the modular multiplicative inverse of e to $\varphi(n)$, that is, $ed \equiv 1 \mod \varphi(n)$.**
- **There we have it. The public key is (e, n), and the private key is (d, n).**

WHY DOES IT WORK

- There we have it. The public key is (e, n), and the private key is (d, n).
- For any integer X, we have $X \equiv X^{ed} \bmod n$.
- See the example.
  - Say the message is M.
  - Alice calculates the encrypted text C using $C = M^e \bmod n$;
  - Bob gets the original message M since $M = C^d \bmod n$.
- *In daily use, the numbers in key set is so large that we use strings to represent them.

SOME QUESTIONS

- **Proof that for any integer X, we have** $X \equiv X^{ed} \bmod n$**.**
- **Design a possible way to calculate the private key using the public key, and explain why it is so hard that RSA is highly secure.**

GET CREATIVE

APPLICATION

WhatsApp

Signal

Telegram

APPLICATION

- If you share the private key to the public and the use public key to encrypt some text.
- You are creating a legit signature that everyone could read but only you could sign.

APPLICATION

- Collect Telegram/QQ/WeChat/WhatsApp IDs in public platform.
- “Friends of benefits”.

OUTRO

A SHALLOW DIVE ON E2EE

Zepto
Faculty of Engineering