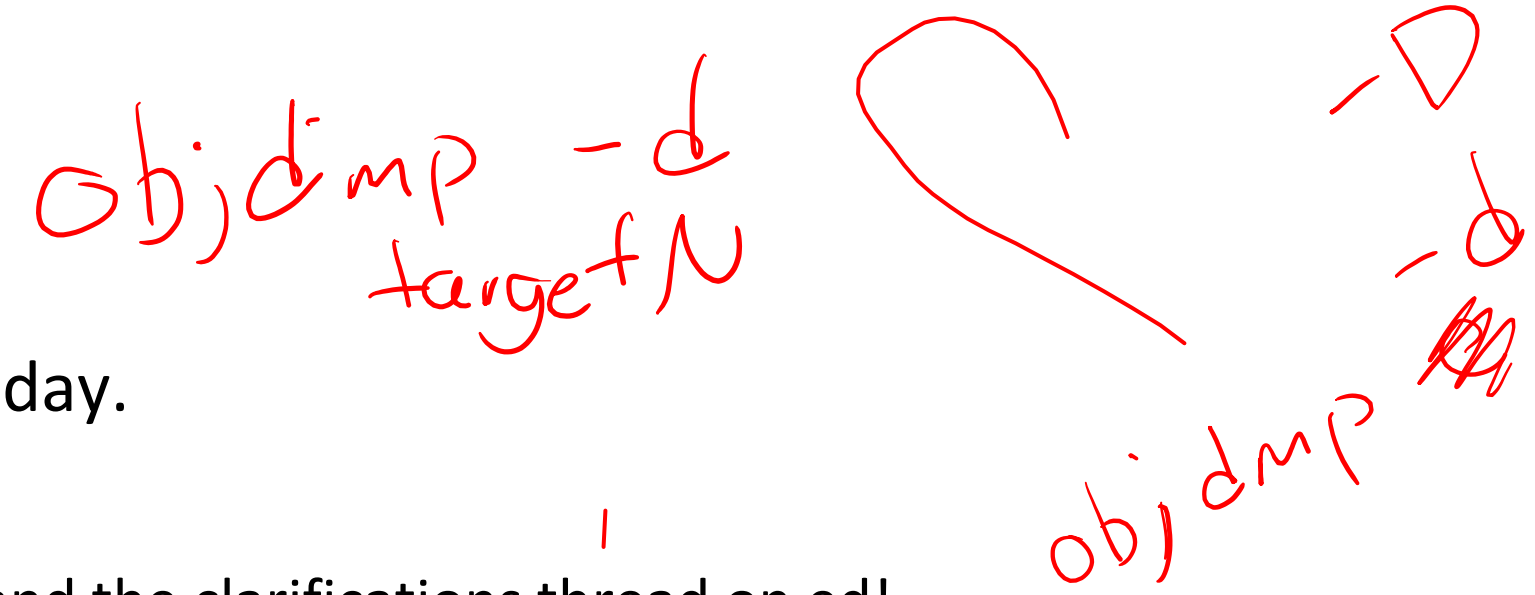
CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials

Admin



- Lab 1b due Wednesday.
  - Ask questions!
  - Do the exercises!
  - Read the readings and the clarifications thread on ed!
    - Remember: C code may be deceptive, disassemble the program (objdump or disassemble)
- Late days:
  - If you go over 3 late days for an assignment, email me to hand it in.
    - Barring a pre-agreed reason, this will result in -20% per day over the limit.

Threat modeling again^4

- You notice that people seem to be writing code with LLMs… a lot!
- These have a habit of ‘hallucinating’ (bullshitting) package names to import that don’t exist
  - E.g. import huggingface-cli
- What might a clever adversary do?
- What behavior by a victim would they be relying on?
- How might they be caught?

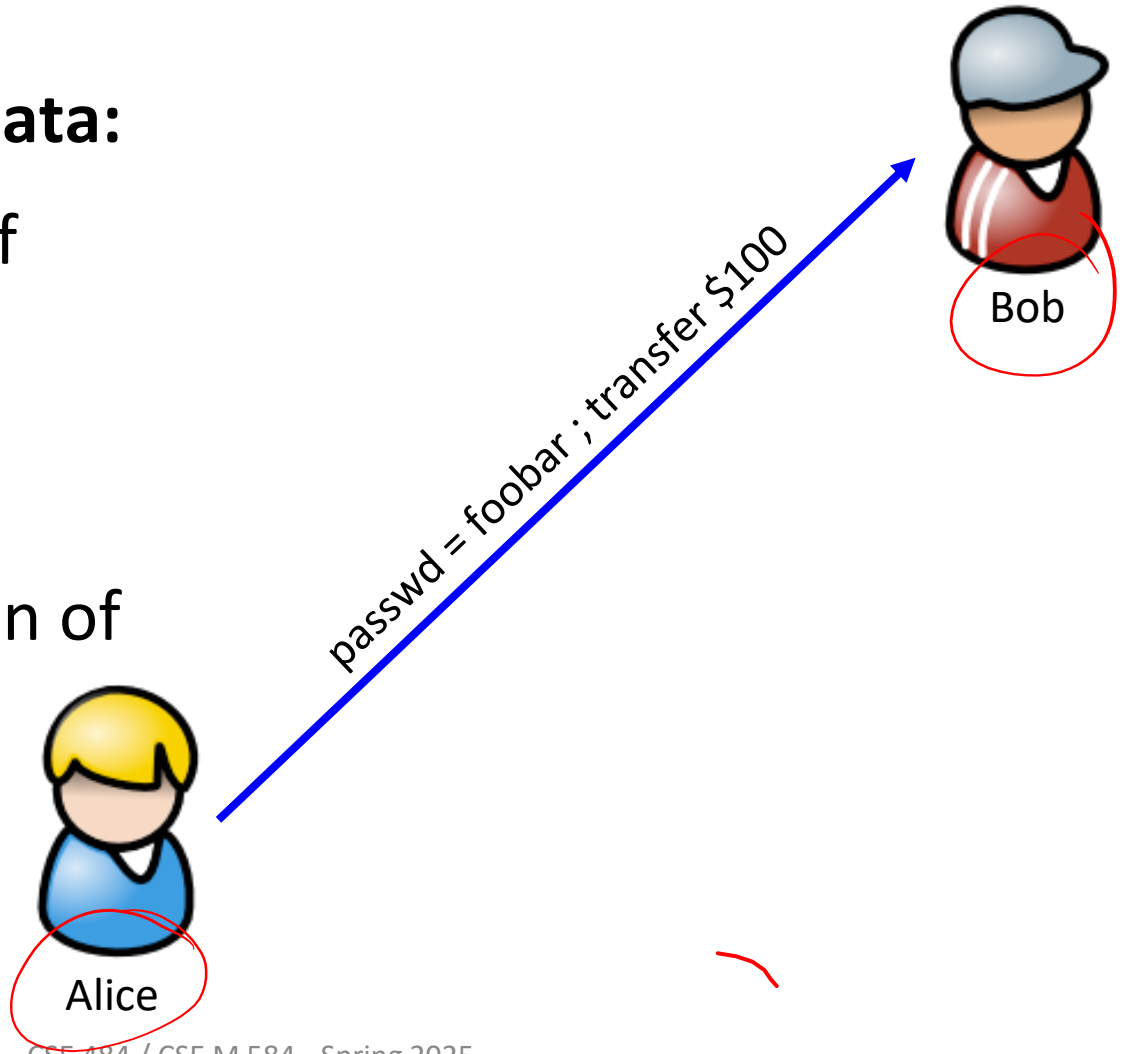
Common Communication Security Goals

Confidentiality of data:

Prevent exposure of information

Integrity of data:

Prevent modification of information



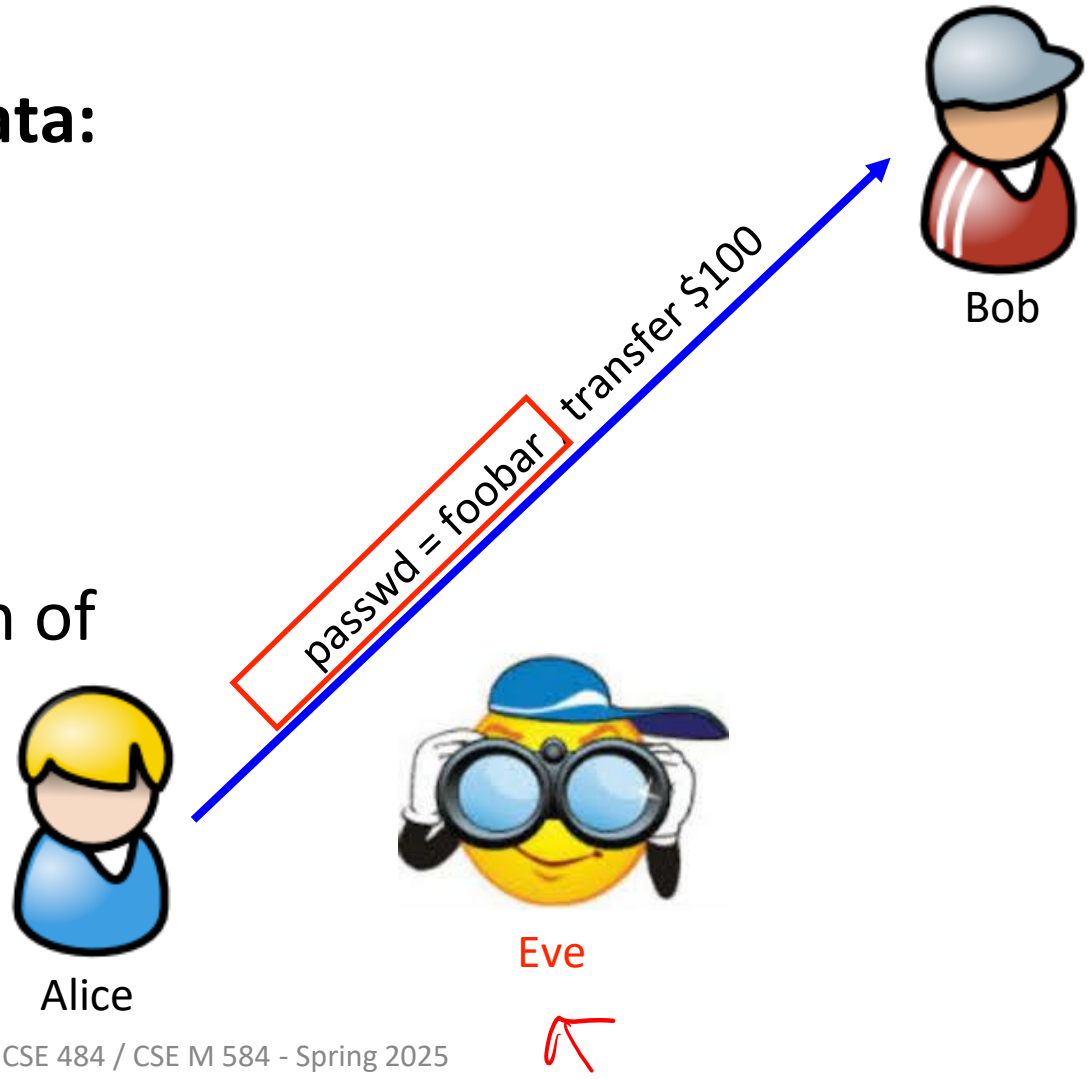
Common Communication Security Goals

Confidentiality of data:

Prevent exposure of information

Integrity of data:

Prevent modification of information



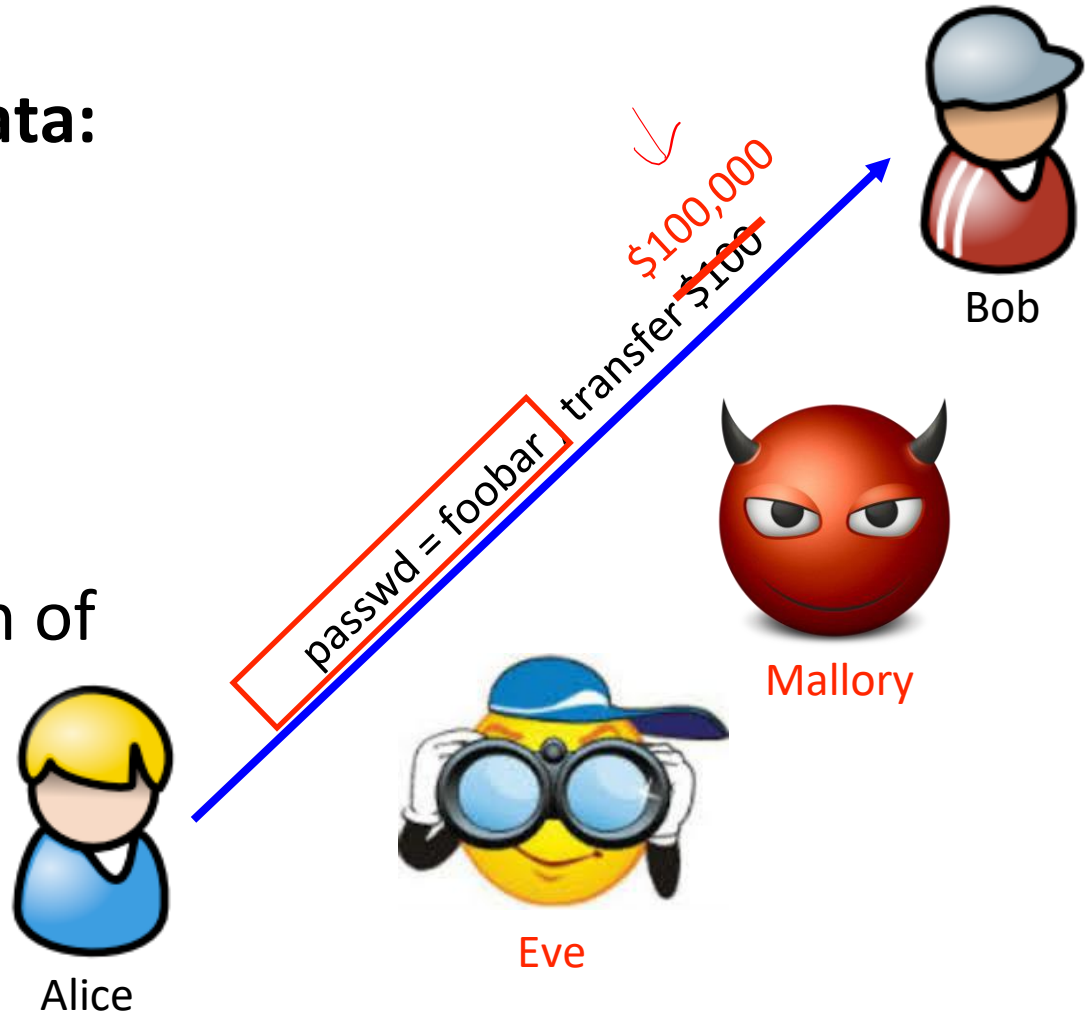
Common Communication Security Goals

Confidentiality of data:

Prevent exposure of information

Integrity of data:

Prevent modification of information



Recall Bigger Picture

- Cryptography only one small piece of a larger system
- Must protect entire system
  - Physical security
  - Operating system security
  - Network security
  - Users
  - Cryptography (following slides)
- Recall the weakest link

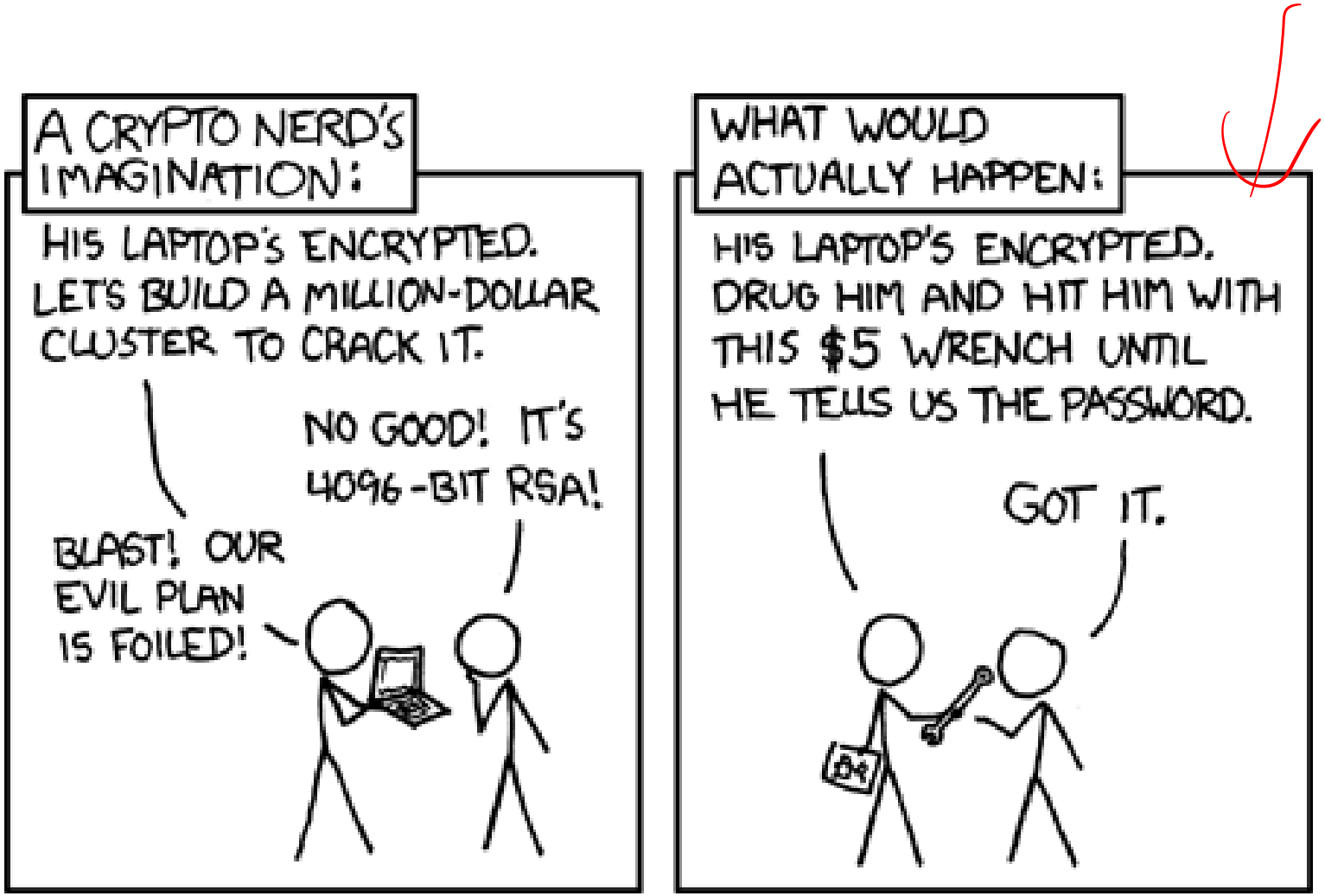
- Still, cryptography is a crucial part of our toolbox

Recall Bigger Picture

- Cryptography only one small piece of a larger system
- Must protect entire system
  - Physical security
  - Operating system security
  - Network security
  - Users
  - Cryptography (following slides)
- Recall the weakest link

- Still, cryptography is a crucial part of our toolbox

XKCD: http://xkcd.com/538/



History

- Substitution Ciphers
  - Caesar Cipher
- Transposition Ciphers
- Codebooks
- Machines

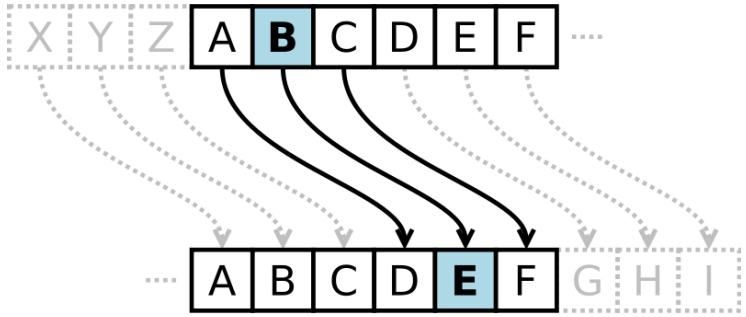
- Recommended Reading: **The Codebreakers** by David Kahn and **The Code Book** by Simon Singh.

History: Caesar Cipher (Shift Cipher)

- Plaintext letters are replaced with letters a fixed shift away in the alphabet.
- Example:
  - Plaintext: `The quick brown fox jumps over the lazy dog`
  - Key: Shift 3

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

  - Ciphertext: `WKHTX LFNEU RZQIR AMXPS VRYHU WKHOD CBGRJ`



History: Caesar Cipher (Shift Cipher)

- What is the key space?
- How to attack shift ciphers?

25

0

History: Caesar Cipher (Shift Cipher)

- What is the key space?
  - 26 possible shifts.
- How to attack shift ciphers?
  - Brute force.

History: Substitution Cipher

- Superset of shift ciphers: each letter is substituted for another one.
- One way to implement: Add a secret key
- Example:
  - Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Cipher: ZEBRASCDFGHIJKLMNOPQTUVWXY
- "State of the art" for thousands of years

26!

A B C
26 25 24 . . .

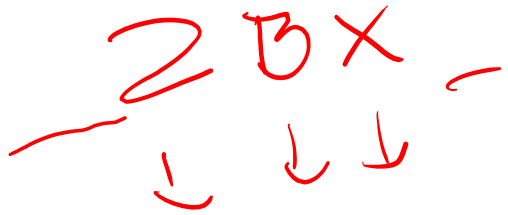
History: Substitution Cipher

- What is the key space?
- How to attack?

History: Substitution Cipher

- What is the key space?
- How to attack?

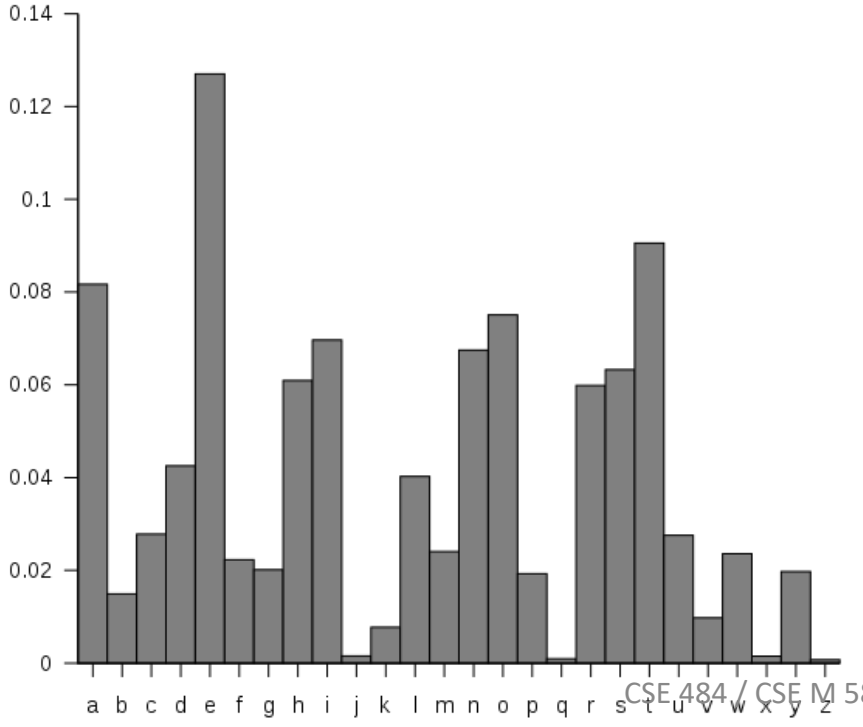
26! ~= 2^88



History: Substitution Cipher

- What is the key space?
- How to attack?
  - Frequency analysis.

26! ~= 2^88



Bigrams:

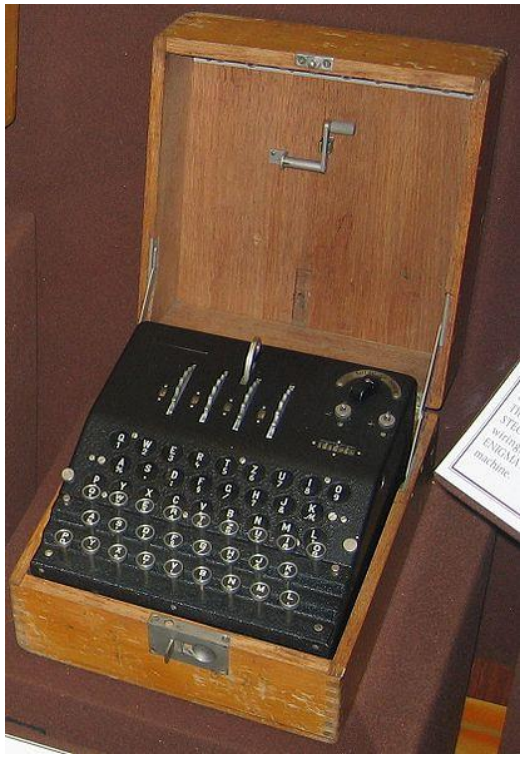
th 1.52%	en 0.55%	ng 0.18%
he 1.28%	ed 0.53%	of 0.16%
in 0.94%	to 0.52%	al 0.09%
er 0.94%	it 0.50%	de 0.09%
an 0.82%	ou 0.50%	se 0.08%
re 0.68%	ea 0.47%	le 0.08%
nd 0.63%	hi 0.46%	sa 0.06%
at 0.59%	is 0.46%	si 0.05%
on 0.57%	or 0.43%	ar 0.04%
nt 0.56%	ti 0.34%	ve 0.04%
ha 0.56%	as 0.33%	ra 0.04%
es 0.56%	te 0.27%	ld 0.02%
st 0.55%	et 0.19%	ur

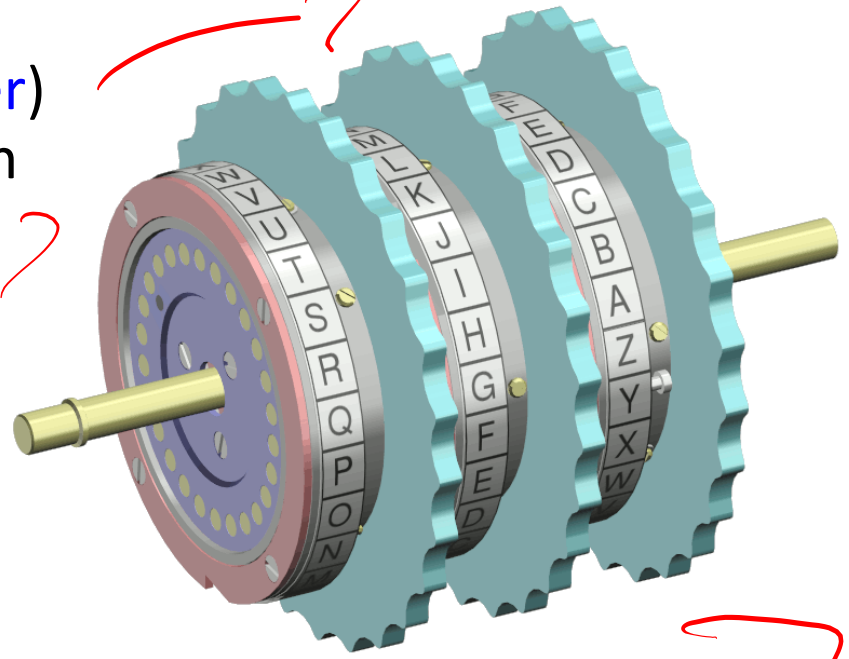
Trigrams:

1. the
2. and
3. tha
4. ent
5. ing
6. ion
7. tio
8. for
9. nde
10. has
11. nce
12. edt
13. tis
14. oft
15. sth

History: Enigma Machine

Uses rotors (substitution cipher) that change position after each key.



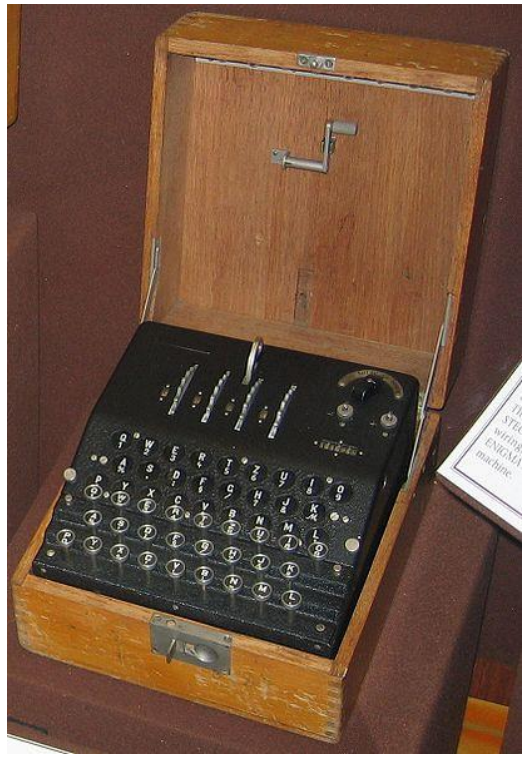


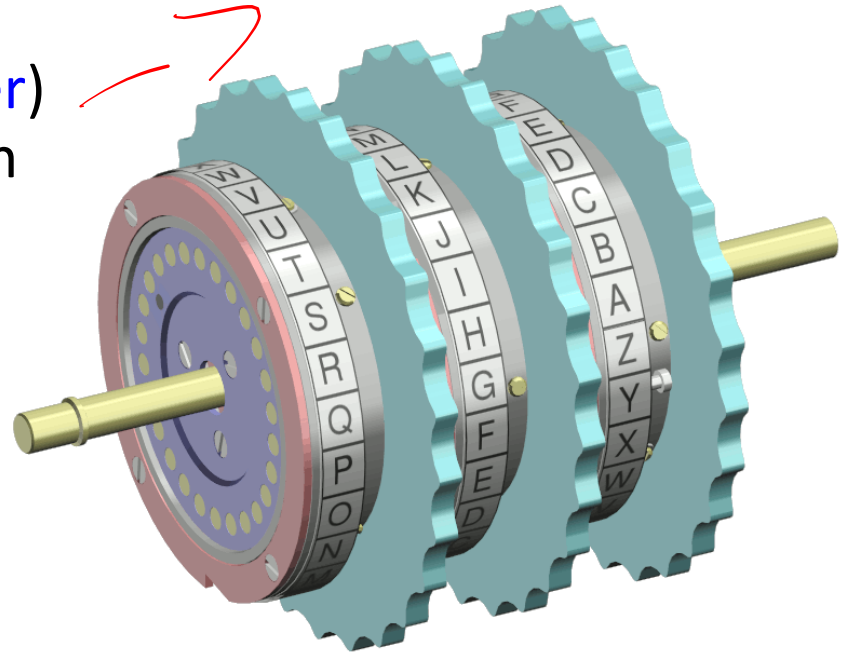
Key = initial setting of rotors

Key space?

History: Enigma Machine

Uses rotors (substitution cipher) that change position after each key.





Key = initial setting of rotors

Key space?

26^n for n rotors

How Cryptosystems Work Today

- **Layered approach:** Cryptographic protocols (like "CBC mode encryption") built on top of cryptographic primitives (like "block ciphers")
- **Flavors of cryptography:**
  - Symmetric (secret key) and asymmetric (public key)
- Public algorithms (Kerckhoff's Principle – next slide)
- Security proofs based on assumptions *(not this course)*
- Be careful about inventing your own!
  (If you just want to use some crypto in your system, use vetted libraries!)

Kerckhoff's Principle

- Security of a cryptographic object should depend only on the secrecy of the secret key.
- Security should not depend on the secrecy of the algorithm itself.

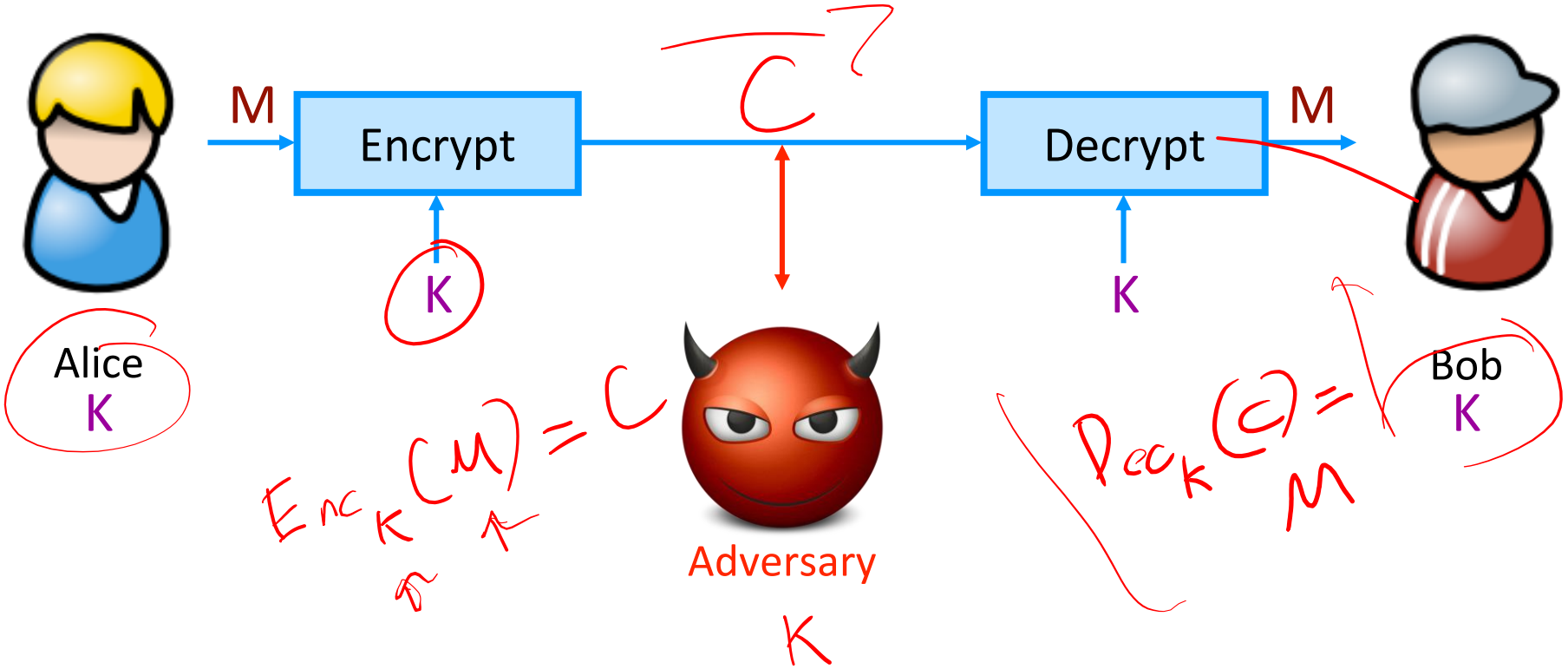
- Foreshadowing: Need for randomness
  - the key is unpredictable and cannot be guessed

Flavors of Cryptography

- Symmetric cryptography
  - Both communicating parties have access to a secret shared random string K, called the key
- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.
  - Communicating parties have access to each other's public key

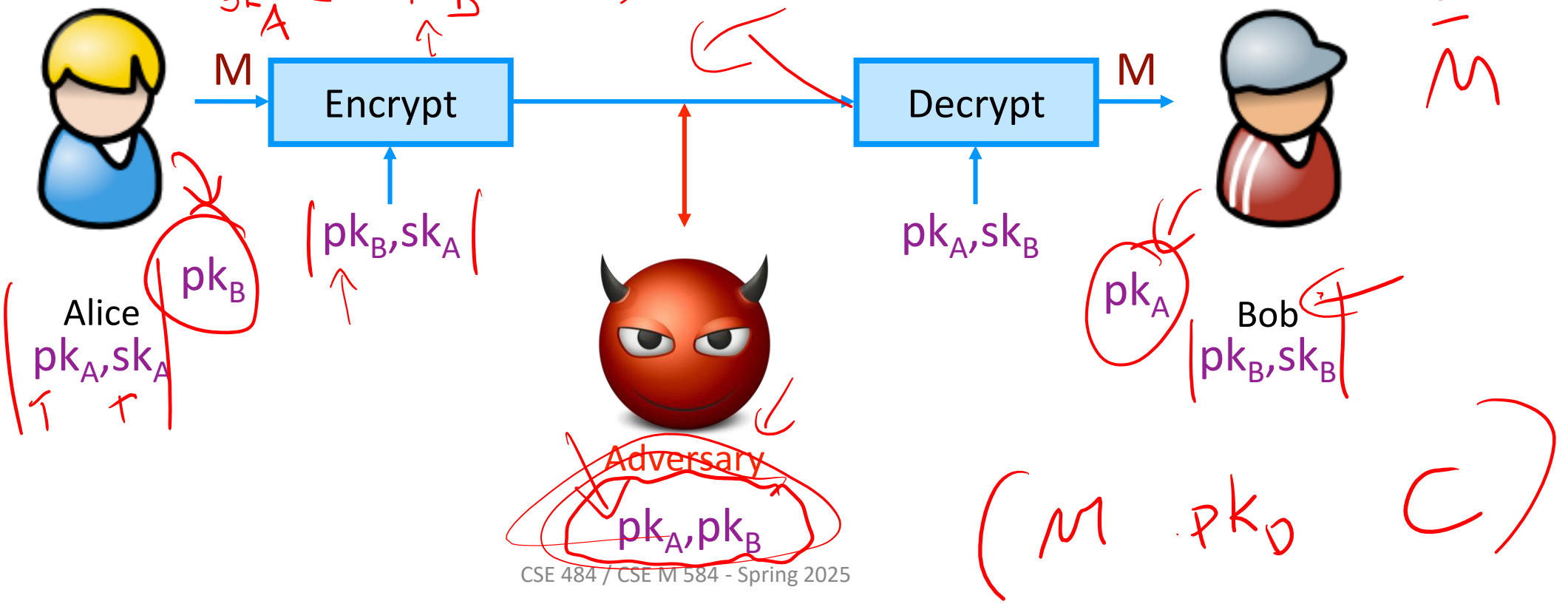
Symmetric Setting

Both communicating parties have access to a secret shared random string K, called the key.



Asymmetric Setting

Each party creates a public key pk and a secret key sk



Bootstrapping Secure Communication

In-class Activity 1/22

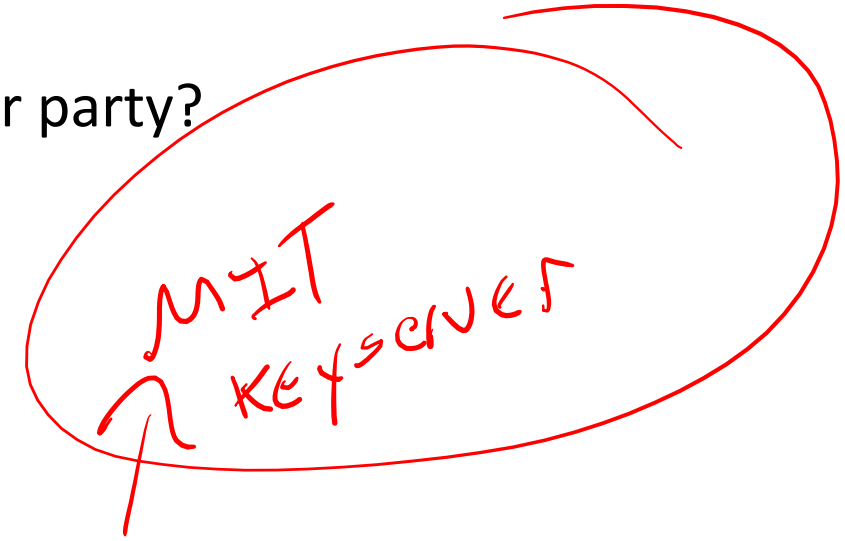
- Symmetric cryptography
  - How do both parties learn the shared secret key?

Bootstrapping Secure Communication

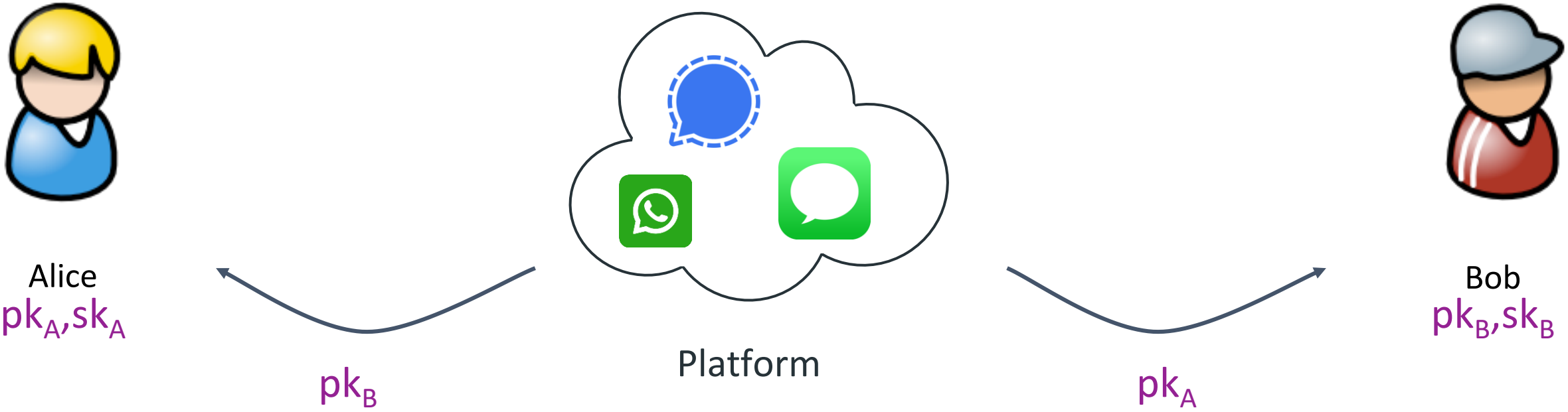
Gradescope!

- Symmetric cryptography
  - How do both parties learn the shared secret key?

- Asymmetric cryptography
  - How does a party learn the public key of the other party?



Preview: Public Key Infrastructure



Preview: Public Key Infrastructure