ENCRYPTION AND PRIVACY

FALL 2021

EMBEDDED ETHICS

KATIE CREEL

WHY ENCRYPTION?

Encryption helps ensure privacy.

So what is the the value of privacy?

HARMS OF PRIVACY VIOLATION … TO THE INDIVIDUAL

- **Harming Relationships —** Privacy enables social relationships, intimacy, and trust.
- **Aggregation** — joining together small pieces of information that together reveal information a user might not want to share.
- **Inhibition —** surveillance can inhibit activity or speech, even without further threats, just because the user or citizen knows the activity will be observed or monitored**.**

Daniel Solove. “I’ve Got Nothing to Hide” and other Misunderstandings of Privacy (2007)

HARMS OF PRIVACY VIOLATION … TO SOCIETY

- **Limiting the Power of Government –** Setting bounds on the sphere of government or
- **Breaking Trust —** Users or citizens may place less trust in governments (or companies) that collect and share their data – and reasonably so! Lack of trust in institutions has many downstream harms.

- **"Privacy should not be understood solely as an individual right…. Instead, privacy protects the individual because of the benefits it confers on society." (Solove, 2008, 98, 171fn.).**

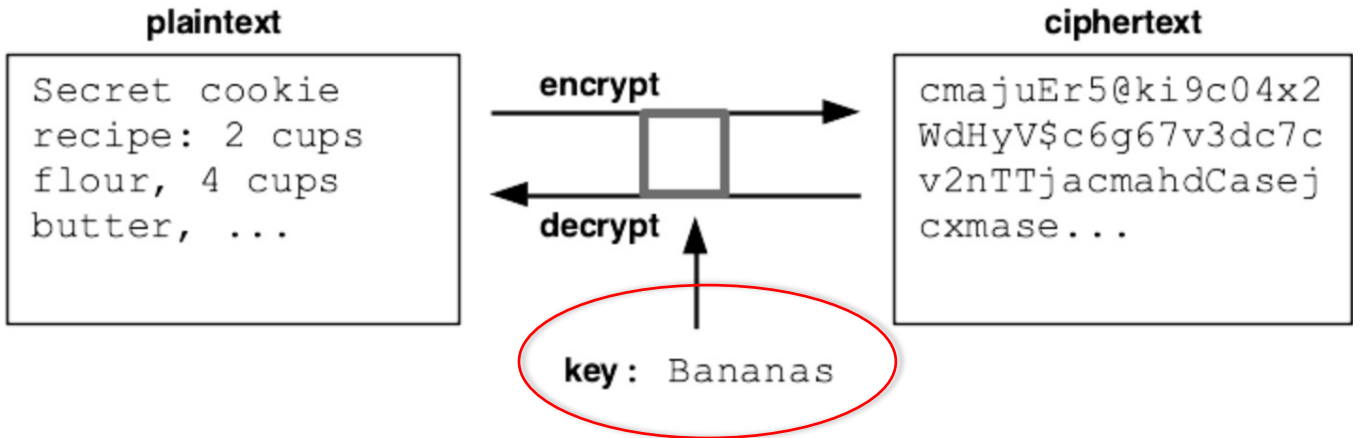
ENCRYPTION

Crypto Introduction

Download the crypto.zip and open the "crypto" folder in PyCharm to get started.

The beginnings of Computer Science are deeply tied up with the famous Alan Turing "Enigma Code" cryptography work in the heat of World War II, so it's neat that we can go a little bit into the area with this project.

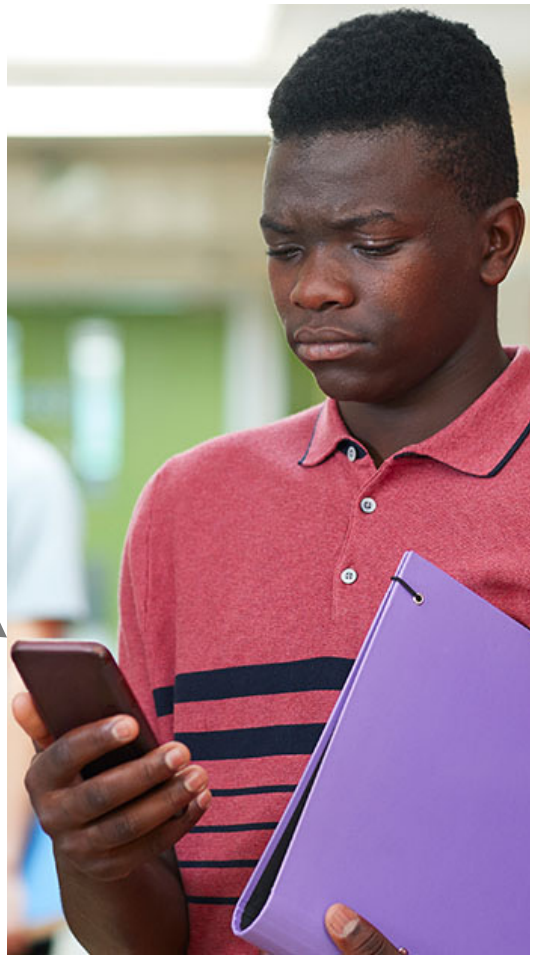
We'll start with a little terminology. In cryptography, we take the original "plaintext", and encrypt it under the control of a key word, yielding an unintelligible "ciphertext". Decryption goes in the opposite direction, using the key to recover the plaintext from the ciphertext. Anyone who intercepts the ciphertext cannot make any sense of it without the key.



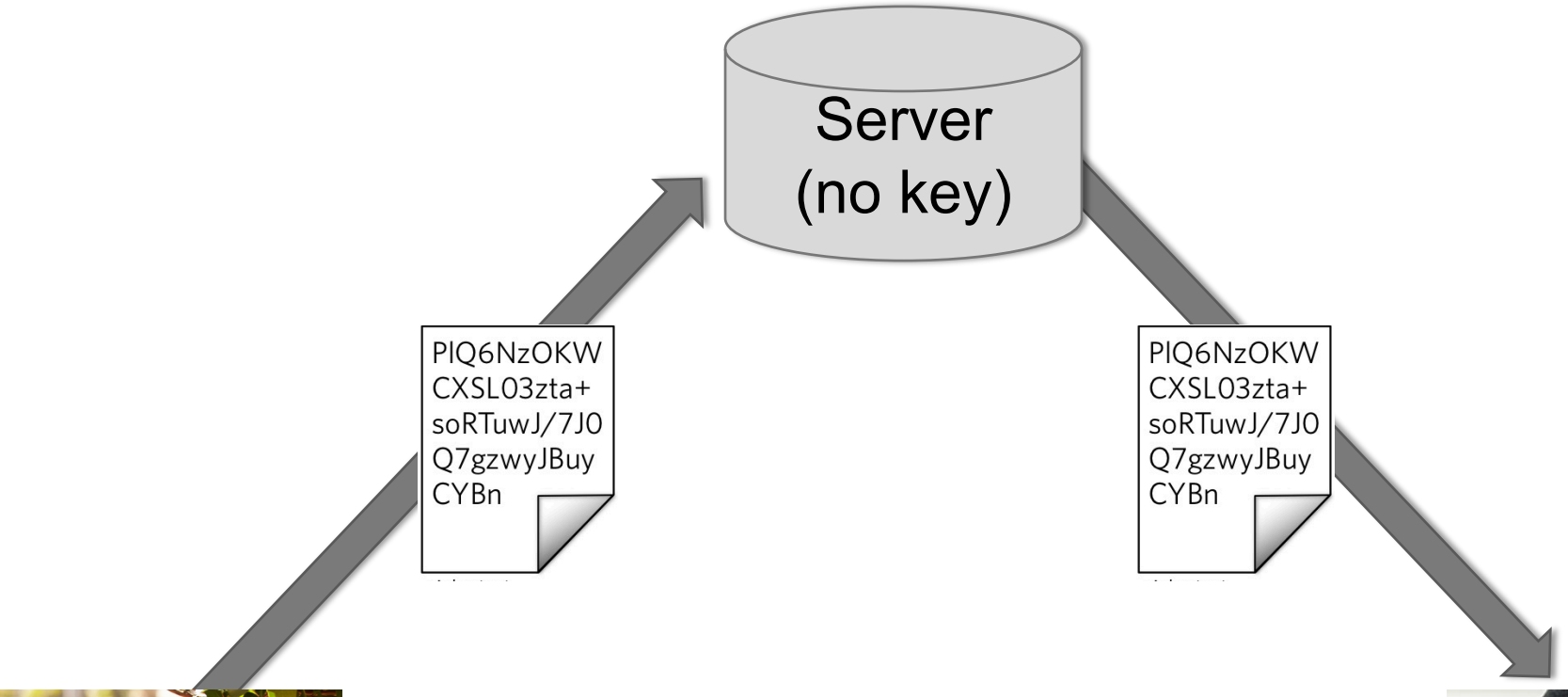
CRYPTOGRAPHY: WHO HAS THE KEY?

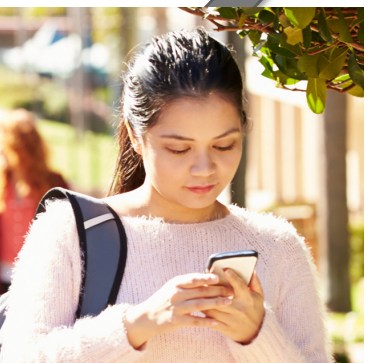
“END TO END” ENCRYPTION

PlQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn



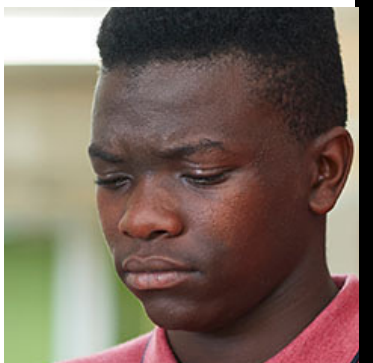
“END TO END” ENCRYPTION





Alice:
Has key

Bob:
Has key



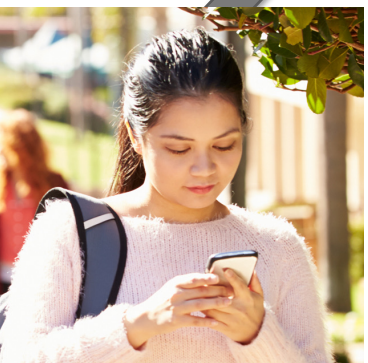
END TO END ENCRYPTION FOR TEXTING

- **Signal –** one of the best
- **iMessage –** messages are end-to-end encrypted but **backups in iCloud are not**
- **WhatsApp –** messages are end-to-end encrypted, but not **backups (on Android)** or metadata, like data about who is texting
- **Telegram –** *can be* end-to-end encrypted, but is **not by default**
- Others ...

PRIVACY AND STORED DATA

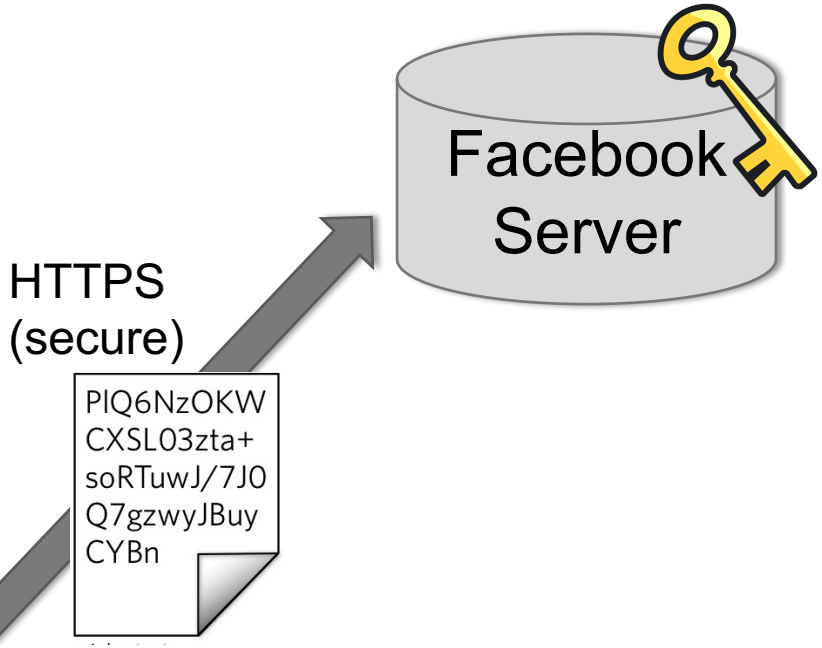
HTTPS
(secure)

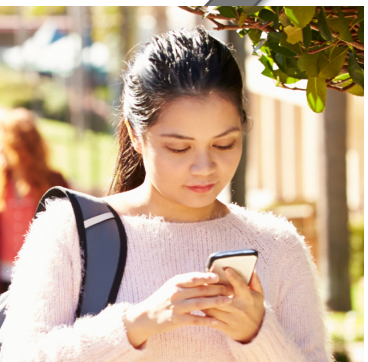
PlQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn



Alice:
Has key

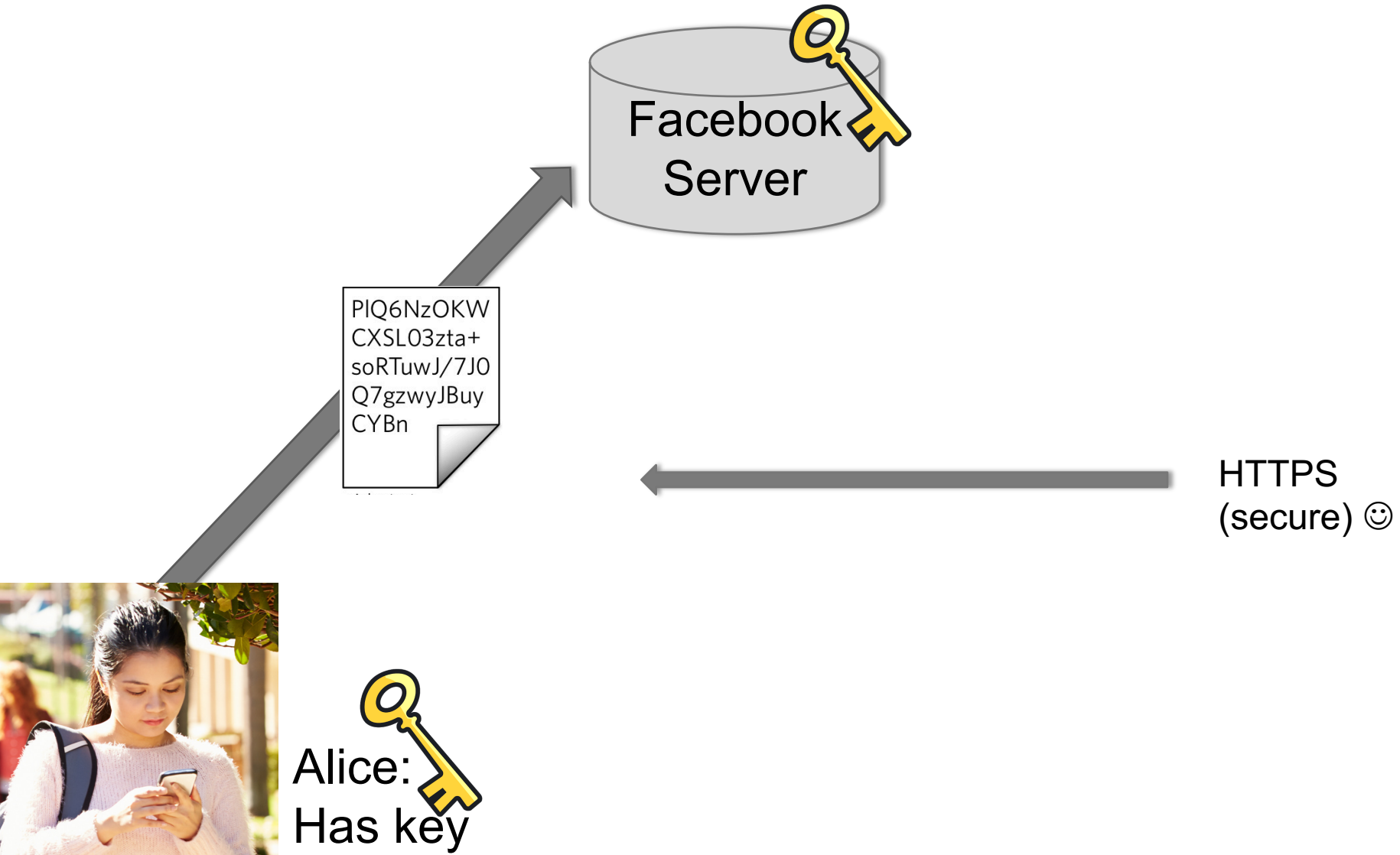
PRIVACY AND STORED DATA



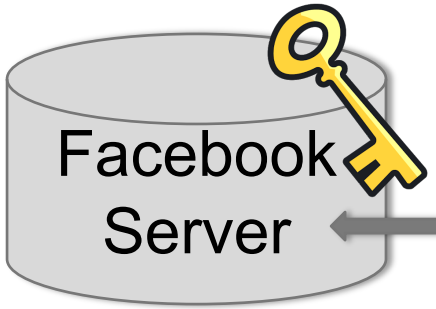


Alice:
Has key

PRIVACY AND STORED DATA

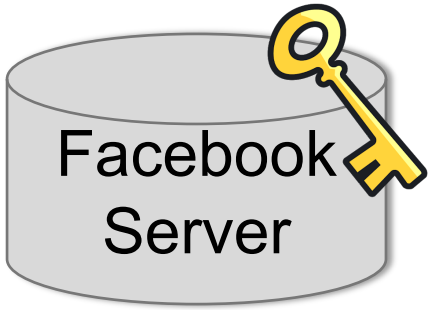


4TH AMENDMENT PROTECTIONS



Only as secure as the database + the willingness to respond to government requests

4TH AMENDMENT PROTECTIONS



4th Amendment:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and **no Warrants shall issue, but upon probable cause**, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

PRIVACY AND STORED DATA

Alice:
Has key

Only as secure as the phone or device itself

5TH AMENDMENT & COMPELLED DECRYPTION

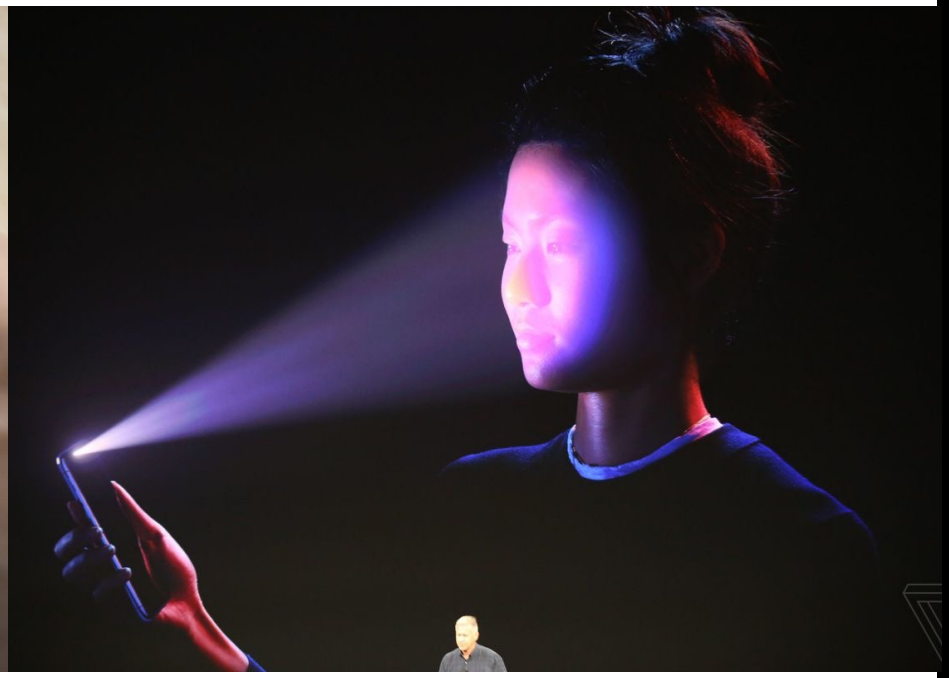
From the 5th Amendment:

"No person … shall be compelled in any criminal case to be a witness against himself …"

Legal Question:

Does being compelled to unlock an encrypted phone fall into the category of being compelled to witness against yourself?

PASSWORDS AND BIOMETRICS (FINGERPRINT/FACE ID) HAVE DIFFERENT STATUS



Legality
of government
compelling
decryption
with a password

Legality
of government
compelling
decryption
with biometric ID

HOW TO PROTECT YOUR OWN PRIVACY WITH ENCRYPTION

- **Use your new understanding of encryption to help yourself and others understand and change user settings**
- **Turn on end-to-end encryption in your messaging app or switch to a service that allows end-to-end encryption**
- **Follow the instructions on this guide to further secure your online life: https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy**
- **Advocate for privacy-preserving laws and policies**

THANK YOU!

KATIE CREEL

KCREEL@STANFORD.EDU

CALENDLY.COM/KATHLEENCREEL