Information Assurance

CSE 365

Dr. Jedidiah Crandall

ASU Biodesign Institute
Arizona State University

About me

- Not Dr. Crandall
- Antonio Espinoza
- Filling in today
- Dr. Crandall will be going over the syllabus on Tuesday
- Post Doctoral researcher at Bio-Design
- Former graduate student of Dr. Crandall

ASU Biodesign Institute
Arizona State University

Today

- Brief cryptography preview.
- Cover the analysis of end-to-end encryption in the LINE messaging application.

Section 1

Cryptography preview

Cryptography

You will be exploring cryptography in more detail early this semester.

Cryptography

You will be exploring cryptography in more detail early this semester.

- Derived from Greek, meaning “secret writing”.
- Art/science of concealing the meaning behind messages with codes(*encryption*).
- Cryptanalysis is the breaking of such codes.

Encryption

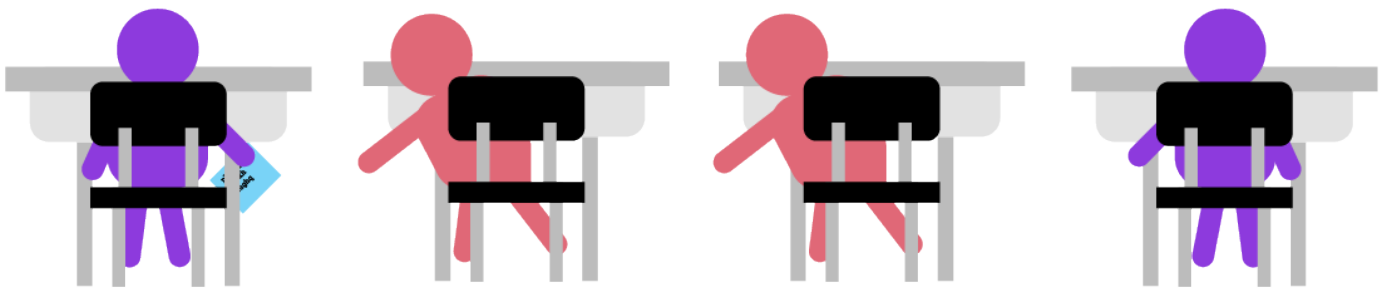
- Symmetric
  - Both parties have the same key
  - ***AES***[1], DES, Blowfish...
- Asymmetric
  - Both parties have different keys
  - Public and pivate keys for each participant.
  - ***Diffie-Hellman***, RSA...

[1] Military grade encryption usually refers to AES.

MAC

- Method Authentication Codes.
  - Not to be confused with Media Access Control from networking (ac:9c:bf:28:d7:b9)
- Makes sure the message has not been altered (integrity).

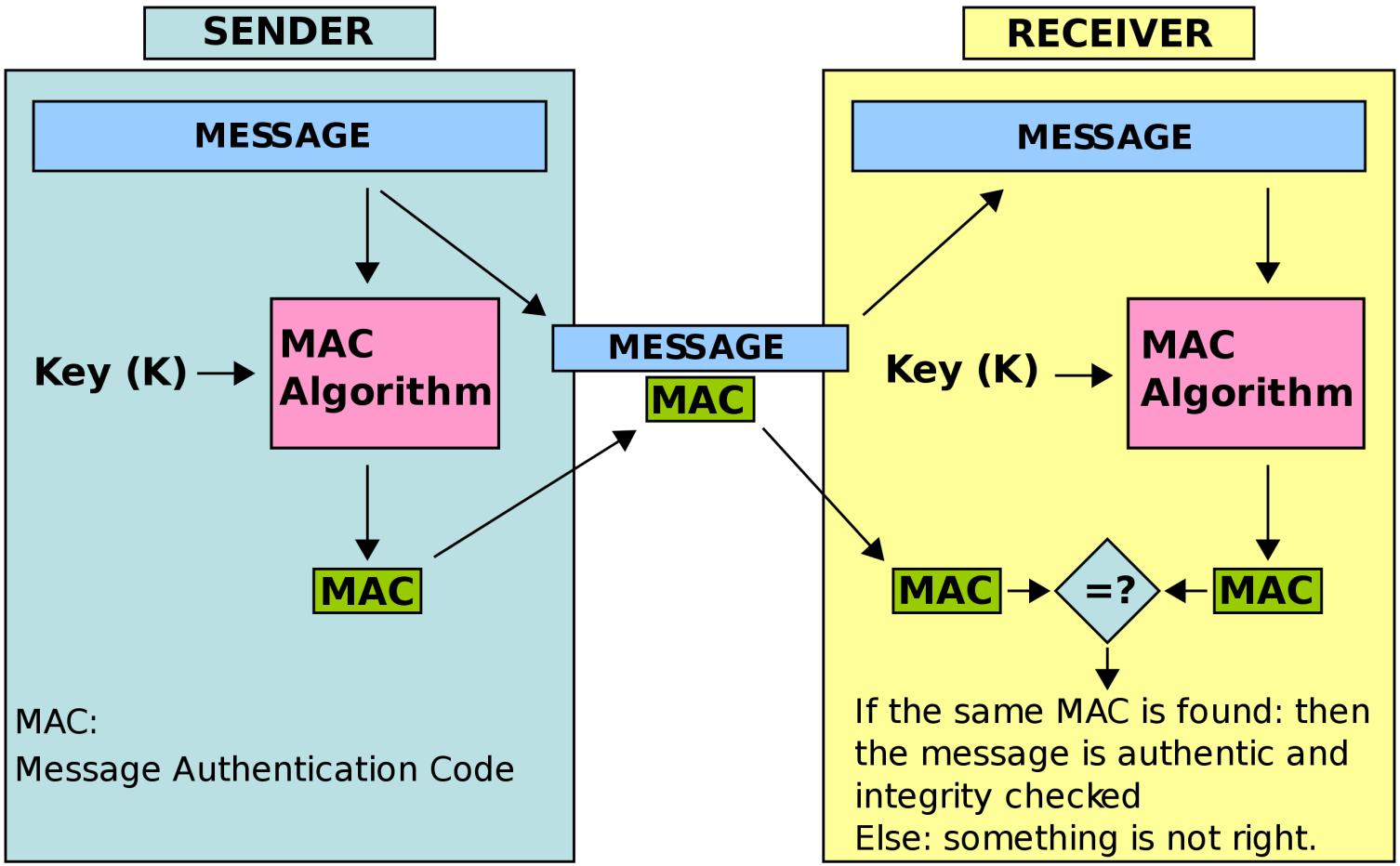
MAC [2]



Biodesign Institute
Arizona State University

[2]Image from: https://ssd.eff.org/

MAC [3]



ASU Biodesign Institute
Arizona State University

[3] Image from: https://en.wikipedia.org/wiki/Message_authentication_code

End-to-end encryption

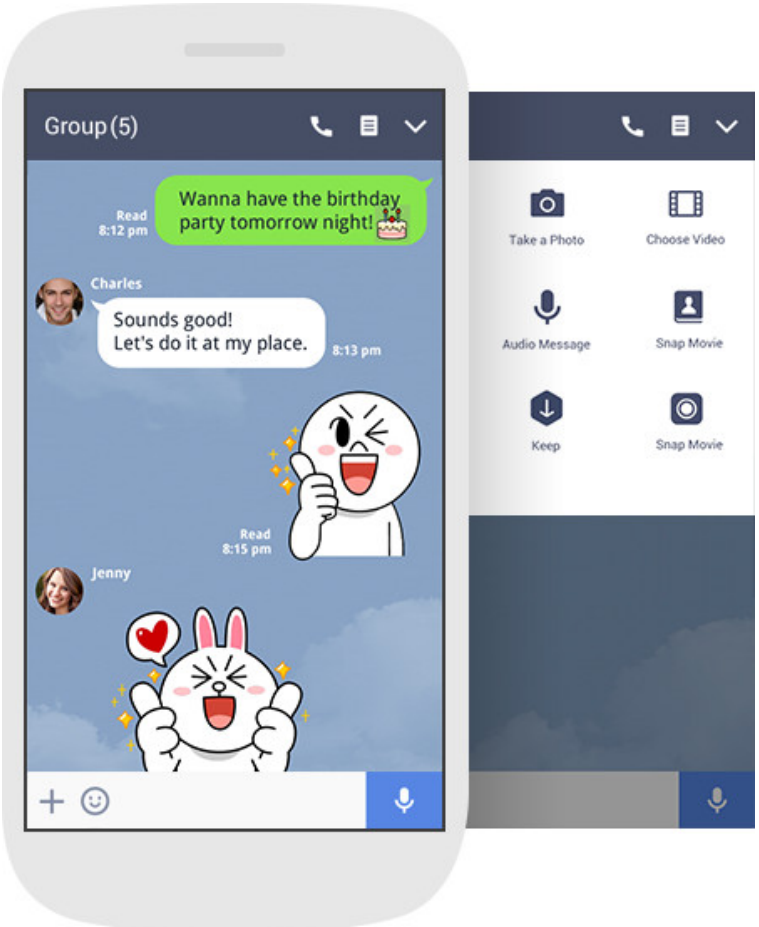
- System where only the parties communicating can decrypt messages.
- Examples?
  - Signal, telegram, wire, WhatsApp, Viber...
- Why E2EE?
- Uses?

Section 2

Analysis of end-to-end encryption in the LINE messaging application

LINE messaging application

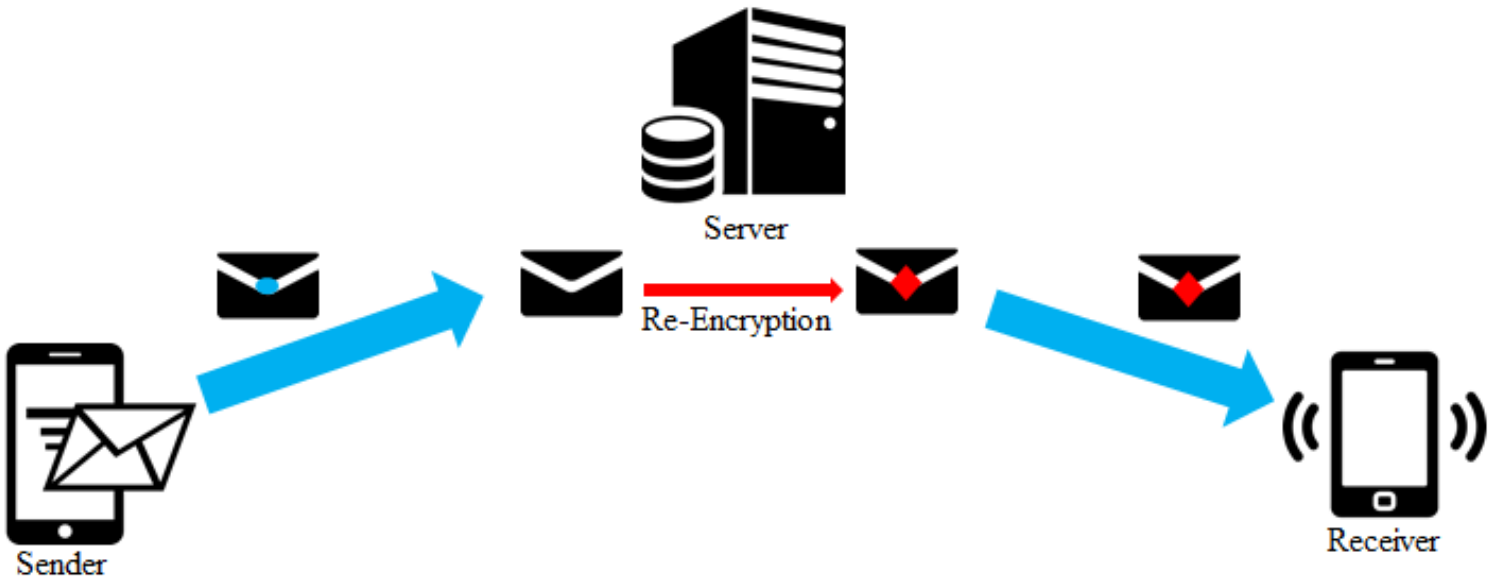
What is LINE? LINE is a Japanese chat application with over 200 million monthly active users.



About LINE

- In 2014 released a "Hidden Chat" feature.
  - "1-to-1 chat"
  - "sent in a secure state"
  - Basically disappearing messages
- In 2015 they released "Letter Sealing".
  - AKA End-to-end Encryption (E2EE)
- In 2016 Letter sealing became the default.
- Everything presented is from 2017 applying to LINE 6.7.1.

LINE pre letter sealing [4]

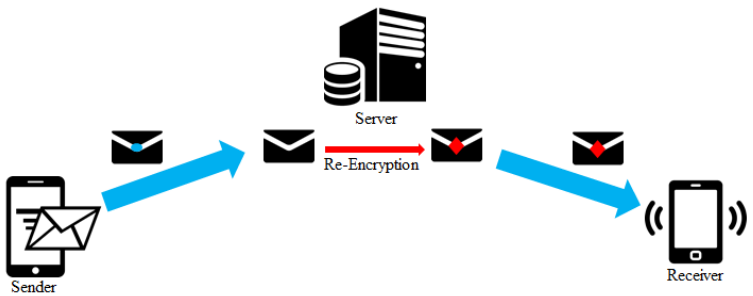


Biodesign Institute
Arizona State University

[4] Line images from https://engineering.linecorp.com/en/blog/detail/65/

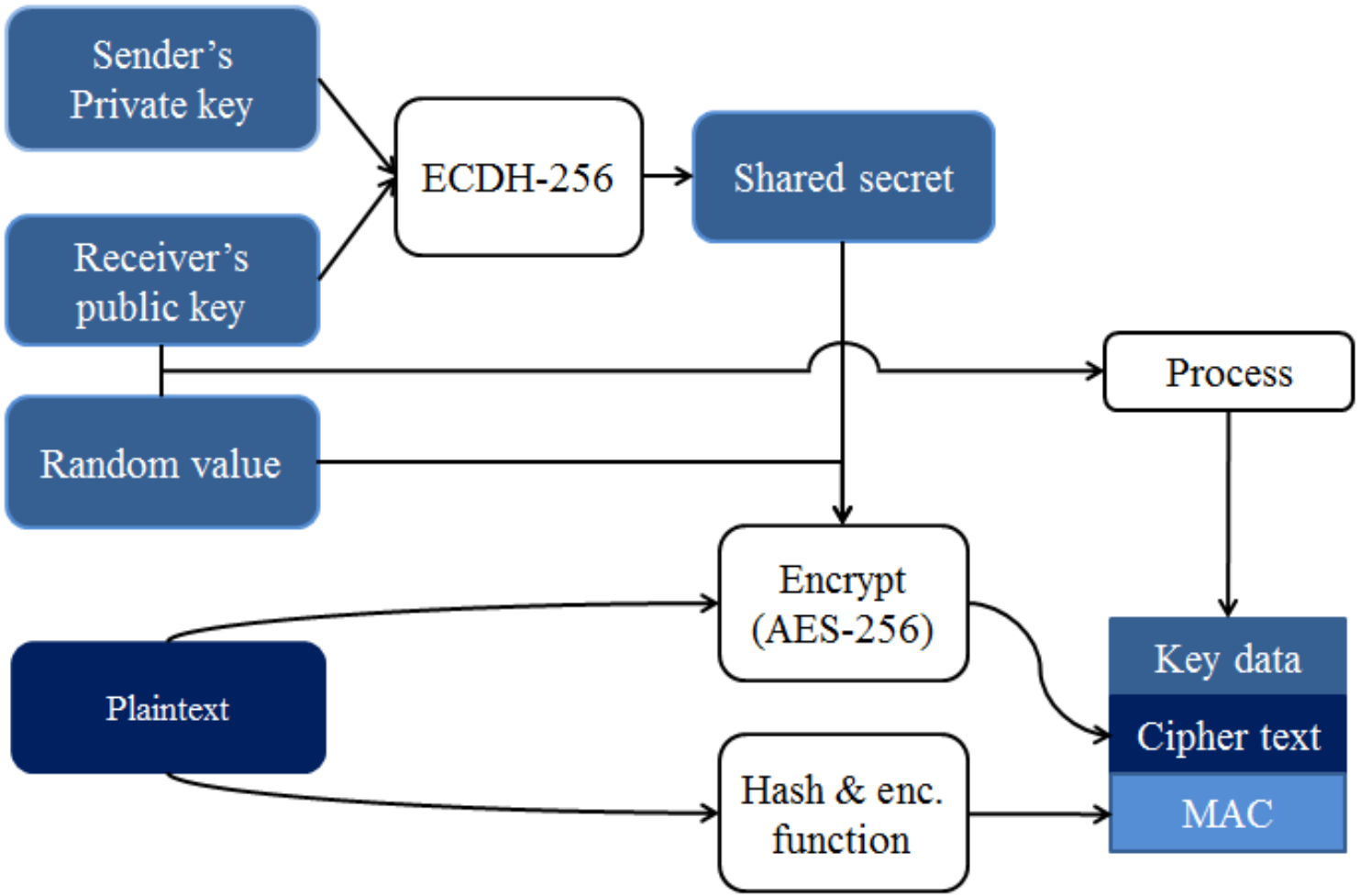
LINE pre letter sealing

- Issues?
- Who can read the decrypted message?
- How would you fix this?



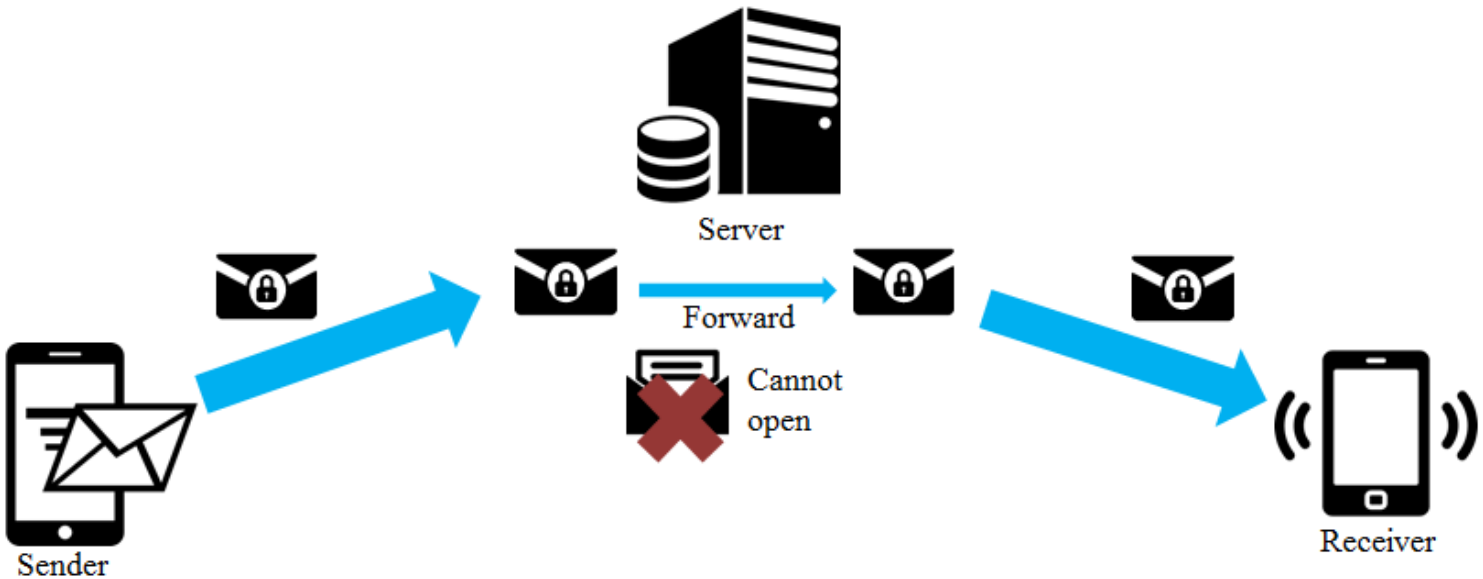
ASU Biodesign Institute
Arizona State University

LINE sealing process



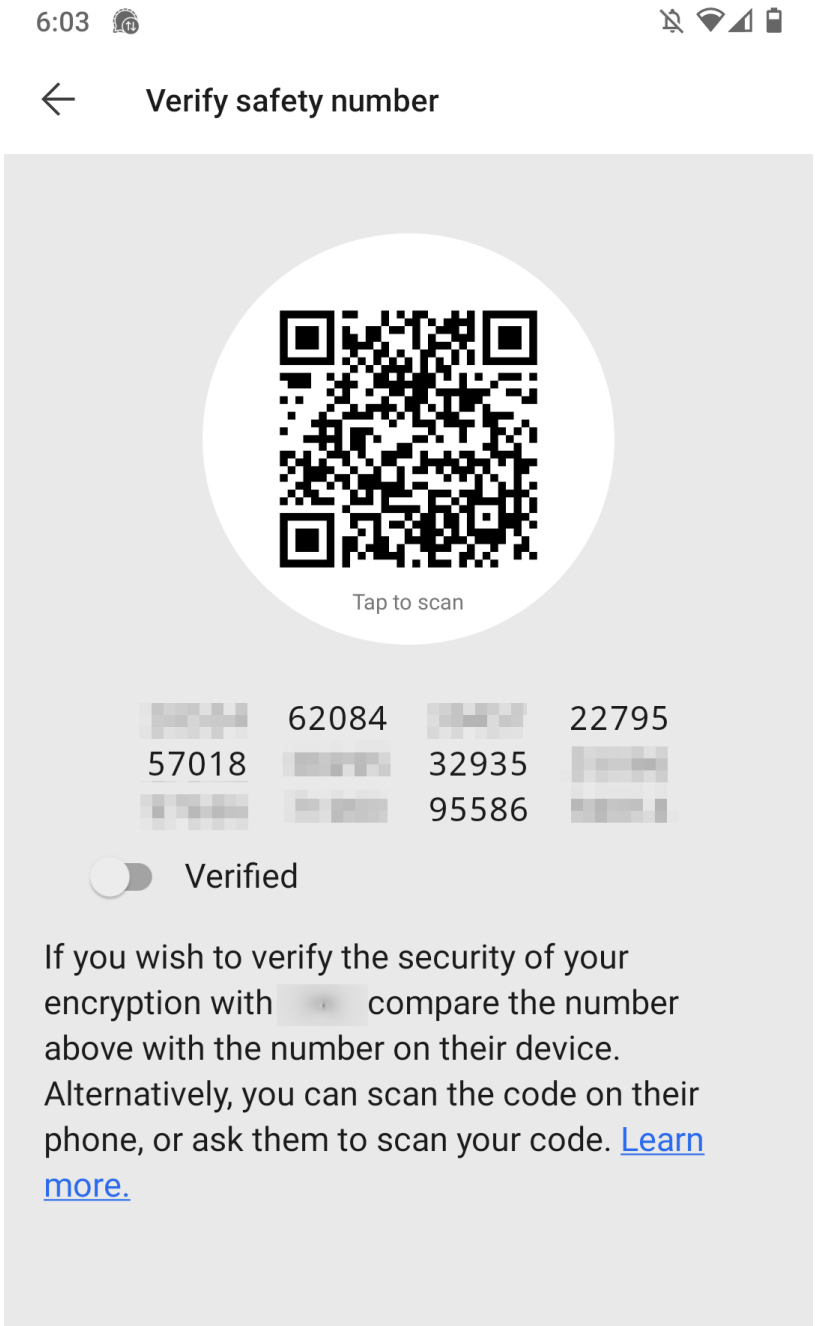
ASU Biodesign Institute
Arizona State University

LINE letter sealing



ASU Biodesign Institute
Arizona State University

LINE letter sealing



ASU Biodesign Institute
Arizona State University

Devil in the details

- Don't need to know the mathematical underpinnings of cryptography to exploit its incorrect use.
- Do have to know how to correctly select values and the implications behind design decisions.
- For example:
  - It's not enough to use a password, you have to use a good password, not "abc123" .
- The following issues were found while reverse engineering the LINE app[5]

[5] I was reading **Cryptography Engineering** at the time.

Line issues

- Lack of end-to-end forward secrecy
- Replay attack (possible due to MAC issues)

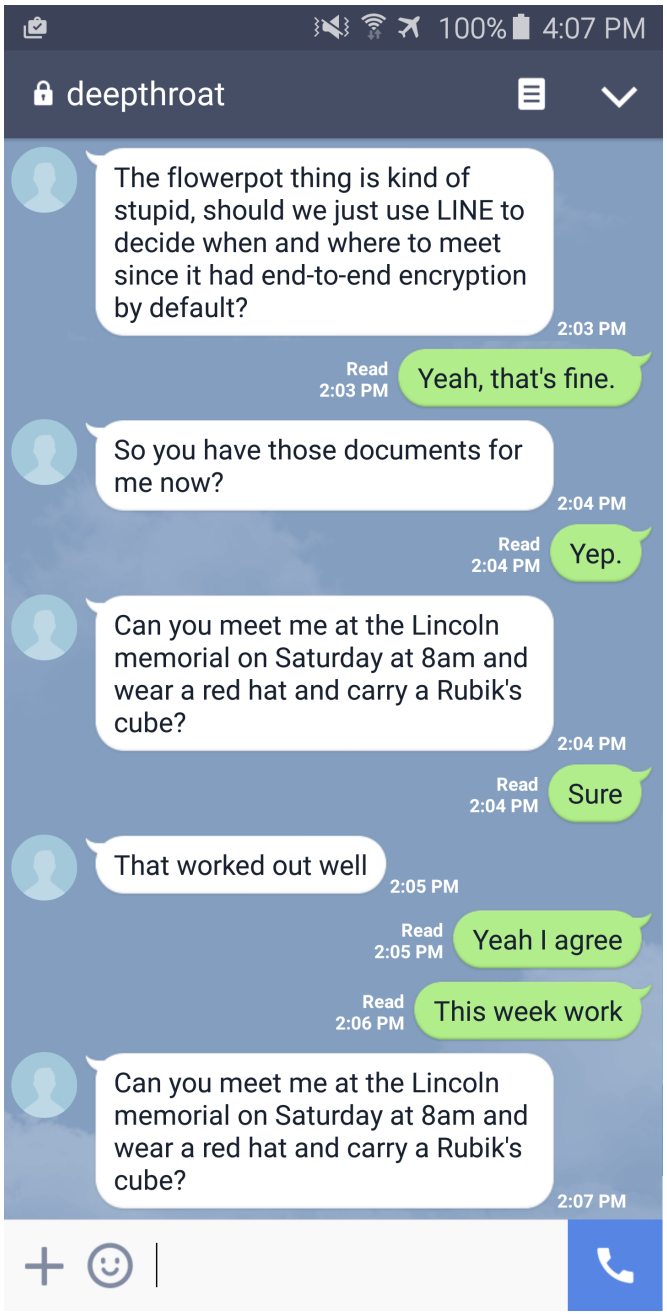
Forward secrecy

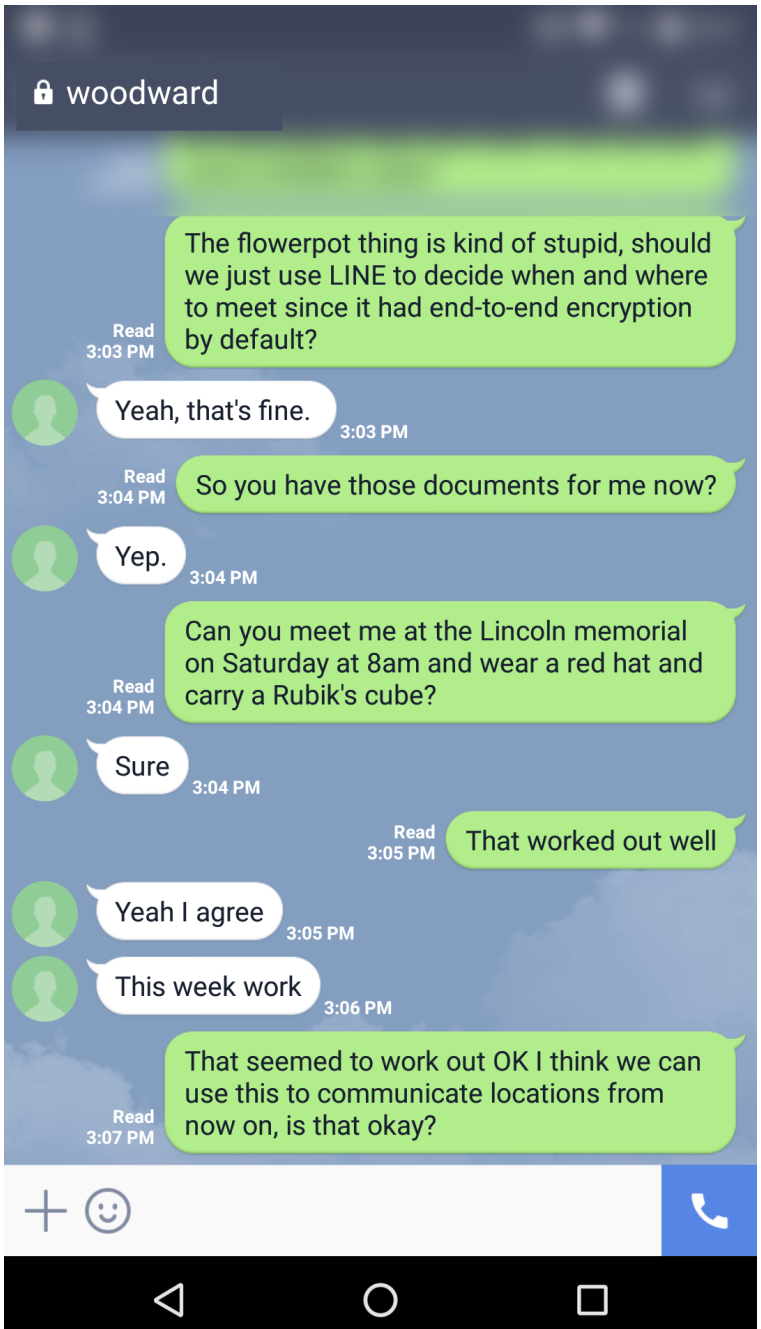
- Forward secrecy is a property of an encryption system that removes an attacker's ability to decrypt past messages even if one or more users' private keys are compromised.
- LINE had forward secrecy from the client to server, but not end-to-end.
- Implications?
  - Adversary can record traffic data and once a key is compromised past conversations can be read.

Replay attack

- A replay attack is an attack where an adversary records messages between two parties and can later replay any of those messages to either party member.
- The attacker does not know the key of either sender or receiver.
- The attacker may not know what the message decrypts to.

Replay attack

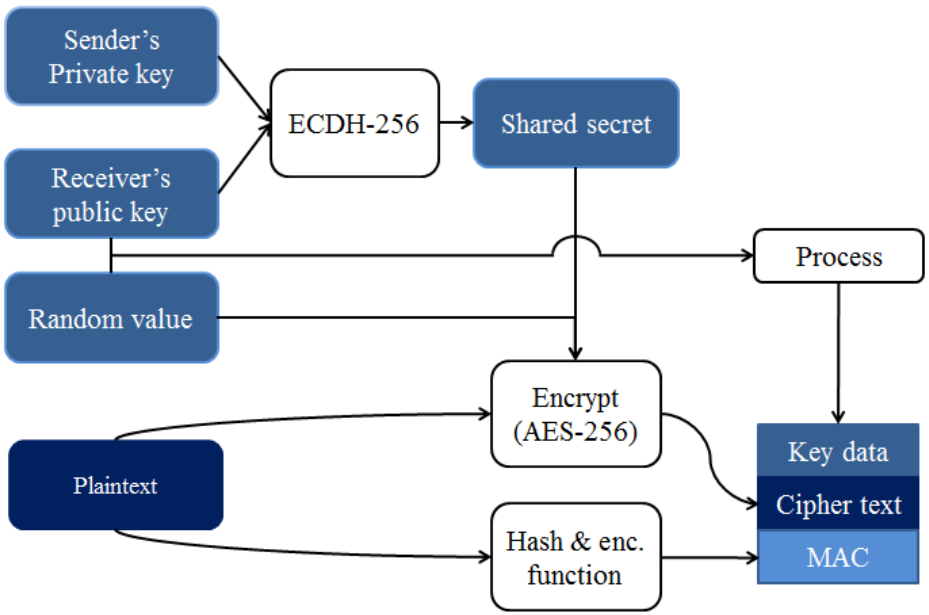




Replay details

Attacker needs 3 things

- Salt “Random value”
- Encrypted message “Cipher text”
- LEGY HMAC function “Hash & enc function”



ASU Biodesign Institute
Arizona State University

Tools

- The tools I used to do reversing of LINE.
- Other helpful tools:
  - wireshark
  - tcpdump
  - python

ASU Biodesign Institute
Arizona State University