Cryptographic Authentication and Encryption for GPS Communications

AA 272 Global Positioning System

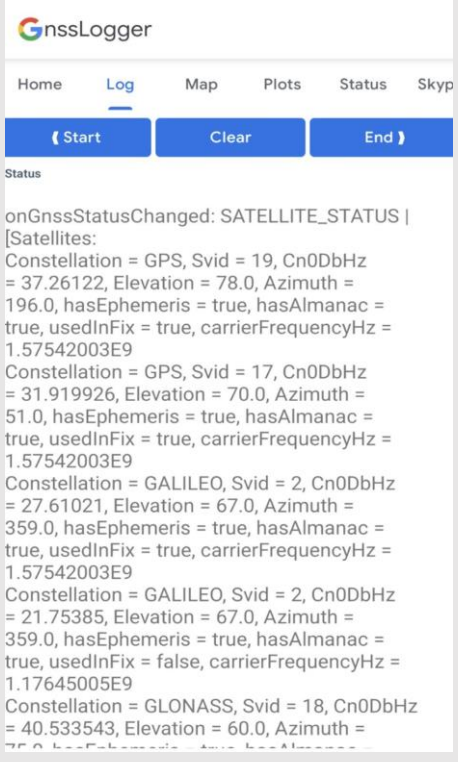
Jiayang Wang
Yonglin He
Yiyang Mu

October 17, 2023

Stanford University

Motivation

- Security concerns associated with GPS communications
- Integrity of location-based services
- Potential threats to data accuracy
- Potential Solution: Encryption and Authentication



GnssLogger, Google Pixel 6

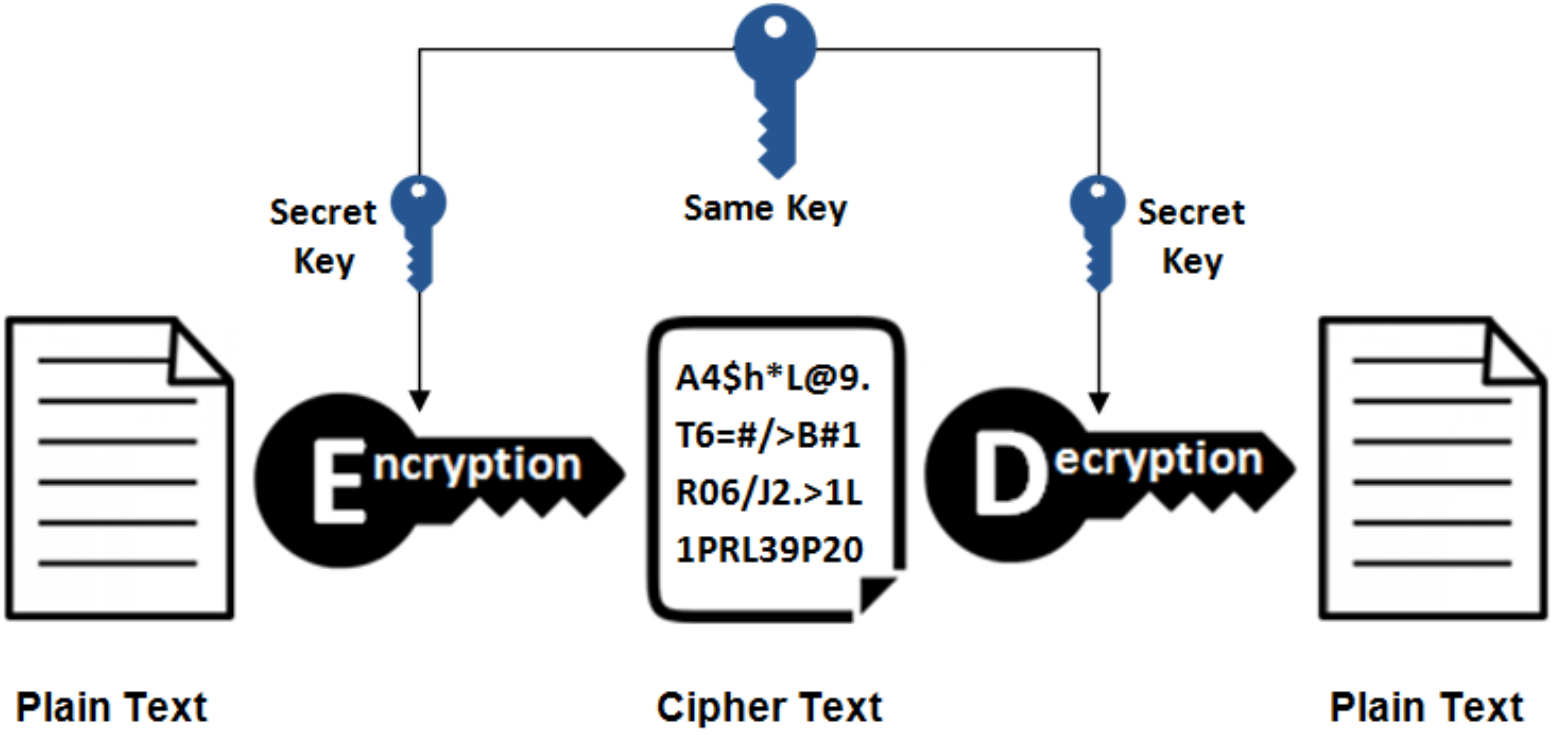
Problem Statement:

- How to securely authenticate received GPS information?
- How to prevent eavesdropping for mission-critical GPS communications?
- How to minimize additional communications with GPS satellites for this purpose?
- How to make the solution scalable for future advancements?

Cryptography - Symmetric Encryption

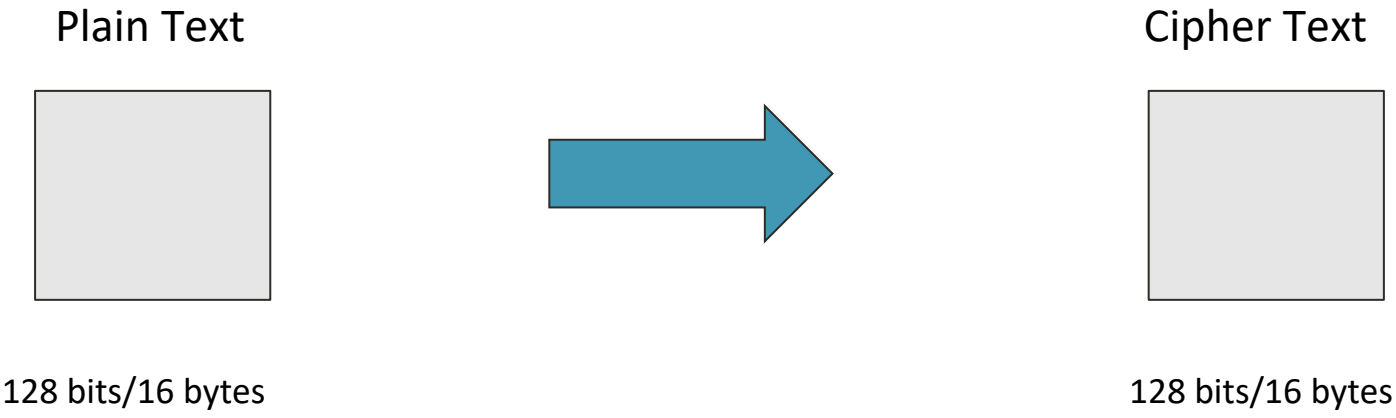
- Shared keys have been obtained by both parties
  - Satellite and Recipient both have a 128-bit cryptographic key (k).
- Use a pair of encryption-decryption algorithm (E,D) to encrypt and decrypt communications
  - m - plain text
  - Satellite sends cipher text c = E(k,m) to recipient, instead of plaintext m.
  - Recipient receives cipher text c, and retrieves plain text m = D(k,c)

Symmetric Encryption



https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Standard Block Cipher - AES128

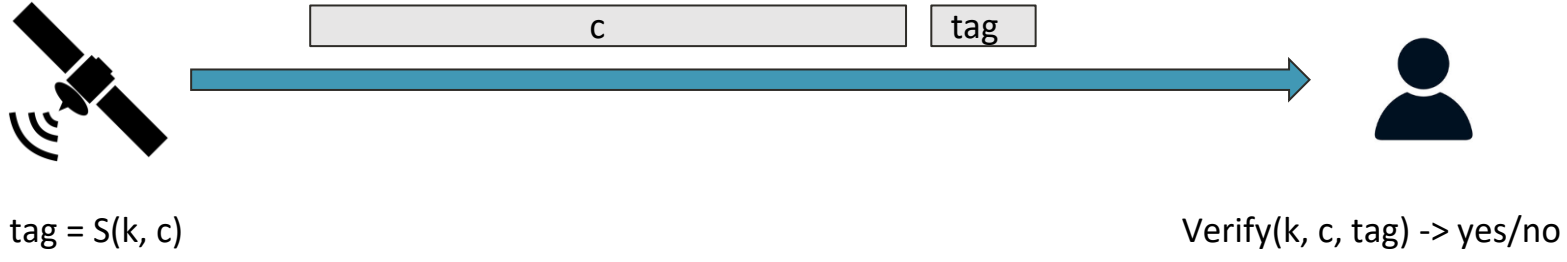


Randomized Counter Mode

IV (Random)	m[0]	m[1]	…	…	m[L]
xor operation	E(k, IV)	E(k, IV+1)	…	…	E(k, IV+L)
IV	c[0]	c[0]	…	…	c[L]

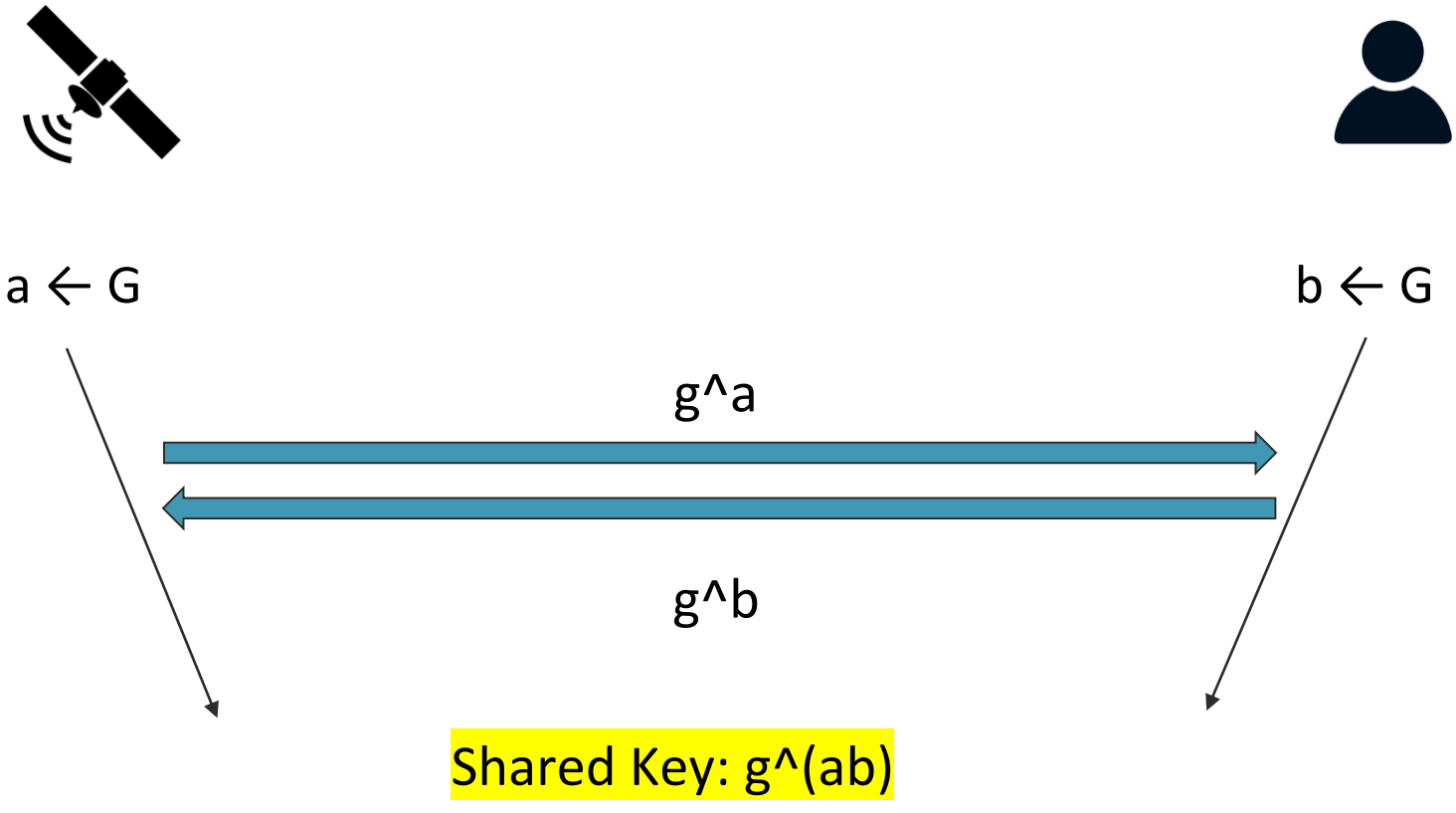
Cryptography - Symmetric Message Authentication

- Used for “Integrity”, not “confidentiality”
  - In GPS applications, this prevents GPS signal spoofing or message alteration.



- CBC-MAC
- HMAC
- …

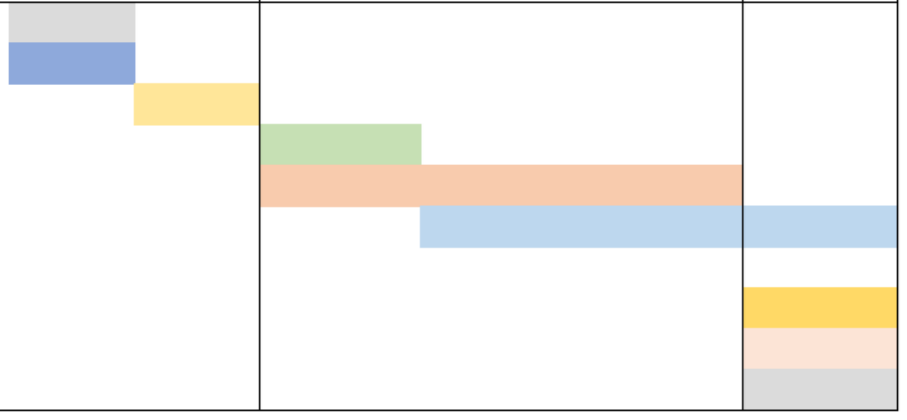
Obtaining Shared Keys: Diffie-Hellman Key Exchange



Improvements

- Digital Signatures
- Signal-Level Encryption/Authentication
- …

Timeline

Deliverables	Start Date	End Date	October	November	December
Project Starts	10/17/2023				
Literature Review	10/17/2023	10/23/2023			
Data Collection	10/23/2023	10/30/2023			
Plain Text Encryption & Decryption	10/30/2023	11/7/2023			
GPS Message Encryption & Decryption	11/5/2023	11/30/2023			
Testing	11/15/2023	12/4/2023			
Improvements if time allowed	TBD	TBD			
Final Project Report	12/1/2023	12/8/2023			
Final Project Presentation	12/5/2023	12/7/2023			
Project ends		12/8/2023			

Thank You