Cryptography For Email

Wilson Li and Minhtri Tran

Data Processing Application

- Email between 2 parties
- Support sending and receiving emails
- Integration with Gmail

Data Eavesdropping

- The email body is in plain text
- Personnels spying on emails
  - Government
  - Companies
  - Malicious attackers
- Forwarded emails can be read by anyone

Confidentiality

- Symmetric encryption
  - Block ciphers
  - Efficient
- AES in CBC mode
  - Randomly generated IV
- 128-bit keys

Key Exchange

- Asymmetric encryption
  - Encrypt shared key using other party’s public key
  - Other party decrypts with their own private key to obtain shared key
- RSA
  - OAEP
  - SHA1 hash
- 2048-bit keys
- All keys are stored locally

Data Modification

- Man in the middle attack
- Attacker modifies email payload contents
- Attack results in miscommunication between the 2 parties

Integrity Detection

- Encrypt then MAC
  - Plaintext integrity
  - Ciphertext integrity
  - Does not leak information about plain text
  - Does not perform decryption if invalid
- HMAC using SHA256
  - Fast

Data Replay

- Attacker sends emails using data from prior emails
- Anyone can send a spoofed email with older payload

Replay Attack Detection

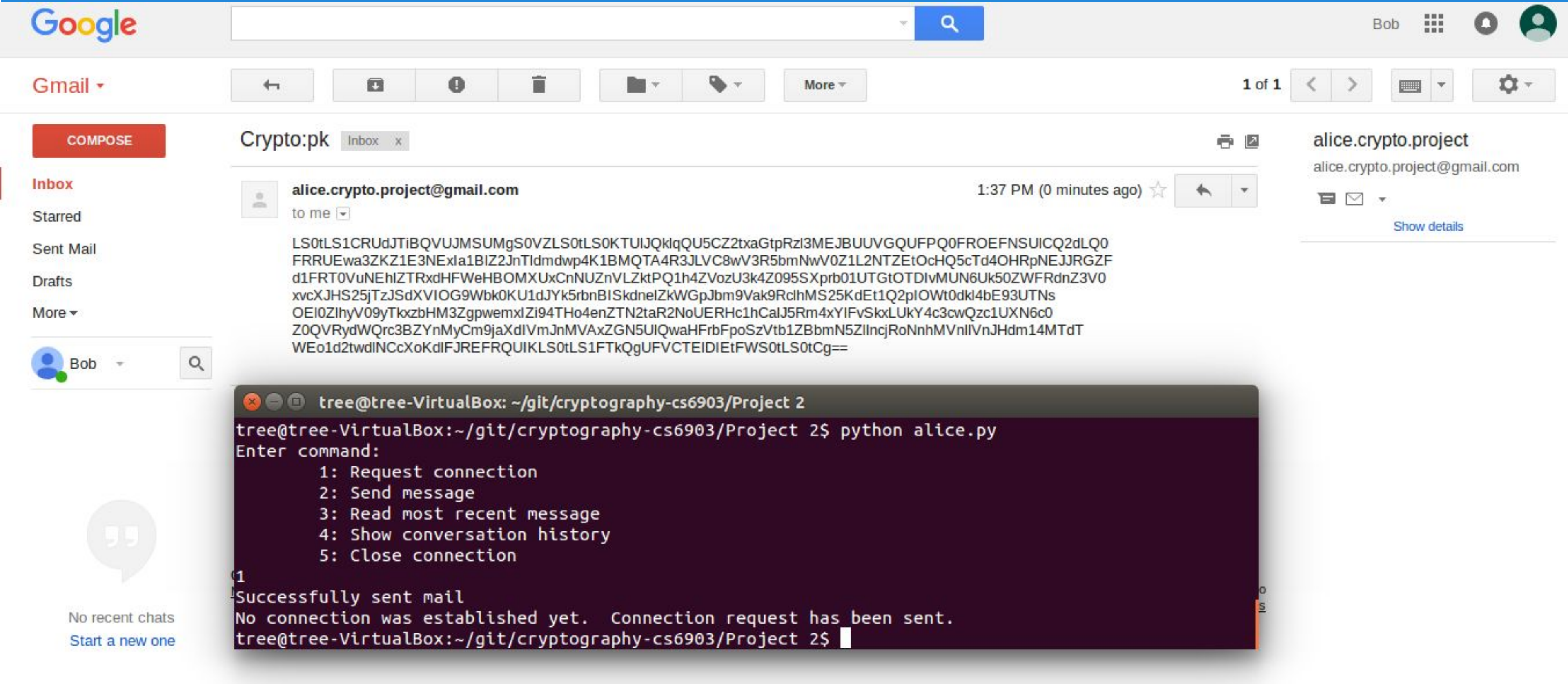
- Sender includes timestamp in payload
- Receiver compares timestamp of payload to date/time the email was sent
- Detect replay attack if difference between timestamp and email date/time too large

Implementation

- Python
- Open source Cryptography library
- Gmail server
- Additional misc. libraries

Demonstration

- Email conversation using our program between Alice and Bob



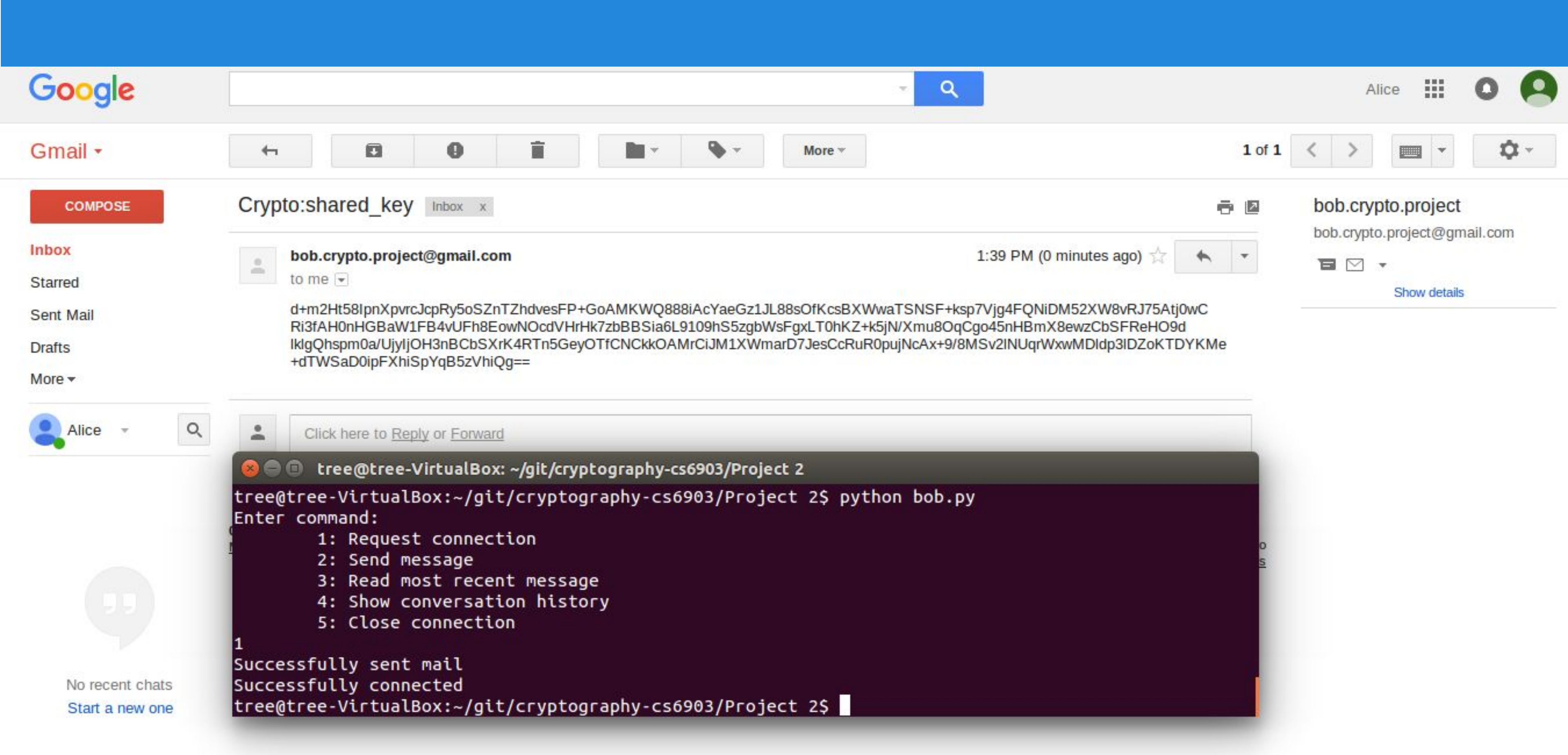
alice.crypto.project@gmail.com
to me

1:37 PM (0 minutes ago)

LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0
FRRUEwa3ZKZ1E3NExla1BIZ2JnTldmdwp4K1BMQTA4R3JLVC8wV3R5bmNwV0Z1L2NTZEtOcHQ5cTd4OHRpNEJJRGZF
d1FRT0VuNEhlZTRxdHFWeHBOMXUxCnNUZnVLZktPQ1h4ZVozU3k4Z095SXprb01UTGtOTDlvMUN6Uk50ZWFRdnZ3V0
xvcXJHS25jTzJSdXVlOG9Wbk0KU1dJYk5rbnBISkdnelZkWGpJbm9Vak9RclhMS25KdEt1Q2plOWt0dkl4bE93UTNs
OEl0ZlhyV09yTkxzbHM3ZgpwemxlZi94THo4enZTN2taR2NoUERHc1hCalJ5Rm4xYlFvSkxLUkY4c3cwQzc1UXN6c0
Z0QVRydWQrc3BZYnMyCm9jaXdlVmJnMVAxZGN5UlQwaHFrbFpoSzVtb1ZBbmN5ZlIncjRoNnhMVnllVnJJHdm14MTdT
WEo1d2twdlNCcXoKdlFJREFRQUIKLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==

```
tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python alice.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
1
Successfully sent mail
No connection was established yet.  Connection request has been sent.
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$
```

Connection step 1: Alice sends Bob her RSA public key



Crypto:shared_key

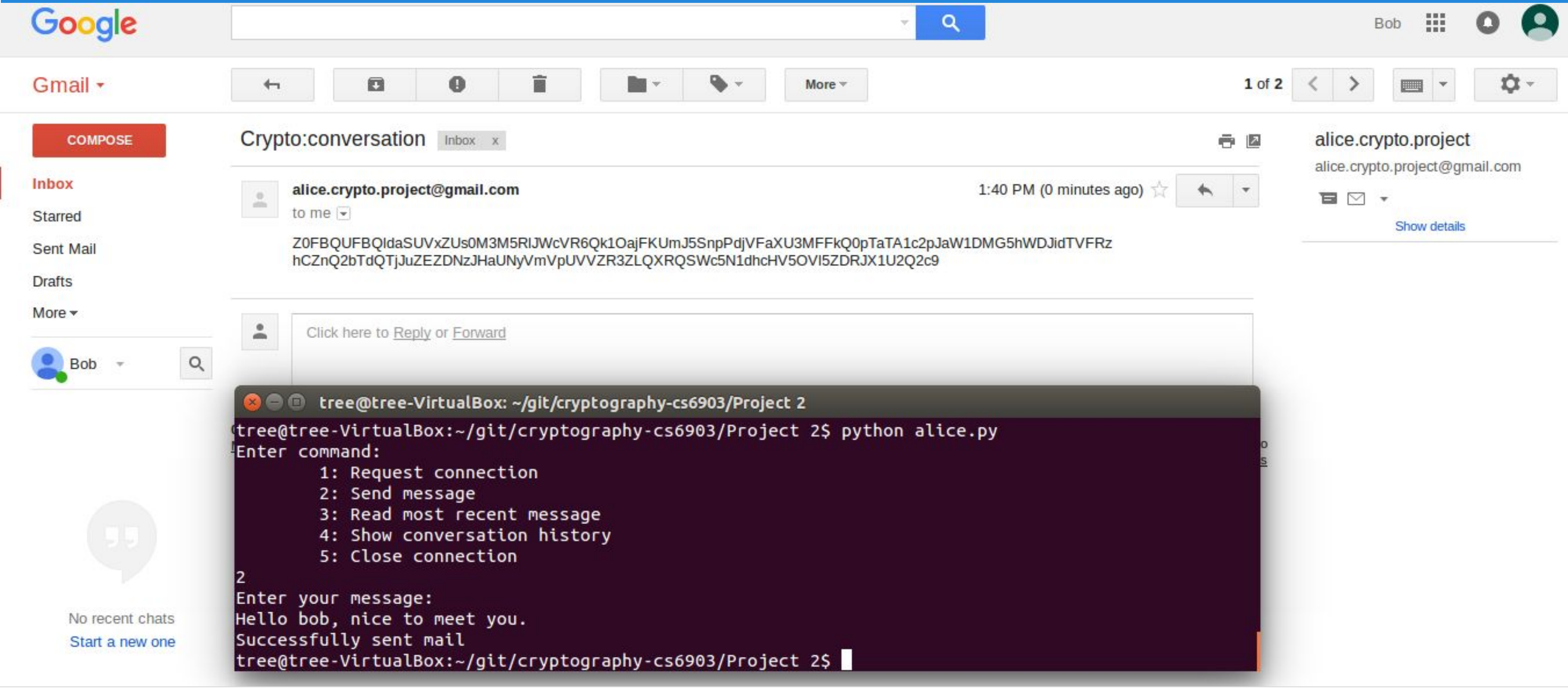
bob.crypto.project@gmail.com
to me
1:39 PM (0 minutes ago)

```
d+m2Ht58IpnXpvrcJcpRy5oSZnTZhdvesFP+GoAMKWQ888iAcYaeGz1JL88sOfKcsBXWwaTSNSF+ksp7Vjg4FQNiDM52XW8vRJ75Atj0wC
Ri3fAH0nHGBaW1FB4vUFh8EowNOcdVHrHk7zbBBSia6L9109hS5zgbWsFgxLT0hKZ+k5jN/Xmu8OqCgo45nHBmX8ewzCbSFReHO9d
IklgQhspm0a/UjyIjOH3nBCbSXrK4RTn5GeyOTfCNCkkOAMrCiJM1XWmarD7JesCcRuR0pujNcAx+9/8MSv2INUqrWxwMDldp3IDZoKTDYKMe
+dTWSaD0ipFXhiSpYqB5zVhiQg==
```

tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2

```
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python bob.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
1
Successfully sent mail
Successfully connected
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$
```

Connection step 2: Bob sends Alice an encrypted shared key



Crypto:conversation Inbox x

alice.crypto.project@gmail.com
to me

1:40 PM (0 minutes ago)

Z0FBQUFBQldaSUVxZUs0M3M5RlJWcVR6Qk1OajFKUmJ5SnpPdjVFaXU3MFFkQ0pTaTA1c2pJaW1DMG5hWDJidTVFRz
hCZnQ2bTdQTjJuZEZDNzJHaUNyVmVpUVVZR3ZLQXRQSWc5N1dhcHV5OVI5ZDRJX1U2Q2c9

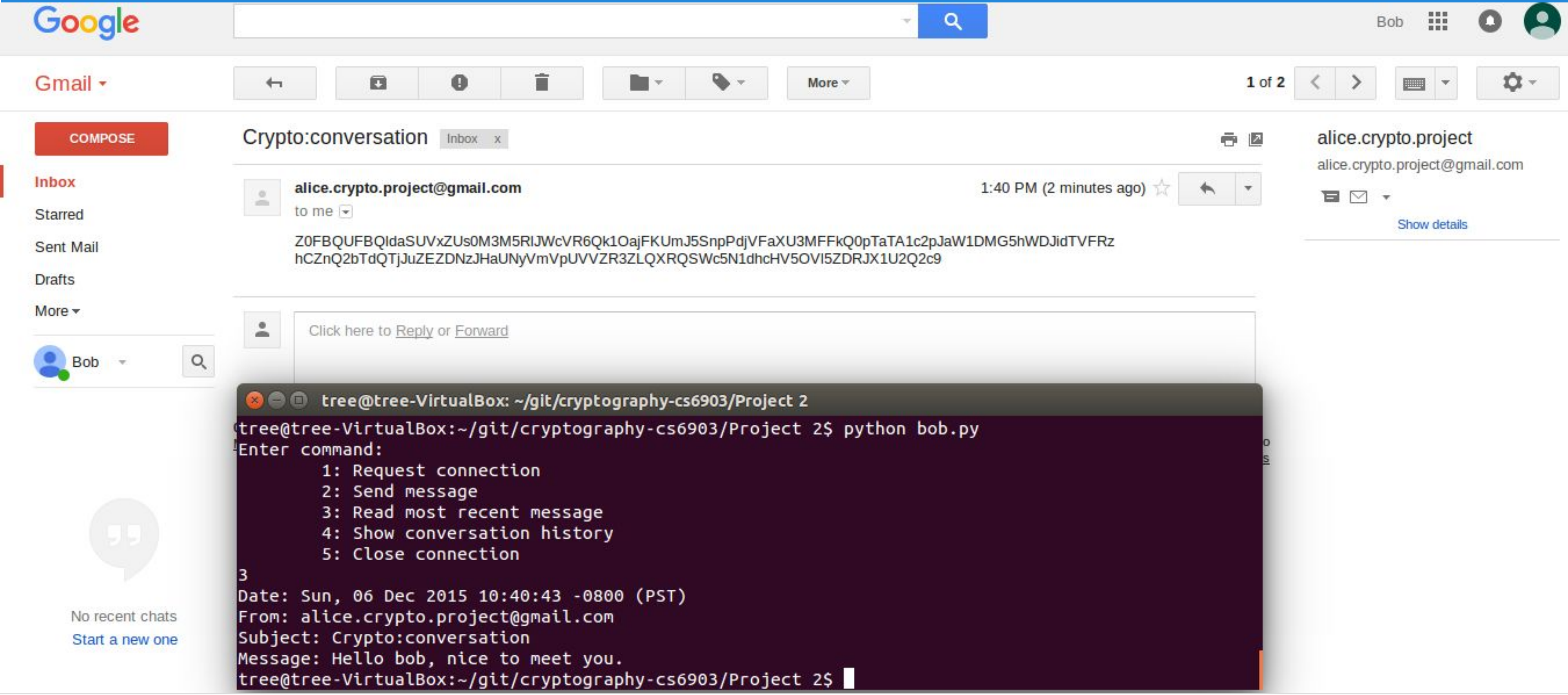
Click here to Reply or Forward

alice.crypto.project
alice.crypto.project@gmail.com

tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2

```
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python alice.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
2
Enter your message:
Hello bob, nice to meet you.
Successfully sent mail
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$
```

Conversation begins: Alice sends Bob an encrypted message



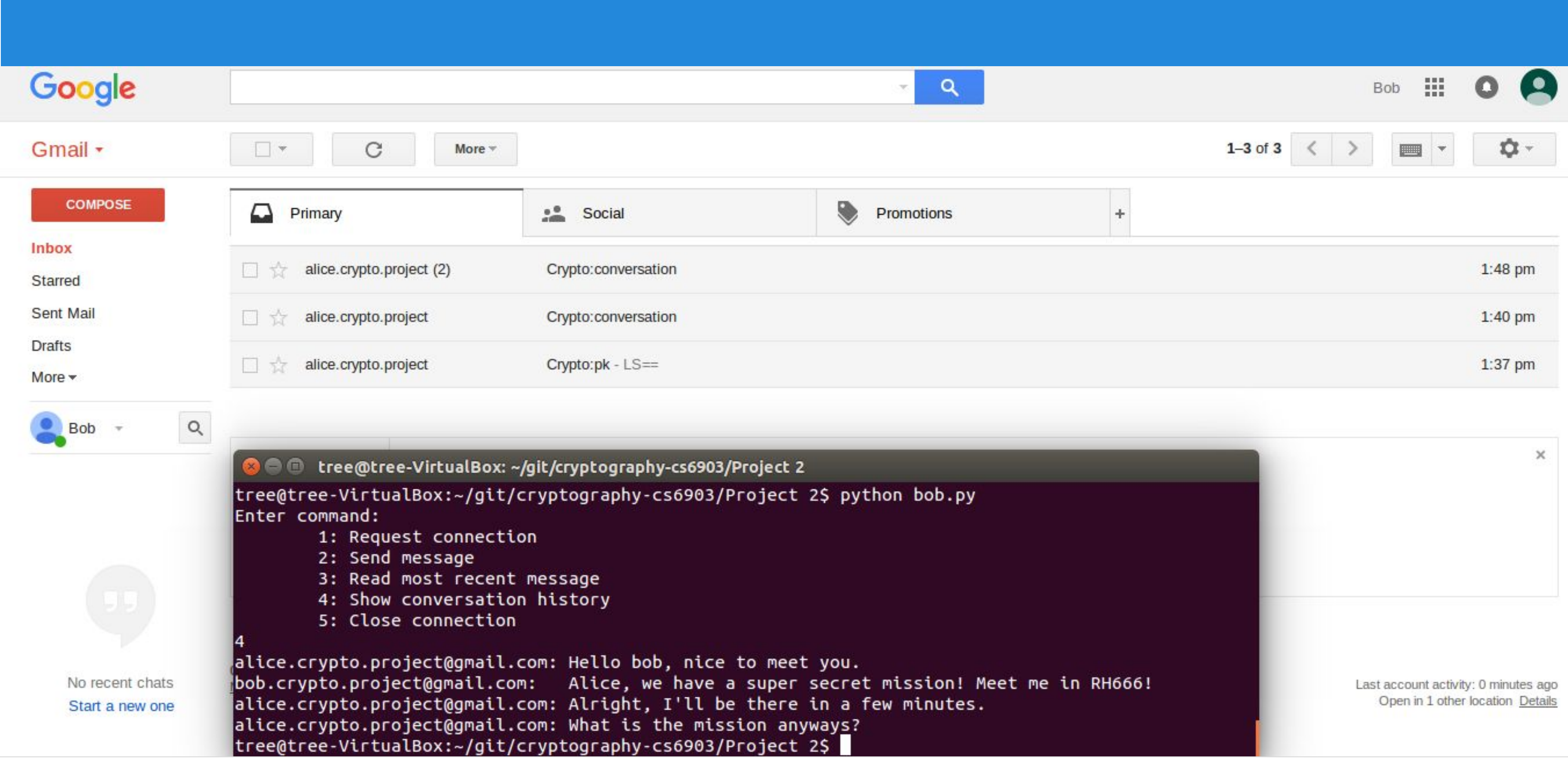
alice.crypto.project@gmail.com
to me
1:40 PM (2 minutes ago)

Z0FBQUFBQldaSUVxZUs0M3M5RlJWcVR6Qk1OajFKUmJ5SnpPdjVFaXU3MFFkQ0pTaTA1c2pJaW1DMG5hWDJidTVFRz
hCZnQ2bTdQTjJuZEZDNzJHaUNyVmVpUVVZR3ZLQXRQSWc5N1dhcHV5OVl5ZDRJX1U2Q2c9

tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2

```
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python bob.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
3
Date: Sun, 06 Dec 2015 10:40:43 -0800 (PST)
From: alice.crypto.project@gmail.com
Subject: Crypto:conversation
Message: Hello bob, nice to meet you.
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ 
```

Bob reads the encrypted mail that Alice sent him



alice.crypto.project (2) Crypto:conversation 1:48 pm

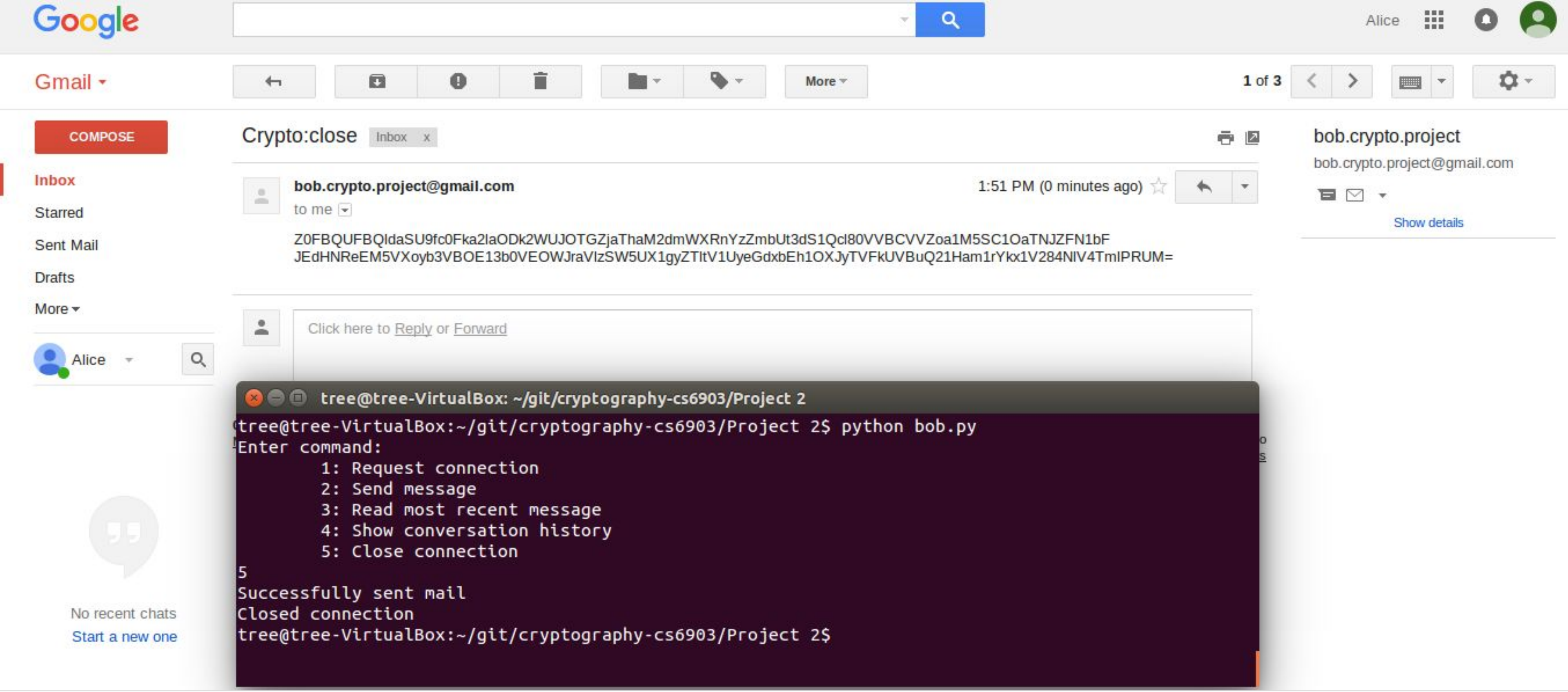
alice.crypto.project Crypto:conversation 1:40 pm

alice.crypto.project Crypto:pk - LS== 1:37 pm

tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2

```
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python bob.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
4
alice.crypto.project@gmail.com: Hello bob, nice to meet you.
bob.crypto.project@gmail.com:   Alice, we have a super secret mission! Meet me in RH666!
alice.crypto.project@gmail.com: Alright, I'll be there in a few minutes.
alice.crypto.project@gmail.com: What is the mission anyways?
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ 
```

After a few more exchanges, Bob checks out the conversation history



Crypto:close Inbox

bob.crypto.project@gmail.com
to me

1:51 PM (0 minutes ago)

Z0FBQUFBQldaSU9fc0Fka2laODk2WUJOTGZjaThaM2dmWXRnYzZmbUt3dS1Qcl80VVBCVVZoa1M5SC1OaTNJZFN1bF
JEdHNReEM5VXoyb3VBOE13b0VEOWJraVlzSW5UX1gyZTltV1UyeGdxbEh1OXJyTVFkUVBuQ21Ham1rYkx1V284NlV4TmlPRUM=

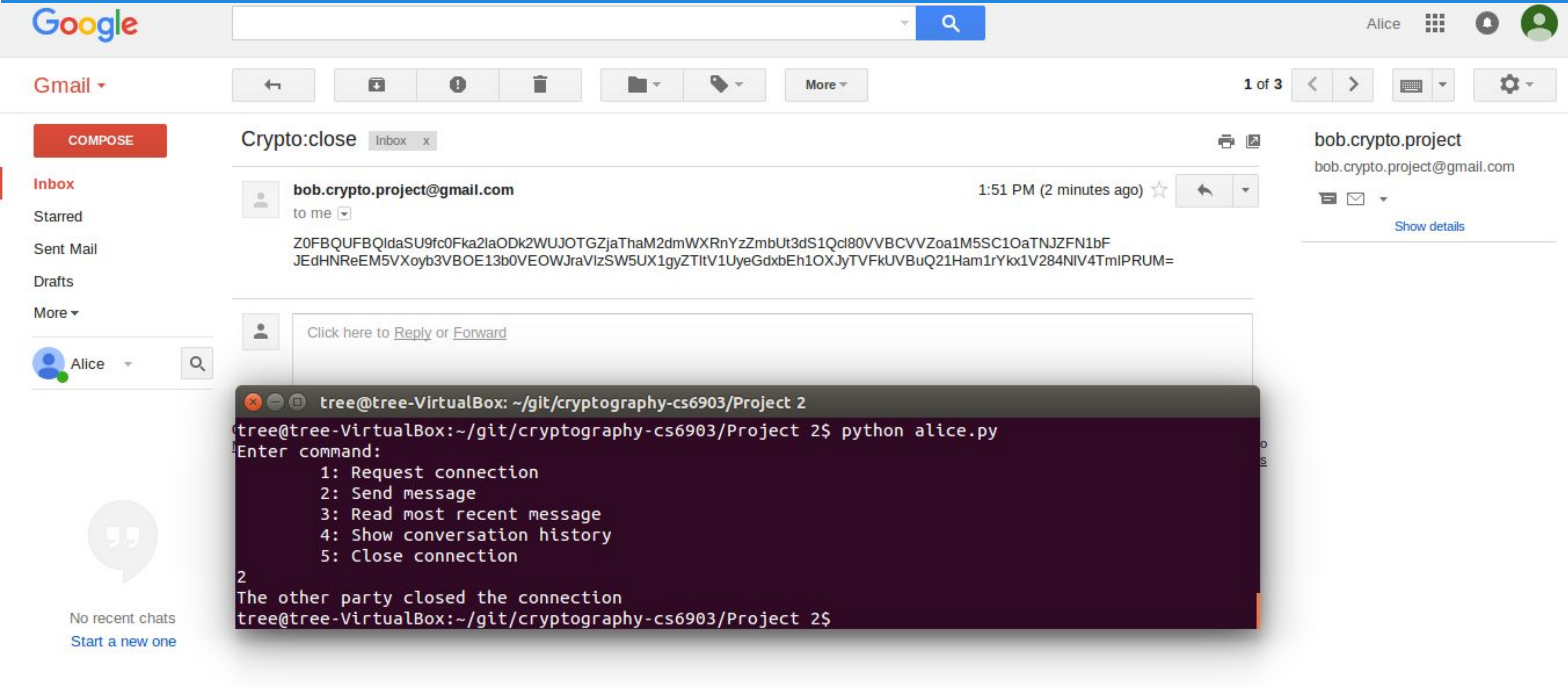
Click here to Reply or Forward

bob.crypto.project
bob.crypto.project@gmail.com

tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2

```
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python bob.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
5
Successfully sent mail
Closed connection
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$
```

Close connection: Bob sends Alice the encrypted shared key



Crypto:close Inbox x

bob.crypto.project@gmail.com 1:51 PM (2 minutes ago)
to me

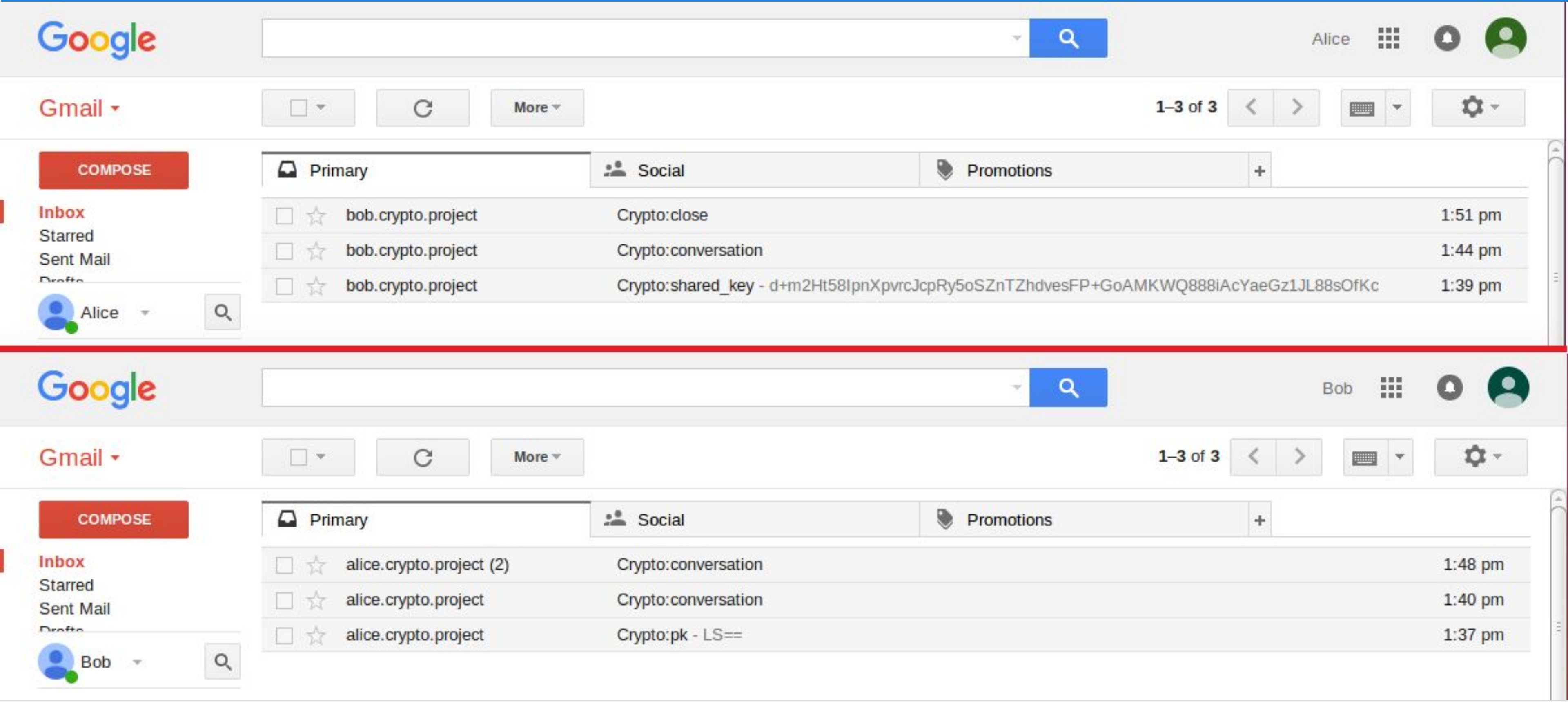
Z0FBQUFBQldaSU9fc0Fka2laODk2WUJOTGZjaThaM2dmWXRnYzZmbUt3dS1Qcl80VVBCVVZoa1M5SC1OaTNJZFN1bF
JEdHNReEM5VXoyb3VBOE13b0VEOWJraVlzSW5UX1gyZTltV1UyeGdxbEh1OXJyTVFkUVBuQ21Ham1rYkx1V284NlV4TmlPRUM=

bob.crypto.project
bob.crypto.project@gmail.com

tree@tree-VirtualBox: ~/git/cryptography-cs6903/Project 2

```
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$ python alice.py
Enter command:
        1: Request connection
        2: Send message
        3: Read most recent message
        4: Show conversation history
        5: Close connection
2
The other party closed the connection
tree@tree-VirtualBox:~/git/cryptography-cs6903/Project 2$
```

Alice tries to send a message, but the connection has already been closed



bob.crypto.project	Crypto:close	1:51 pm
bob.crypto.project	Crypto:conversation	1:44 pm
bob.crypto.project	Crypto:shared_key - d+m2Ht58IpnXpvrcJcpRy5oSZnTZhdvesFP+GoAMKWQ888iAcYaeGz1JL88sOfKc	1:39 pm

alice.crypto.project (2)	Crypto:conversation	1:48 pm
alice.crypto.project	Crypto:conversation	1:40 pm
alice.crypto.project	Crypto:pk - LS==	1:37 pm

Alice’s (top) and Bob’s (bottom) Gmail inboxes after the conversation