gpg (gnu privacy guard)

Mannan Shukla - RUSLUG

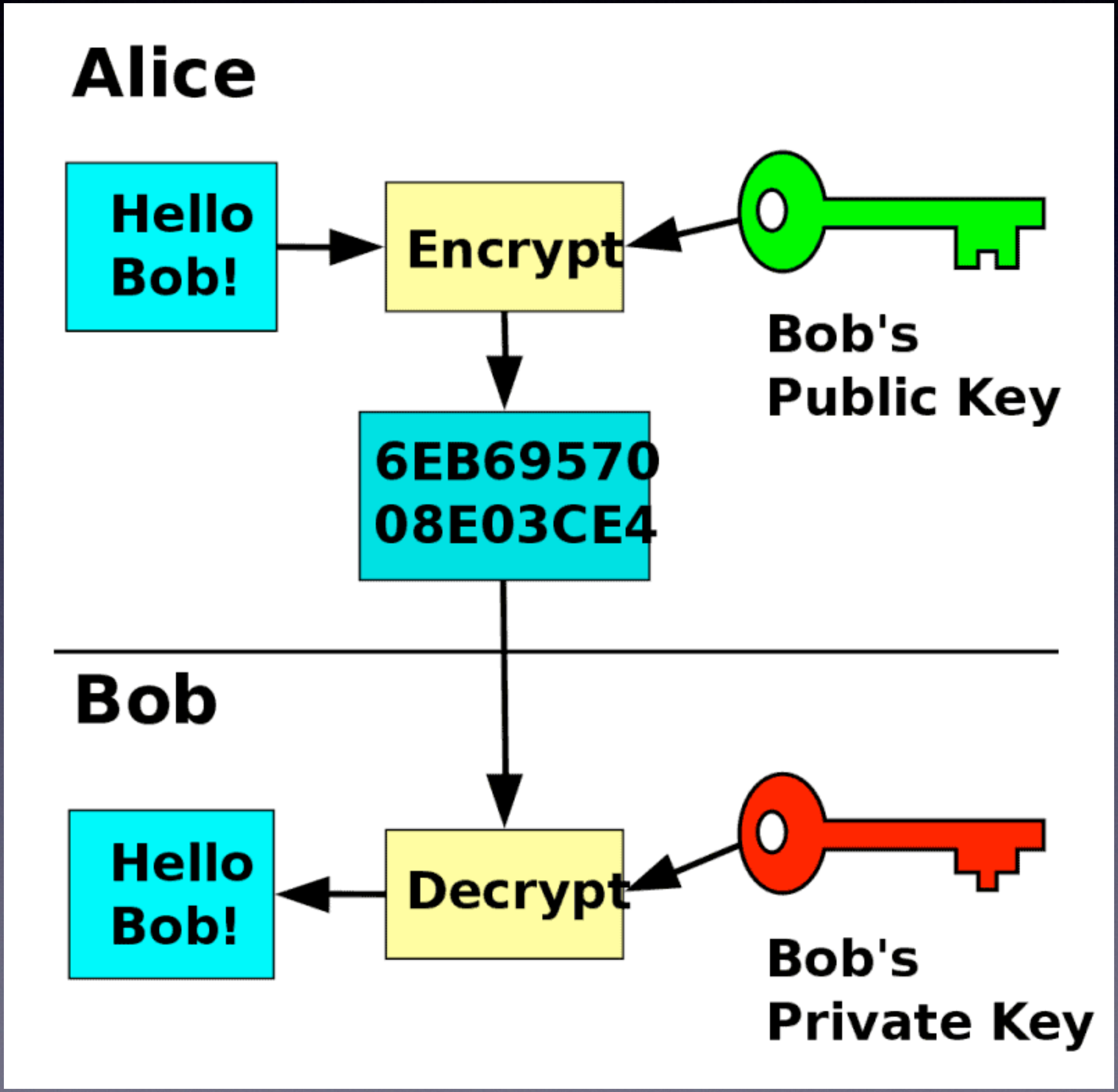
The need for encryption

- keep data password protected and secured
- keep bad actors from taking important data if they breach your machine
- keep documents about the cia private

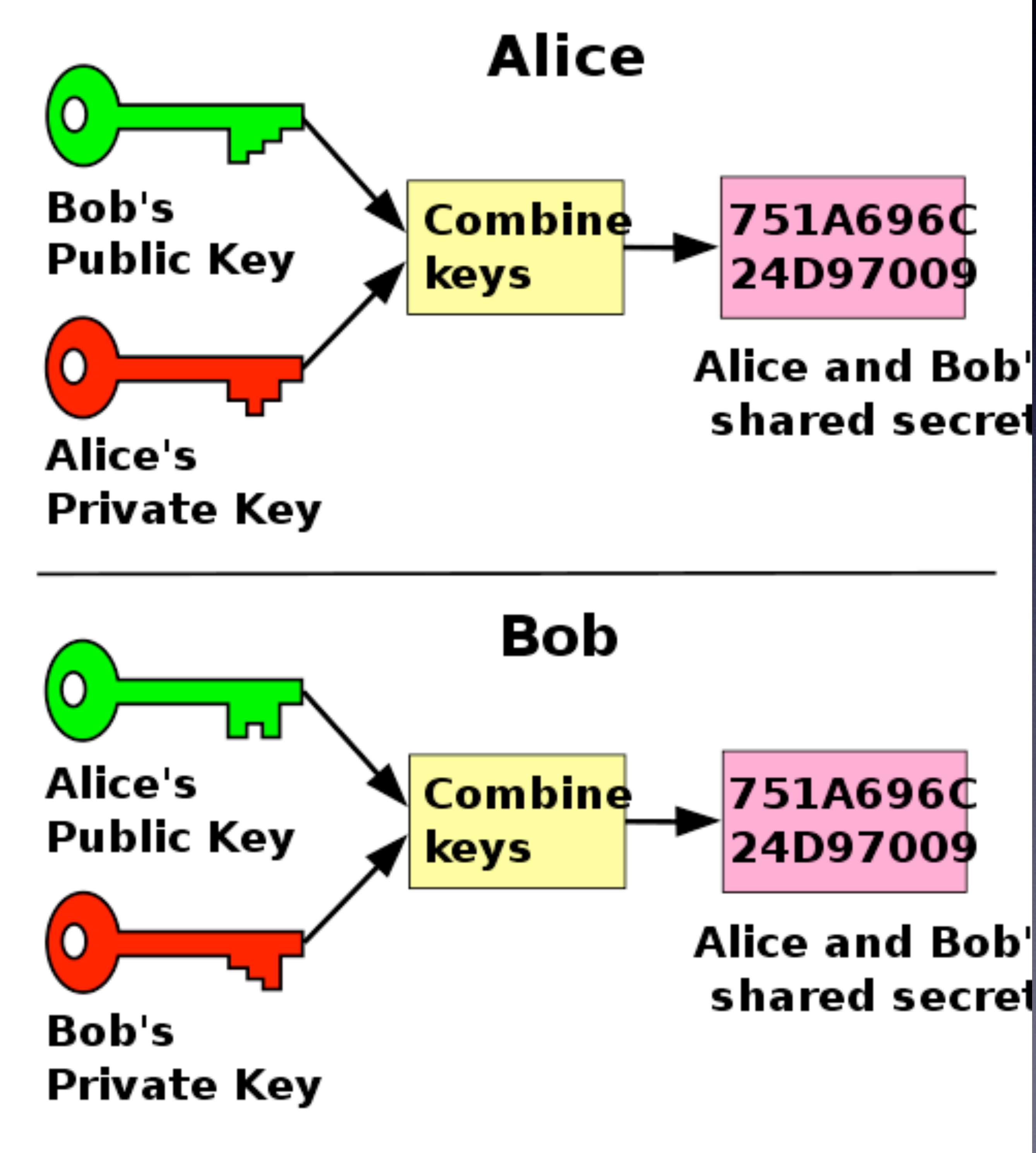
different types of ciphers

- symmetric
- asymmetric
    - public key cryptography

typical use


Alice
Hello Bob!
Encrypt
Bob's Public Key
6EB69570 08E03CE4
Bob
Hello Bob!
Decrypt
Bob's Private Key

Diffie–Hellman scheme



signing files

```
gpg —full-generate-key

gpg -r <email> -e <filename>
```

to decrypt: gpg -d <filename>

in practice

- email clients (gmail, thunderbird, mutt)
  - encryption
  - signing
- protecting files locally
- pass (the unix password manager)
- signing github commits

resources

- https://www.gnupg.org/gph/en/manual/c14.html