Cryptography Primer

folkert@feedface.com

July 2015, May 2016

Overview:
Crypto Concepts

- Symmetrical Cryptography vs Asymmetrical Cryptography
- Asymmetrical Key Pairs
- Centralised Trust vs Decentralised Trust
- Public Key Exchange

Symmetrical Cryptography

- All correspondents share the same *KEY*
- Key need to be exchanged before communication starts

Asymmetrical Cryptography

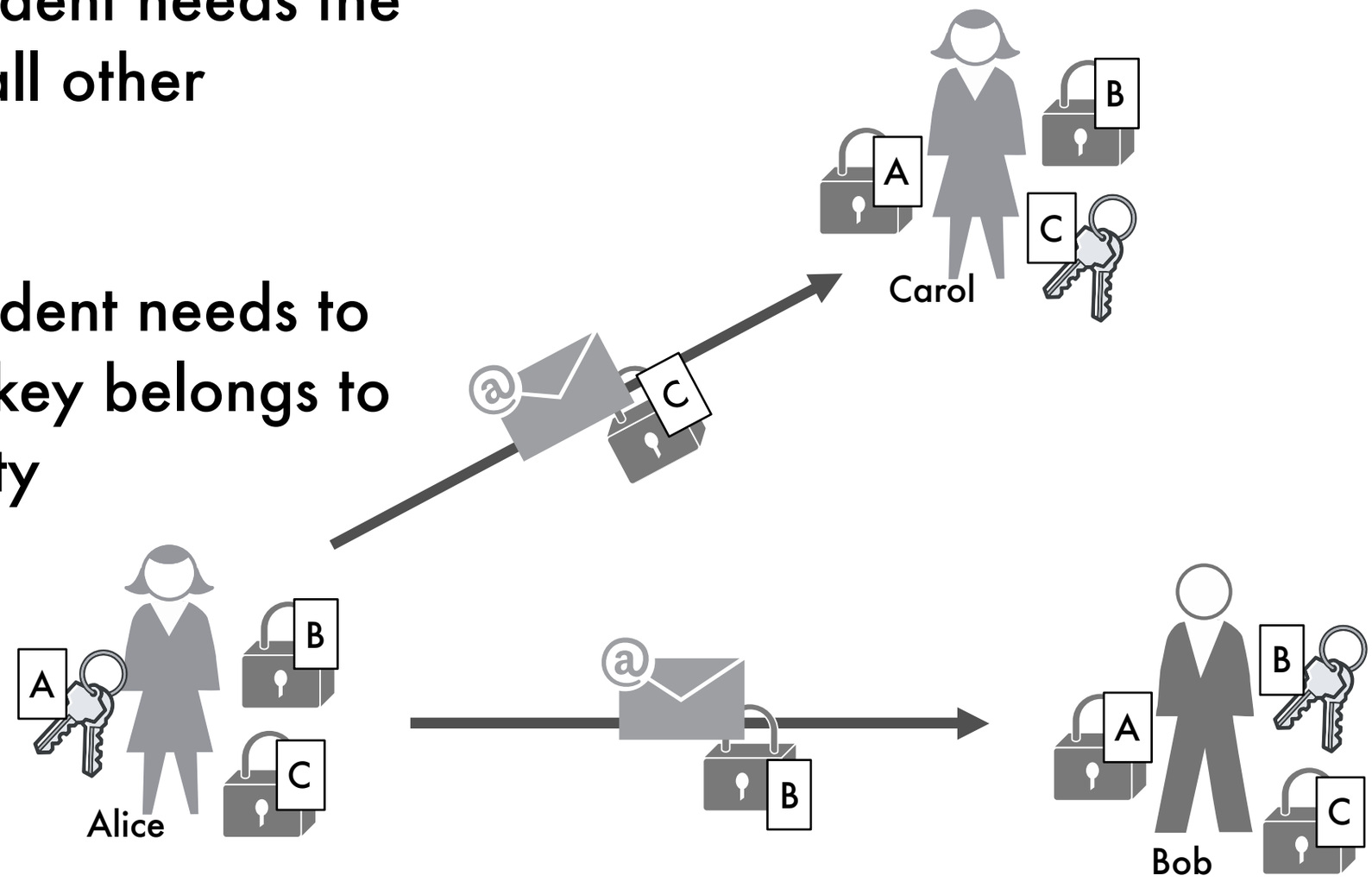
- Each correspondent has a pair of *KEYS*
- The *PRIVATE* Key is used to DECRYPT incoming messages and to SIGN outgoing messages
- The *PUBLIC* Key is used to ENCRYPT outgoing messages and to VERIFY incoming messages

Private Key

Public Key

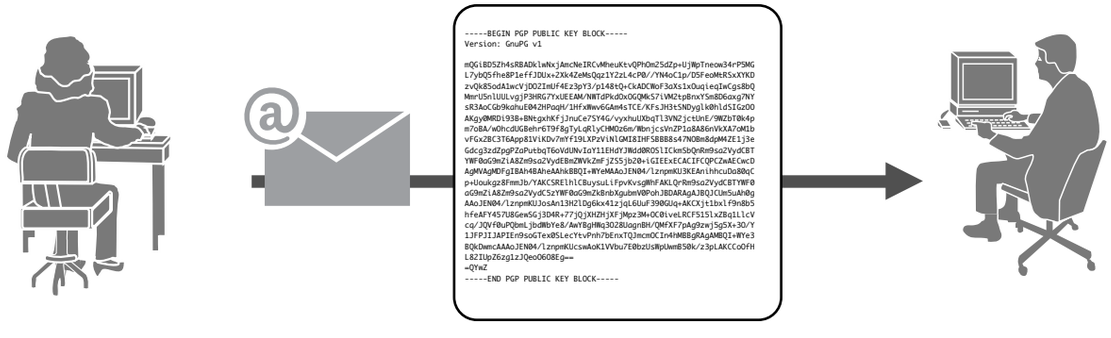
Asymmetrical Cryptography

- Each correspondent needs the PUBLIC key of all other correspondents
- Each correspondent needs to TRUST that the key belongs to the desired party



Public Key Exchange

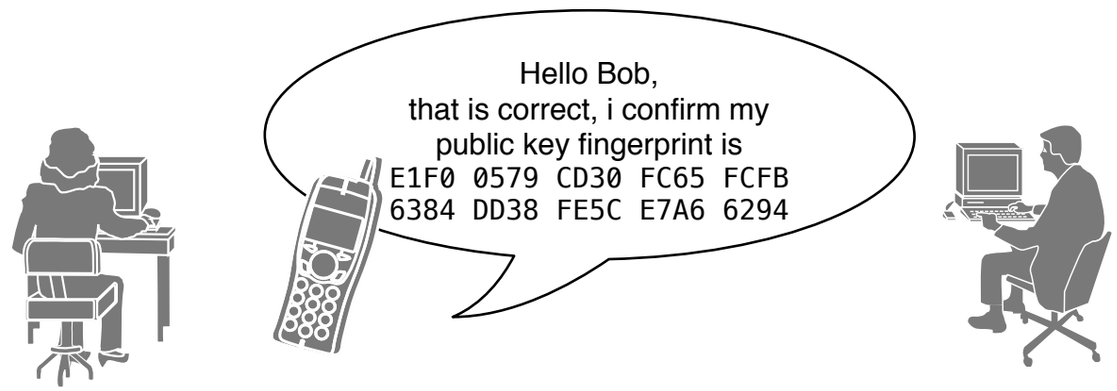
1. Alice sends her PUBLIC KEY to Bob



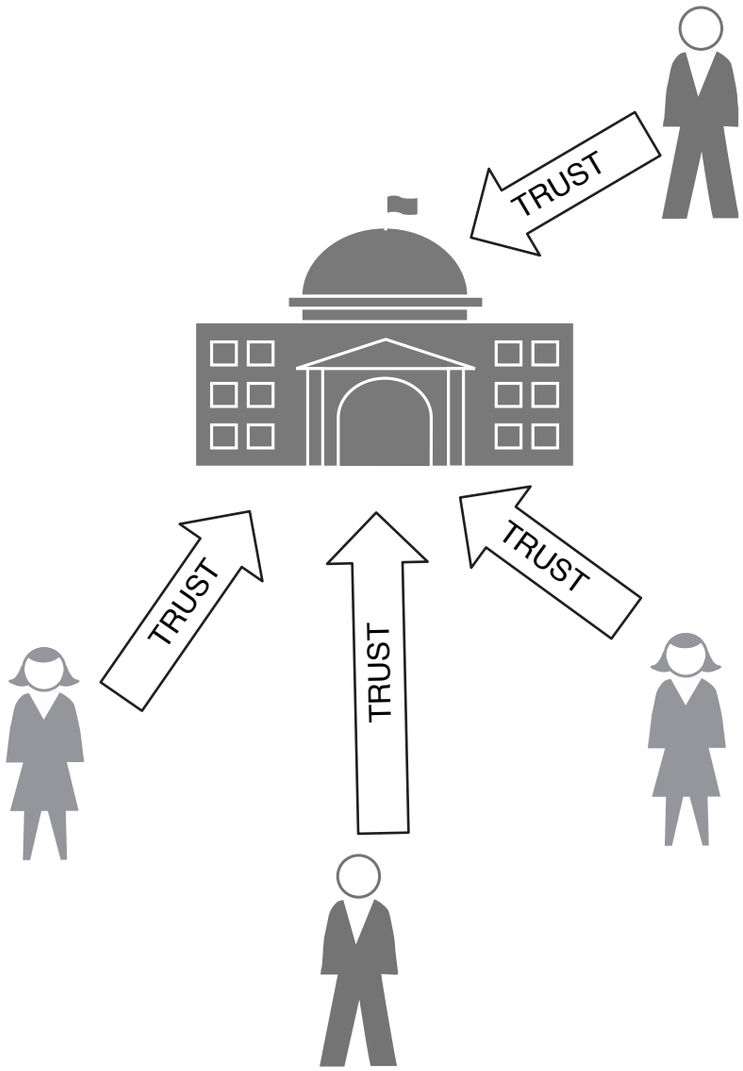
2. Bob asks Alice to confirm her public key FINGERPRINT over a secure channel

3. Alice confirms the fingerprint

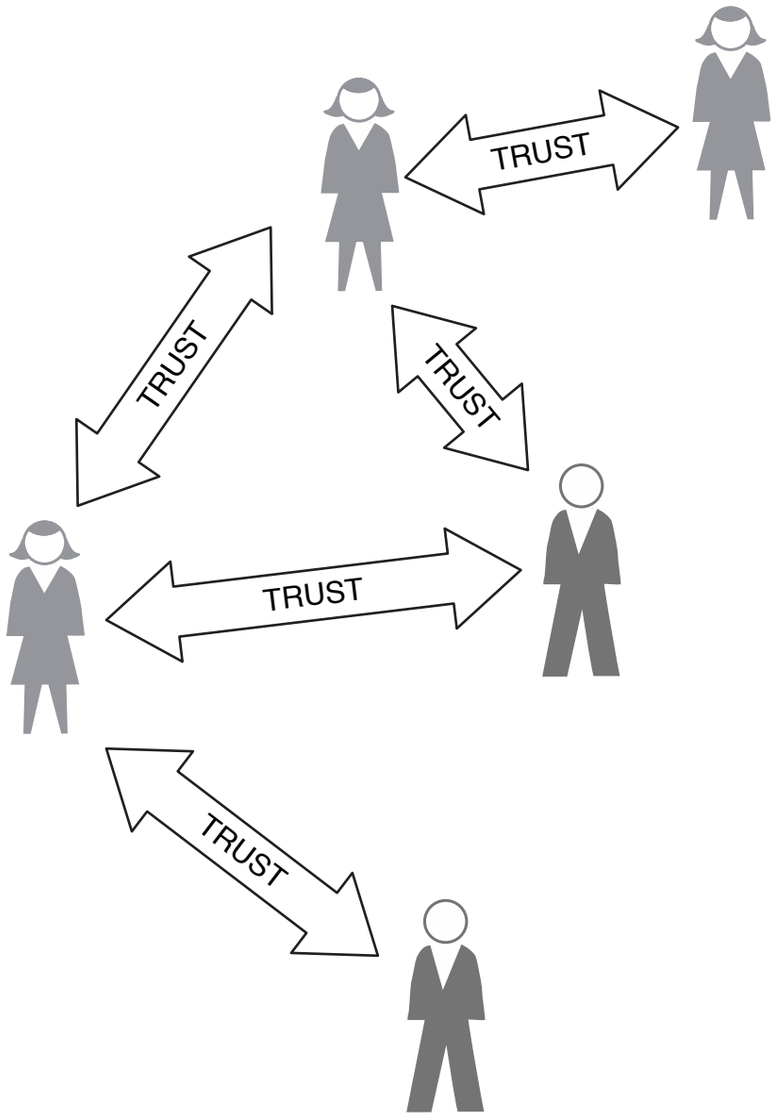
Bob can now encrypt messages to Alice, and verify messages from Alice



Centralised Trust vs Decentralised Trust



Public Key Infrastructure



Web Of Trust

Overview:
Platforms & Tools

- Internet Messaging (Jabber/OTR)
- Electronic Mail (GPG)
- Smartphone Messaging
- Virtual Private Networks (VPN)
- Online Anonymity (TOR)

Internet Messaging
Jabber/OTR

- End-To-End Encryption, Off-The-Record Encryption
- Open Protocol, Multiple Providers and Apps
- Works over Facebook, Google Talk
- Chaos Computer Club Jabber Service
  http://jabber.ccc.de
- Adium Instant Messenger
  http://www.adium.im
- Pidgin Instant Messenger
  http://www.pidgin.im

Electronic Mail
PGP / GPG

- End-To-End Encryption,
  Web Of Trust

- Open Standard, works with eMail

- GNU Privacy Guard
  http://gnupg.org

- GPG For Windows
  http://www.gpg4win.org

- GPG Tools
  https://gpgtools.org

Smartphone Messaging

- End-To-End Encryption
- Single Commercial Providers
- Phone Number as Address

- Signal
  https://whispersystems.org
- Telegram
  http://telegram.org
- WhatsApp
  http://facebook.com

Virtual Private Networks

- All Internet Traffic goes through Tunnel Provider

- Open Protocols, Various Commercial Providers

- OpenVPN + Tunnelblick Applications
  https://www.openvpn.net
  https://code.google.com/p/tunnelblick/

- iPredator VPN Provider
  https://www.ipredator.se

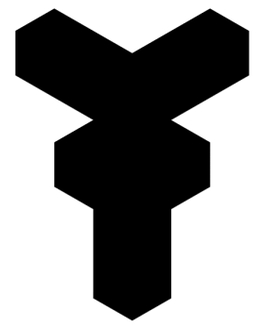
Online Anonymity

- Hides where internet traffic is coming from

- Open Protocol, Volunteer Network
- TOR Network
  http://www.torproject.org
- TAILS Operating System
  http://tails.boum.org

Resources

- The Crypto Party Handbook
  http://www.cryptoparty.in/learn/handbook



http://www.feedface.com/tech/cryptoprimer.html