CRYPTOGRAPHY

THE STUDY OF ENCRYPTION

Created by Chris Foster / @chrisfosterelli

THE PLAN

Things we will be covering:

- Basic Cryptography History
- What is Encryption Used For?
- Common Encryption Ciphers
- Symmetric vs. Asymmetric
- How Can I Use Encryption?
- Hi PGP!
- *Workshop Component*
- Coinbase.io
- *Workshop Component*
- End

BASIC CRYPTOGRAPHY HISTORY

- Spies, military leaders, diplomats...
- Transposition Ciphers, Substitution Ciphers, Caesar Ciphers...
- Steganography & Cryptography
- Enigma Machine and WWII
- Birth of computing
- Then, Cryptography became hard

WHAT IS ENCRYPTION USED FOR?

Most common uses:

- TLS/SSL
- Databases
- Disk Encryption
- Copyright Protection
- Reverse Engineering Protection

SYMMETRIC VS. ASYMMETRIC

Symmetric:

- One password
- Both people must know the password
- Hard for communication
- Fast

Asymmetric:

- Two 'passwords'
- Only one person needs to know the secret
- Perfect for communication
- File, not password
- Slow

COMMON ENCRYPTION CIPHERS

- AES
- Blowfish
- DES
- Triple DES
- Serpent
- Twofish
- RSA

HOW CAN I USE ENCRYPTION?

Reaons you might want to use encryption:

- Secure communication
- Keeping data private
- Developing software

KEEPING DATA PRIVATE

- Android phones self-encryption
- Truecrypt for Windows/Linux/OSX
- Plenty of other options...

HI PGP!

- De-facto standard for secure communication
- Works over anything
- GPG, specifically
- Asymmetric

WORKSHOPPIN’

http://bit.ly/1rmzWO4

COINBASE.IO

Bringing PGP to the web...

WORKSHOPPIN'

http://bit.ly/1r6DSnh

END

@chrisfosterelli

TRUSU Computer Science Club

http://trucsclub.ca/