Class 2: Cryptography

Schedule

Before the next class (Wednesday, Sept 2):

- **Read:** *Chapter 3: The Bitcoin Client* and *Chapter 4: Keys, Addresses, Wallets* from Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* book (also available in print).
- **Read:** *Chapter 1: Introduction to Cryptography and Cryptocurrencies*, from Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. This chapter starts with cryptographic hashing and authenticated data structures (which we are deferring until until later, but is still worth reading now), and Section 1.3 covers digital signatures.

Monday, September 7: Check-up 1. This will be a short in-class quiz to test your understanding of the main concepts covered so far. It will cover material from the readings and classes 1-3.

Tuesday, September 15 (8:29pm): Problem Set 1 due.

Cryptography

kryptos is a Greek root meaning hidden ("secret")

crypto + *graphy* = "secret writing"

Decryption is what the intended receiver does.
Cryptanalysis is what an attacker does.

How are cryptography and security related?

Simple Message Cryptosystem

Two functions:

- **Encrypt:** $E(m\text{: byte}) \rightarrow \text{byte}$. The input is called the **plaintext**; the output is called the **ciphertext**.
- **Decrypt:** $D(c\text{: byte}) \rightarrow \text{byte}$.

Required properties:

- **Correctness:** for all possible messages, m, $D(E(m)) = m$
- **Security:** given the output of $E(m)$, it is "hard" to learn anything interesting about m.

Goldwasser and Micali win Turing Award: Team honored for 'revolutionizing the science of cryptography', MIT News, 13 March 2013.

Their paper that introduced semantic security notions is: *Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information*, ACM Symposium on Theory of Computing, 1982. (We will not get into formal security definitions or proofs in this class, but you should take Mohammad Mahmoody's class to learn them.)

Keyed Symmetric Cryptosystem

Claude Shannon, *Communication Theory of Secrecy Systems*, 1949 (work done during World War II, but declassified later).

Two functions:

- **Encrypt:** $E(k$: byte, m: byte$) \rightarrow$ byte.
- **Decrypt:** $D(k, c$: byte$) \rightarrow$ byte.

Required properties:

- **Correctness:** for all possible messages, m, and keys, k, $D(k, E(k, m)) = m$.
- **Security:** given E, D, and the output of $E(k, m)$ it is "hard" to learn anything interesting about m (without knowing k).

Are these properties enough to be secure against an active attacker?

Keyspace: set of all possible keys. Assume (hopefully for user!) that key is drawn uniformly from this set.

Brute Force Attack: for all possible keys, k_i, try computing $D(k_i)$ to see if it looks like a reasonable plaintext.

In order for a brute force attack to succeed, what properties are necessary about (1) the keyspace and (2) the message space?

Where is symmetric cryptography used in your bitcoin wallet?

Asymmetric Cryptosystems

Asymmetric cryptosystems use *different functions* for encrypting and decrypting, with the property that revealing the encryption function does not reveal the decryption function. With Kerckhoff's Principle, this means there are different keys for encryption and decryption.

- **Generate:** produce key pair, (KU_X, KR_X), and publish the public key, KU_X.
- **Encrypt:** $E(KU_X$: byte, m: byte) $\rightarrow$ byte.
- **Decrypt:** $D(KR_X$, c: byte) $\rightarrow$ byte.

Messages: Sender encrypts a message with the recipient's public key. Recipient decrypts the message using her private key.

Signatures: Signer encrypts a message with her own private key. Verifier checks the message using the signer's public key.

How can we use asymmetric cryptosystems to *prove* ownership?

How can we use asymmetric cryptosystems to *transfer* ownership?

Where is asymmetric cryptography used in your wallet?

Assuming we have a strong asymmetric cryptosystem, what hard problems are left to solve to make a cryptocurrency?