University of Virginia **cs4501: Cryptocurrency Cafe** January 14, 2015

Class 2: Cryptography

Schedule

Before the next class (Wednesday, Jan 21):

1. **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).
2. Pay attention to your email. You should receive an email by Sunday, and it will include some other things to do before Wednesday's class.

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

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:** $E(k\text{: bytes}, m\text{: bytes}) \rightarrow$ bytes.
- **Decrypt:** $D(k, c\text{: bytes}) \rightarrow$ bytes.

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?

Jefferson's Wheel Cipher

There are, of course, better ways to break a message encrypted using Jefferson's Wheel cipher than just trying all possible keys as in a brute force attack. Here's how Geoff Stoker solved it: *Jefferson Wheel Challenge solved!*.

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

Brute Force Attack: try for all possible keys, k_i, computing $D(\_k_i)$ and 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?

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:** $E(KU_X$: bytes, m: bytes$) \rightarrow$ bytes.
- **Decrypt:** $D(KR_X, c$: bytes$) \rightarrow$ bytes.

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?

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

Martin Luther King at the University

There's no class on Monday to honor Martin Luther King day. Students are encouraged to use the class time to read Paul Gaston's *Honor to the Class of 1969* and to learn about *Desegregation at the University of Virginia and its Surrounding Communities* (including President Darden's letter).

Why is Edgar Shannon the only past-president of UVa with nothing significant at the University named after him? Why does the University still have courtyards and schools named after Colgate Darden and none for Gregory Swanson or Sarah Patton Boyle?

How do the actions of our current administration (especially in response to recent events) compare to those of the 1960s?

Will there be justification for an *Honor to the Class of 2015/2016/2017/2018* essay?