Cybersecurity for Future Presidents

Lecture 11:
DEBATE #4:
Resolved: Commercially stored genomic data requires no further government regulatory controls.

Any Questions?

My office hours:
Wed. afternoon, 12-3pm, 442 RH. Signup sheet circulating

- About previous lecture?
- About homework? (debate questions)
- About reading? (debate reading)

Reading for next week: D is for Digital Part II Software: Intro and Chapter 4 Algorithms (pp. 51-63)
Exercises: Accountability topics and more.

Next Debate (in 2 weeks): Resolved: The U.S. Treasury Department should treat bitcoin as currency rather than as property.
Debate teams please sign up to see me this week or next week (as teams).

Cybersecurity events from the past week of interest to future (or current) Presidents:

- DHS, FBI begin briefing power grid operators on Ukraine power grid attacks as potential U.S. threat
- Senate Intelligence Committee reportedly drafting legislation to require "technical assistance" from vendors of products with encryption
- Senate passes bill to provide stronger basis for prosecuting theft of trade secrets
- Justice Dept continues to press Apple

Coming up: … ?

Today's Debate

DEBATE #4:
Resolved: Commercially stored genomic data requires no further government regulatory controls.

Change to topic for final debate!

I've learned more about bitcoin and how it is treated by the government
The original debate topic I framed is not appropriate

NEW TOPIC:
RESOLVED: Bitcoin transactions are better for consumers than credit card transactions

Here's how parts of the government view bitcoin today

- IRS – it's property
- FINCEN – it's money
- CFTC – it's a commodity

Cryptographic Hashing

What is a secure hash function / secure hash algorithm?

- Random (but deterministic) function from a large source space to a smaller target space
- Random: given the input, you can't predict the output
- Deterministic: given the same input, you get the same output

Properties desired of cryptographic hashes:

- quick to compute the hash value for any given message
- infeasible to generate a message from its hash value
- infeasible to modify a message without changing the hash value
- infeasible to find two different messages with the same hash value.

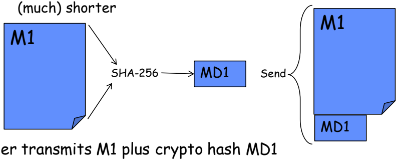
Collisions

Since the target space is smaller than the source space, some things in the source space must map to the same thing in the target space.

- That's called a COLLISION.
- Collisions should be rare and should be difficult to generate

Using Cryptographic Hashes

- "Message Digest": given a message, crypto hash of the message is (much) shorter



Sender transmits M1 plus crypto hash MD1

(signed with sender's private key)

Receiver uses M1 and sender's public key to re-compute crypto hash MD1'

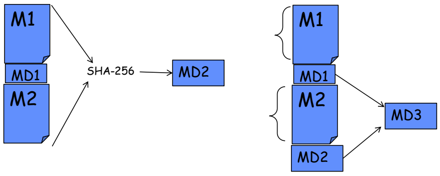
If received MD1 matches re-computed MD1' all is well

If not, message has been modified en route

If attacker can find M2 that has same digest as M1, could substitute M2 for M1 and receiver would be deceived

Putting hashes together

- Suppose you want to bind a new message to a collection of messages


M1
MD1
M2
SHA-256
MD2
M1
MD1
M2
MD2
MD3