Ethics of Encryption

CS489 Computer Ethics and Social Issues

Shin Yoo

Encryption

- “The process of transforming information in a way that, ideally, only authorized parties can decode (Wikipedia: https://en.wikipedia.org/wiki/Encryption)

- It is generally considered to be… a good thing?

  - As in… we are constantly told not to store anything in raw data (e.g., storing user passwords)

Single-Key Encryption
(aka Symmetric Encryption)

- Encrypt the given message using an encryption algorithm and a number called the “key”: both the sender and the recipient share the same key to encrypt and decrypt the message.
    - Password on word documents, or PIN on your bank account
    - Inherently not secure!
        - Sender and receiver needs to share the key: they need to trust each other, they cannot maintain anonymity from each other.
        - Communication of sharing the key needs to be secure.

Public Key Encryption

(aka Asymmetric Encryption)

- Each user owns a private and public key pair: they are mathematically linked to each other.
  - Only one key of the pair is needed to encrypt a message; then the other key can be used to decrypt the message.
  - Sender uses receiver’s public key to encrypt the message; receiver uses the private key to decrypt the message. Sender does not know receiver’s private key.
- Public keys can be public - no secure communication required.

Rivest-Shamir-Adleman (RSA)

The most widely used public-key encryption

- Depends on the notion of one-way function regarding primes. It is easy to compute the product of two numbers, but much harder to factor a large number.

- RSA depends on two large prime numbers. Intuitively, their product is the public key, whereas the private key is computed using the two primes (i.e., the factors of the public key).

  - Only the person who knows the factors can compute the private key, which then decrypts the message.

  - Knowing the public key does not help you much in terms of knowing the private keys (=the factors), due to the one-wayness of factorization.

Okay… but… what about encryption and ethics?

Silk Road Marketplace

- The first modern “dark-web” market where illegal goods (including drugs) could be purchased.
    - Transactions were made using Bitcoins: between February 2011 and July 2013, sales through Silk Road amounted about 9.5Million BTC.
    - Invented by Ross Albright, and taken down by FBI in October 2023. Albright is serving two life sentences, without possibility of parole.
    - Operated on TOR network.

Onion Routing

- A data packet is protected by multiple layers of encryption (like layers of onion skins): each layer, when decrypted, only tells you the next destination, and NOT the final destination.
- At any single point, one cannot trace the packet back to the origin, and cannot know where the packet is headed.
- Ironically, this was originally developed by US Naval Research Lab, and further refined by DARPA :)
    - Naval Research Lab even released the code under open source license

TOR (The Onion Routing) Network

- The user chooses a path that consists of TOR server nodes; there is a public directory of servers.

- Using public key from the directory, the user then establishes a secure connection to the first note of the path; then, using encryption that can only the second node can decrypt, the user connects to the second note, and repeat this until the entire path is connected.

- Each node does not know whether the preceding one is the origin, nor whether the next node is the exit.

“And now for something completely different…”[1]

[1] https://en.wikipedia.org/wiki/And_Now_for_Something_Completely_Different

Crypto-Anarchy

- A political ideology focusing on the protection of privacy, political freedom, and economic freedom, using cryptographic software for confidentiality and security while communicating over computer networks.

- 😧 😧 😧 😧 😧 😧 😧 😧????

The Crypto-Anarchist Manifesto

Timothy C. May, 1988

- https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

“Isn’t that taking things too far? How can you claim that cryptography leads to anarchy?? 😧 😧 😧”

State and Social Contract

- Why does “a state” (as in country, government) work?
- We sign an implicit contract when we are born: *“the society grants us rights but also assigns us responsibilities, which the state is able to enforce by violence”* - The People vs. Tech, Bartlett
- Based on this social contract, we agree that some of our rights can be reserved for the good of the society.
- The state maintains monopoly over two important elements: violence (police, military, etc) and money (taxation, monetary policy, etc)

So, what about cryptography?

- Essentially cryptography aims to hide your actions: whatever you do becomes invisible from public space (i.e., out of the state’s eyes) - meaning you take your actions out of the social contract. For example:
    - Cryptocurrency as a means of payment that is untraceable
    - End-to-end communication channel as a way of blocking censorship

Why is ~~bitcoin~~ any money valuable?

- Gold Standard System (19th Century, as well as Bretton Woods system that lasted 1944~1971): there is a fixed conversion ratio between any money and gold - central banks of countries need to have corresponding amounts of gold to mint more money.
- Nowadays: money is a legal tender, just because the country says so (and we all decided to agree with it)
- Who guarantees the exchange value of real money vs. bitcoins?
  - For the real money, it is the state's monopoly on violence :)
  - For the bitcoin, is it the potential, unrealized future value…?

Cryptography and State Regulation

- After WWII, initially cryptography was considered a military technology and its export was banned in US (just like weapons technologies).
- In 60s, commercial banks wanted safer communication to wire money. Companies like IBM applied for individual export licenses.
- PGP (https://en.wikipedia.org/wiki/Pretty_Good_Privacy) was released on the Internet in 1991 by Phil Zimmermann. He was investigated for violating munitions export ban.
- The charge was dropped in 1996. Regulations about export ban became a bit more relaxed after this.

Cryptography and State Regulation

- Netscape used to maintain two versions of its web-browser. US-version used the full 1024-bit RSA, whereas the international version was restricted to 512-bit.
- US still controls the non-military exports of encryption technology with Export Administration Regulations (EAR), although the regulation is more relaxed than the pre-1996.

A Hard Balancing Act

- On one hand, cryptography has this anarchic tendency; on the other hand, cryptography can also be used to fight authoritarian governments.
- Consider Telegram in Korea:
  - It became widely known when KakaoTalk was under criticism that it opened up private communications to the government without trying to protect users.
  - But it has now also become known as a massive ground for criminal activities, precisely because of the protection it provides.

A Hard Balancing Act

- We do balance the state monopoly on violence and money. Police and military are regulated by the law; monetary policies are controlled by democratic means.

- Perhaps we haven't found the right way to balance some of the digital technology YET, because often the technology as well as their end product exists virtually (e.g., as software) - they are intangible, invisible, and do not conform to laws of nature.

Ongoing Story of Telegram

- “How a tech company prevailed against the state in Putin’s Russia” - Washington Post, 2020.06.30 (https://www.washingtonpost.com/opinions/2020/06/23/how-tech-company-prevailed-against-state-putins-russia/)

- “Telegram CEO Pavel Durov arrested at French Airport” - BBC, 2024.08.26 (https://www.bbc.com/news/articles/ckg2kz9kn93o)

- “Inside the DeepFake porn crisis engulfing Korean schools” - BBC, 2024.09.03 (https://www.bbc.com/news/articles/cpdlpj9zn9go)

Let’s try RSA encryption :)

- Hands-on with RSA encryption provided by PyCryptoDome (https://www.pycryptodome.org/)