Cryptography: Public Key Encryption

12-10-18

Journal:
Cryptography expert Whitfield Diffie said he wanted to solve the key distribution problem for benefit of "ordinary people," as opposed to just governments and corporations.
How do you and I benefit from his team's solutions to the Key Distribution Problem?

yeet

Objectives
•Students will understand the impact of the key distribution problem on secure communication.
•Students will understand that a carefully designed one-way mathematical function allows people to exchange keys or use public keys to solve the key distribution problem.
•Students will understand that digital certificates are used for authentication, and that these certificates rely on the trust model: the certificate authorities are being *trusted* to provide accurate information

CS Matters

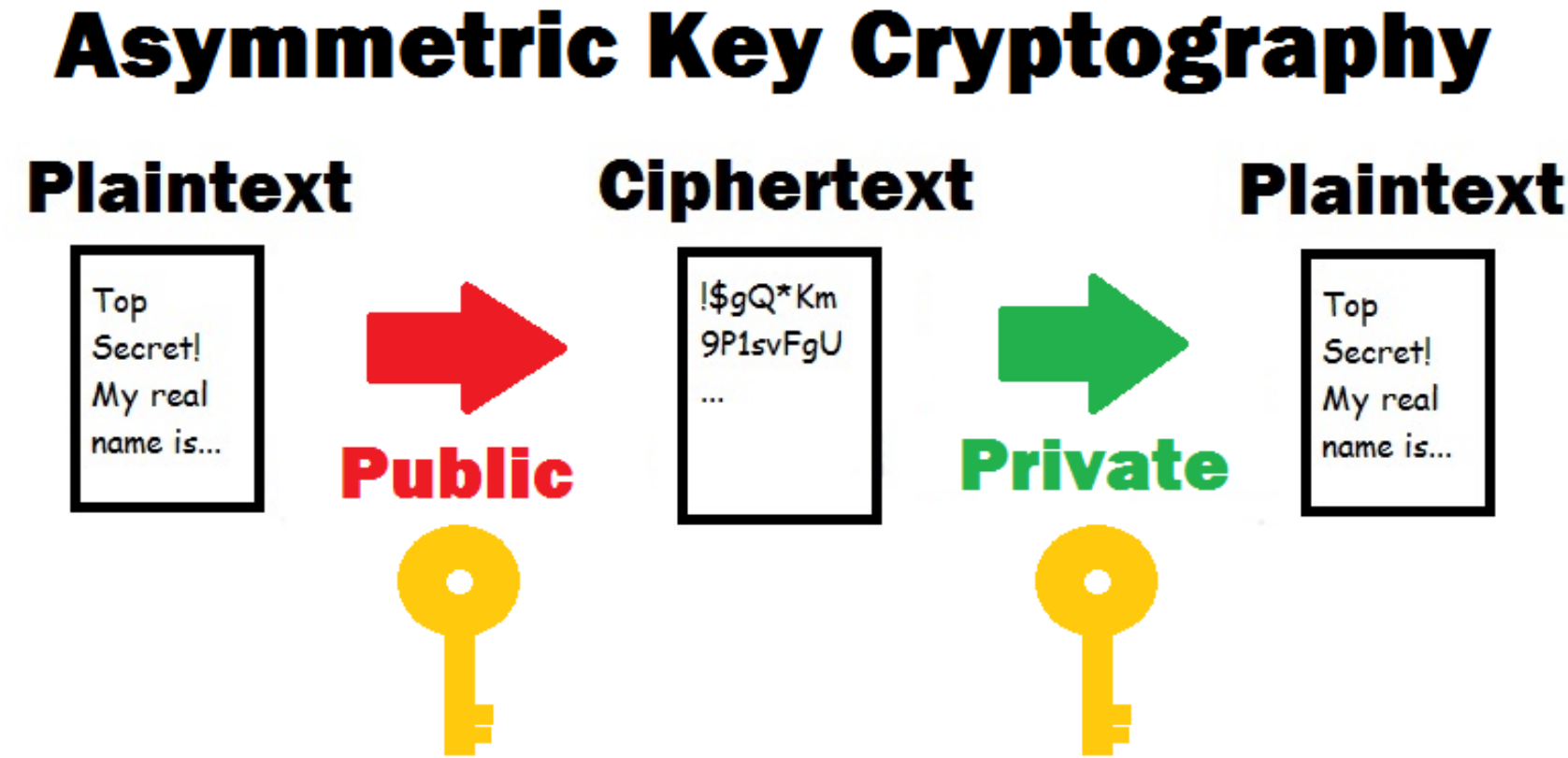
Key Distribution Problem

- Whitfield Diffie's Solution
  - "Public Key" Cryptography
  - Big Idea: Encrypt with one key (public key), decrypt with a second key (private key)
    - Everybody has a public key that they distribute freely to anyone who wants to send them an encrypted message.
    - The private key is kept secret and is used to decrypt the message.

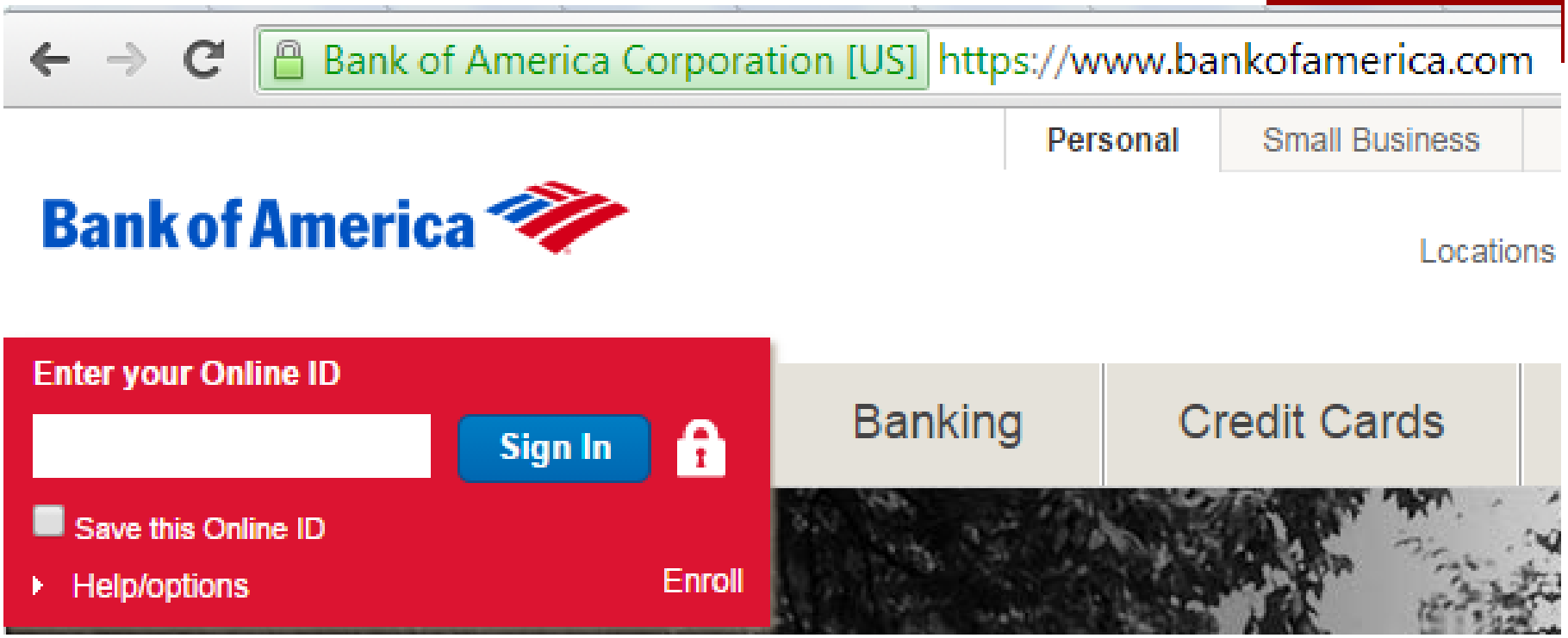
Analogy w/ Physical Locks

- Li gives out open padlocks (public key) to anybody who wants to send her a secret message.
- Alice puts her secret in a box and shuts the padlock that Li gave her (easy).
- When Li gets the box, she uses the combination (private key) to open the padlock.

Asymmetric Encryption



Secure Websites – SSL / TLS



Public Key 3 Act Play

- Roles
  - Customer
  - Store
  - Store Impersonator
  - Certificate Authority

Who Do You Trust?

- Who do you have to trust for this system to work?

Math in Public Key Crypto

- Diffie didn’t figure out the math! (Abstraction)

- RSA
  - Large prime numbers are multiplied as part of the one way function.
  - It is very hard to factor the product to figure out what the two prime numbers were.

Open Standards

- Open Standards are available for anyone to see the details of how they work.
- Proprietary standards have the details of how they work kept secret.

yeet

dab*

- If Cryptography is all about secrecy, does it make sense to have "Open Standards" of encryption?
- https://www.internetsociety.org/policybriefs/openstandards/

Exit Slip

"Open standards result in strong security."

- Do you agree or disagree with this statement? Give specific reasons to back up your position.