How cryptography protects your information every day

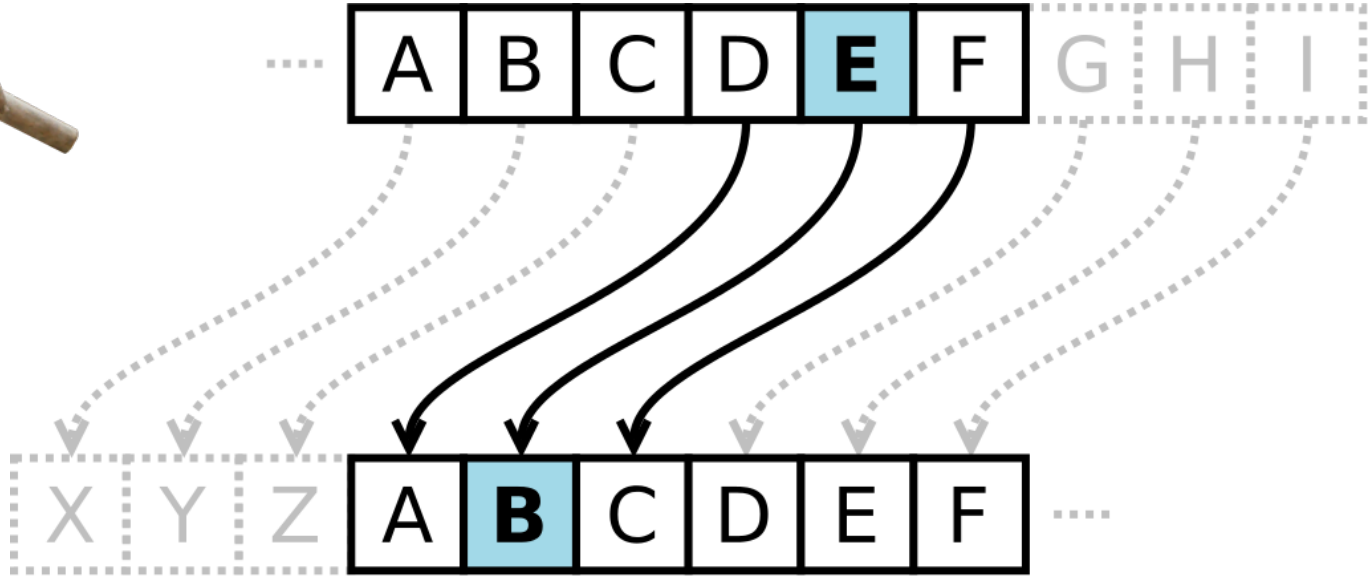
Douglas Stebila McMaster University

Funding acknowledgements:

NSERC CRSNG

Faculty of Engineering Lunch & Learn • February 16, 2017

Caesar cipher



Images courtesy of Wikipedia

Caesar cipher

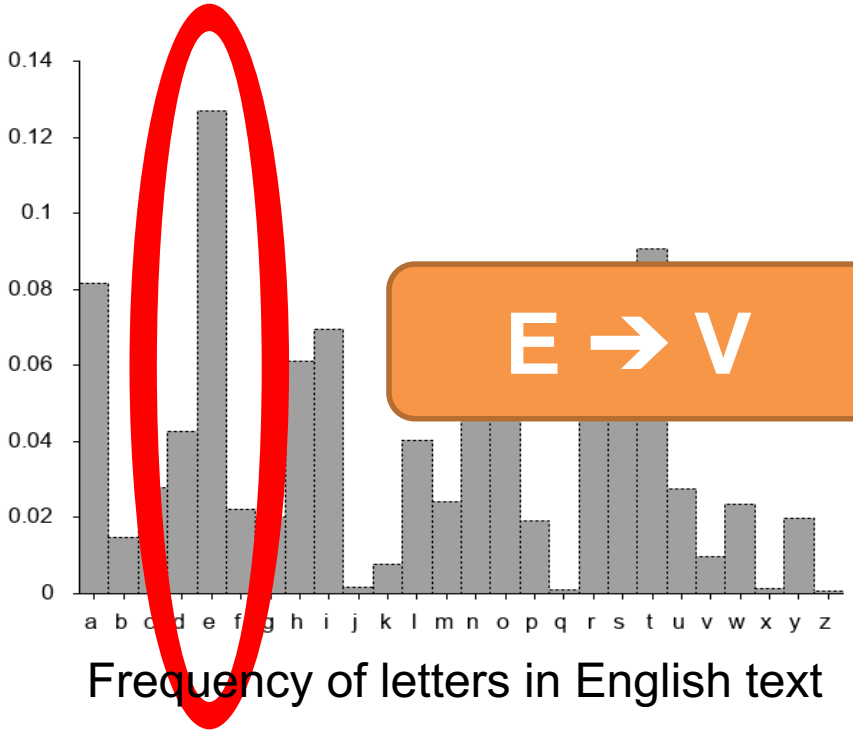
ATTACK AT DAWN

↓

XQQXZH XQ AXTK

Frequency analysis

Zk nrj kyv svjk fw kzdvj, zk nrj kyv nfijk fw kzdvj, zk nrj kyv rxv fw nzjufd, zk nrj kyv rxv fw wffczjyevjj, zk nrj kyv vgfty fw svczvw, zk nrj kyv vgfty fw zetivulczkp, zk nrj kyv jvrjfe fw Czxyk, zk nrj kyv jvrjfe fw Uribevjj, zk nrj kyv jgizex fw yfgv, zk nrj kyv nzekvi fw uvjgrzi, nv yru vmvipkyzex svwfiv lj, nv yru efkyzex svwfiv lj, nv nviv rcc xfzex uzivtk kf Yvrmve, nv nviv rcc xfzex uzivtk kyv fkyvi nrp—ze jyfik, kyv gvizfu nrj jf wri czbv kyv givjvek gvizfu, kyrk jfdv fw zkj efzjzvjk rlkyfizkzvj zejzjkvu fe zkj svzex ivtvzmvu, wfi xffu fi wfi vmzc, ze kyv jlgvicrkzmv uvxivv fw tfdgrizjfe fecp.



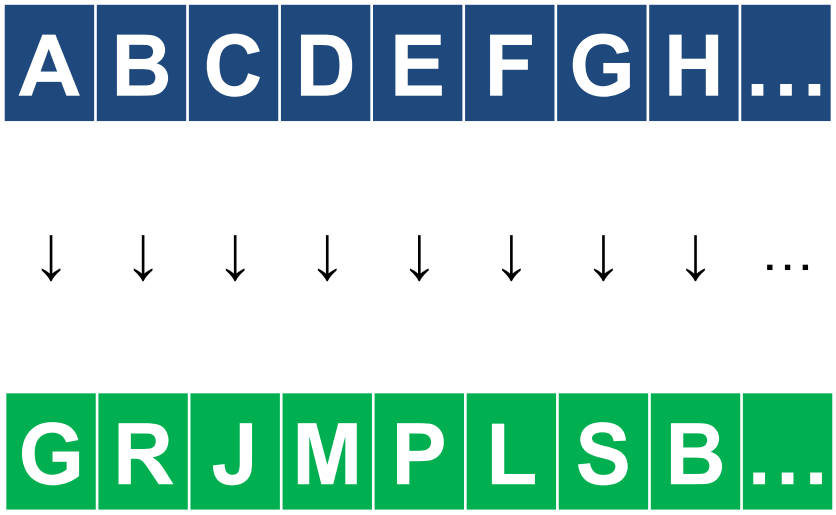
Frequency of letters in English text

E → V shift of 17

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way—in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only.

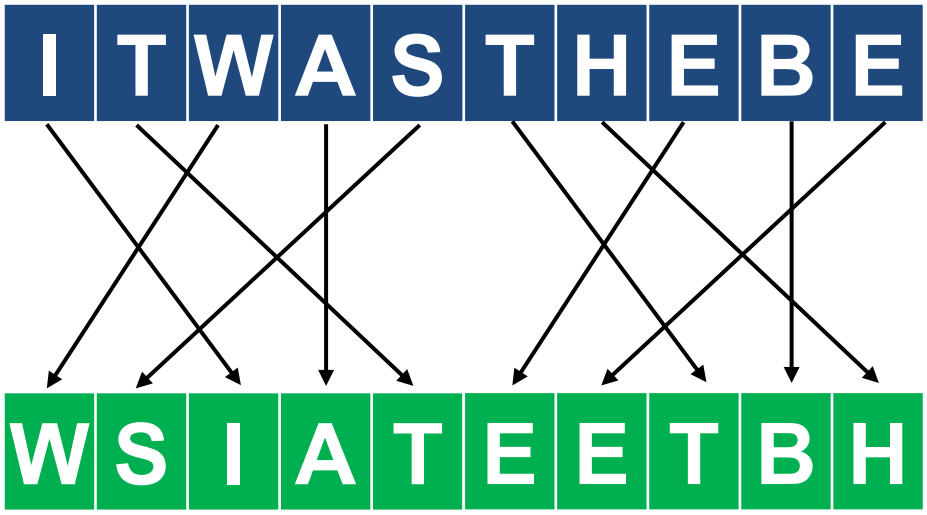
Substitutions

- **Replace each letter** according to a pre-defined table



Permutations

- **Rearrange the letters** according to a pre-defined pattern



Substitutions

- **Replace each letter** according to a pre-

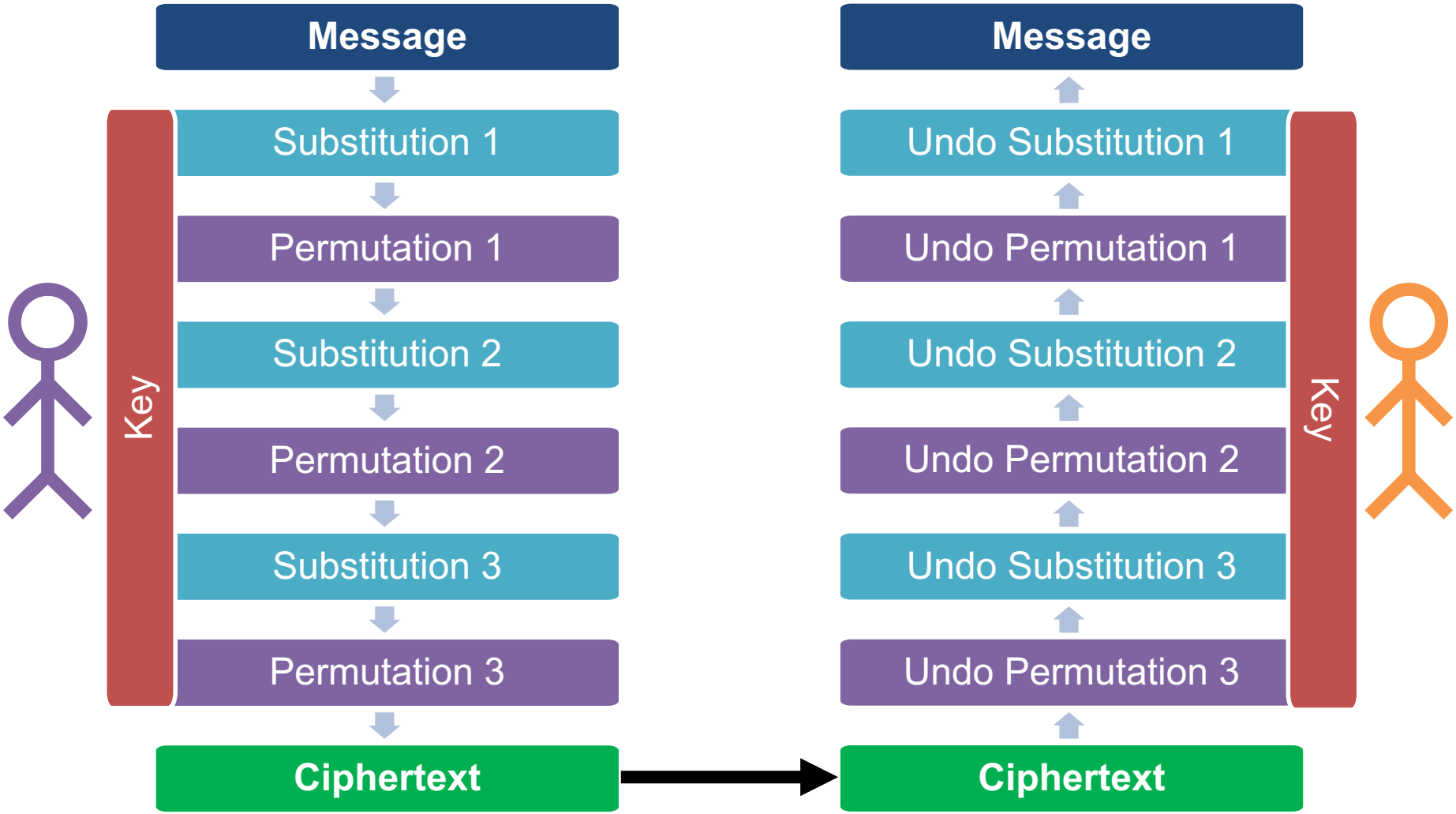
Permutations

- **Rearrange the letters** according to a

rn

Still vulnerable to statistical analysis

Making it harder



Kerckhoff's Principles – 1883

Security should not depend on keeping the design of the system secret.

Only a (small) key should have to be kept secret.

World War II – The Engima Machine

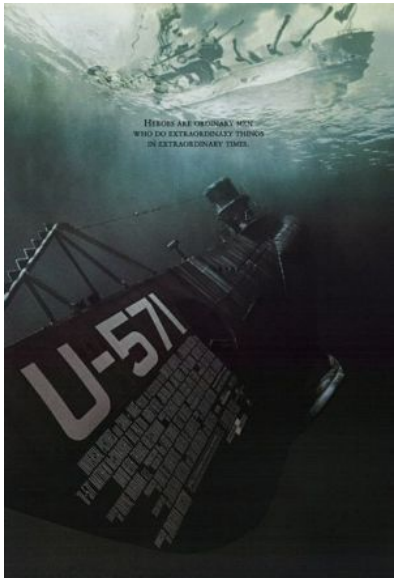
- Electrical wirings lead to a sequence of permutations and substitutions, updated with each letter typed

https://en.wikipedia.org/wiki/Enigma_machine

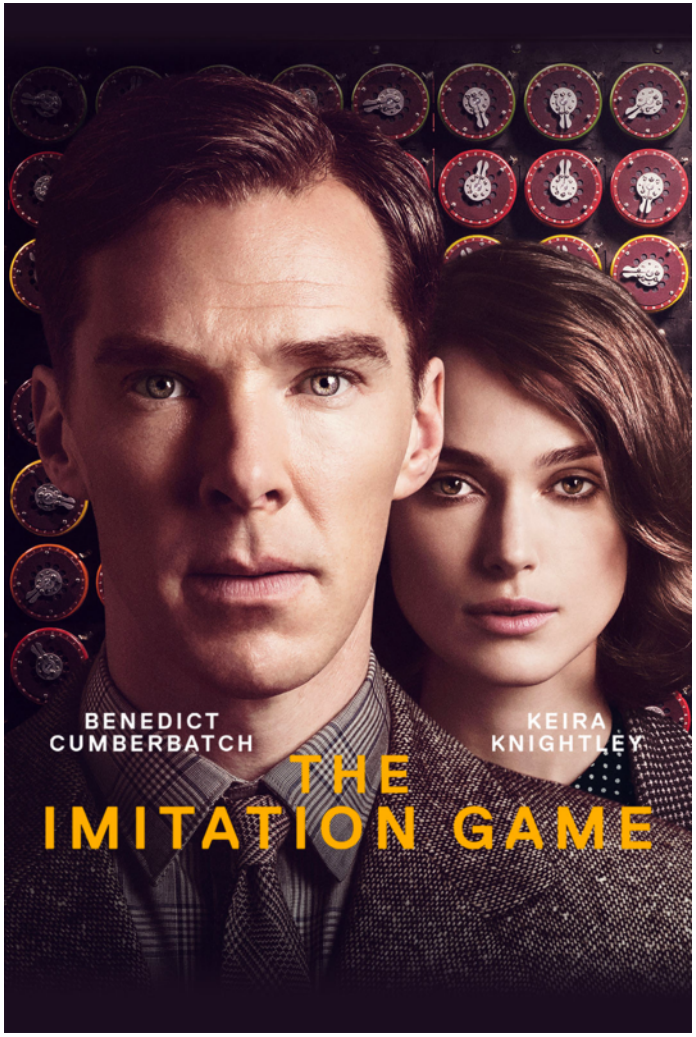
World War II – The Engima Machine

https://en.wikipedia.org/wiki/Enigma_machine

- Initial dial positions were set based on a key for the day
- Keys distributed in codebooks from headquarters
- **Keys had to be kept secret!**
- **Destroy the codebook at all costs!**



One of the first electronic computers



https://en.wikipedia.org/wiki/Bombe

Modern cryptography

1975 – present

1970s – Birth of modern cryptography

- 1975–1977: US government publishes Data Encryption Standard (DES)
  - First government cipher for public use

1970s – Birth of modern cryptography

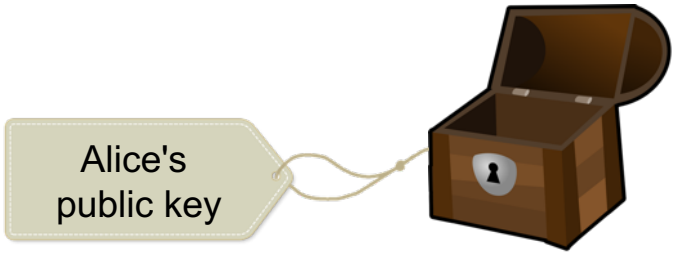
- 1976: Diffie, Hellman, and Merkle invent **public key cryptography**
  - Two parties can communicate privately without having to share a secret key in advance

Public key cryptography

- A pair of related keys:
  - public key
  - private key
- Publish the public key
- Anyone can use the public key to encrypt
- Only the person with the private key can decrypt

public key

private key



encrypt a message

Public key cryptography

- A pair of related keys:
  - public key
  - private key
- Publish the public key
- Anyone can use the public key to encrypt
- Only the person with the private key can decrypt

We need a mathematical function

(that we can tell everyone)

that's easy to compute but hard to undo.

Some brief mathematics

Modular arithmetic

$9 + 5 = 14$

9am + 5 hrs = 2pm

$9 + 5 \equiv 2 \pmod{12}$

Exponentiation

$5^2 = 25$

$5^{17} = 762939453125$

$5^2 \equiv 1 \pmod{12}$

$5^{17} \equiv 5 \pmod{12}$

Rabin public key encryption

Key generation

1. Pick two big prime numbers p and q
2. Compute $n = p \times q$
3. Public key: n
4. Private key: p and q

Encryption

1. Let the message m be a number between 1 and n
2. Ciphertext: $c \equiv m^2 \pmod{n}$

Rabin public key encryption

Key generation

1. Pick two big prime numbers p and q
2. Compute $n = p \times q$
3. Public key: n
4. Private key: p and q

Decryption

1. Compute $m \equiv \text{sqrt}(c) \pmod{n}$

   (Need to use p and q to compute square roots modulo n.)

Is it hard to break the encryption?

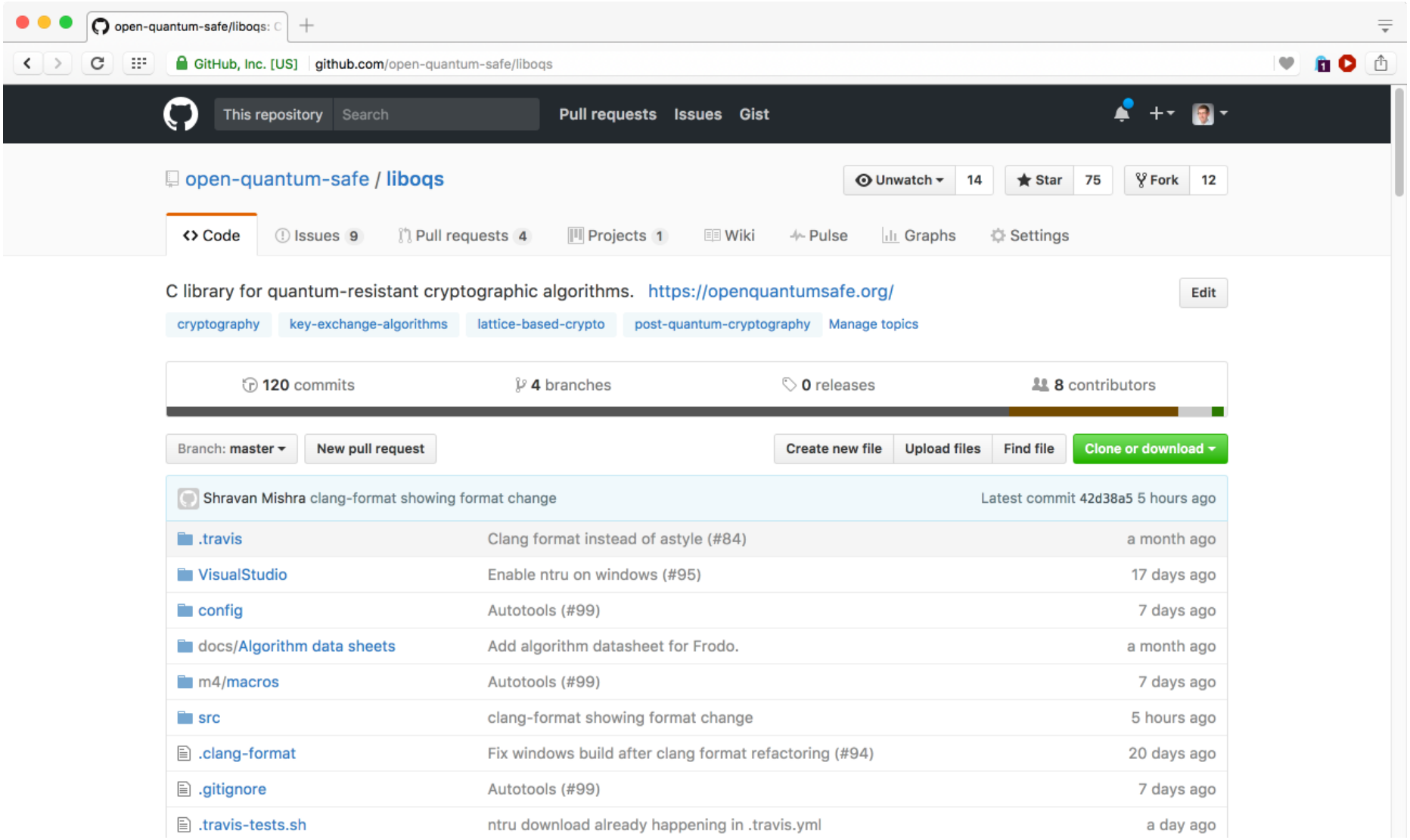
If it is hard to split n
into its prime factors p and q,

then it is hard
to decrypt the ciphertext.

Is it hard to factor *n*?

- Maybe?
- The fastest algorithm we have is really slow.
- For the size of *n* we use today on the Internet, all the computers on Earth would take about **1 billion years** to break the encryption.
- **Quantum computers** (which represent information using quantum mechanics rather than 0s and 1s), could factor efficiently.
- So we need "quantum-resistant" cryptography.

Post-quantum cryptography at McMaster



Cryptography for privacy and security

Disk encryption

Automatically encrypt all files on your hard drive.

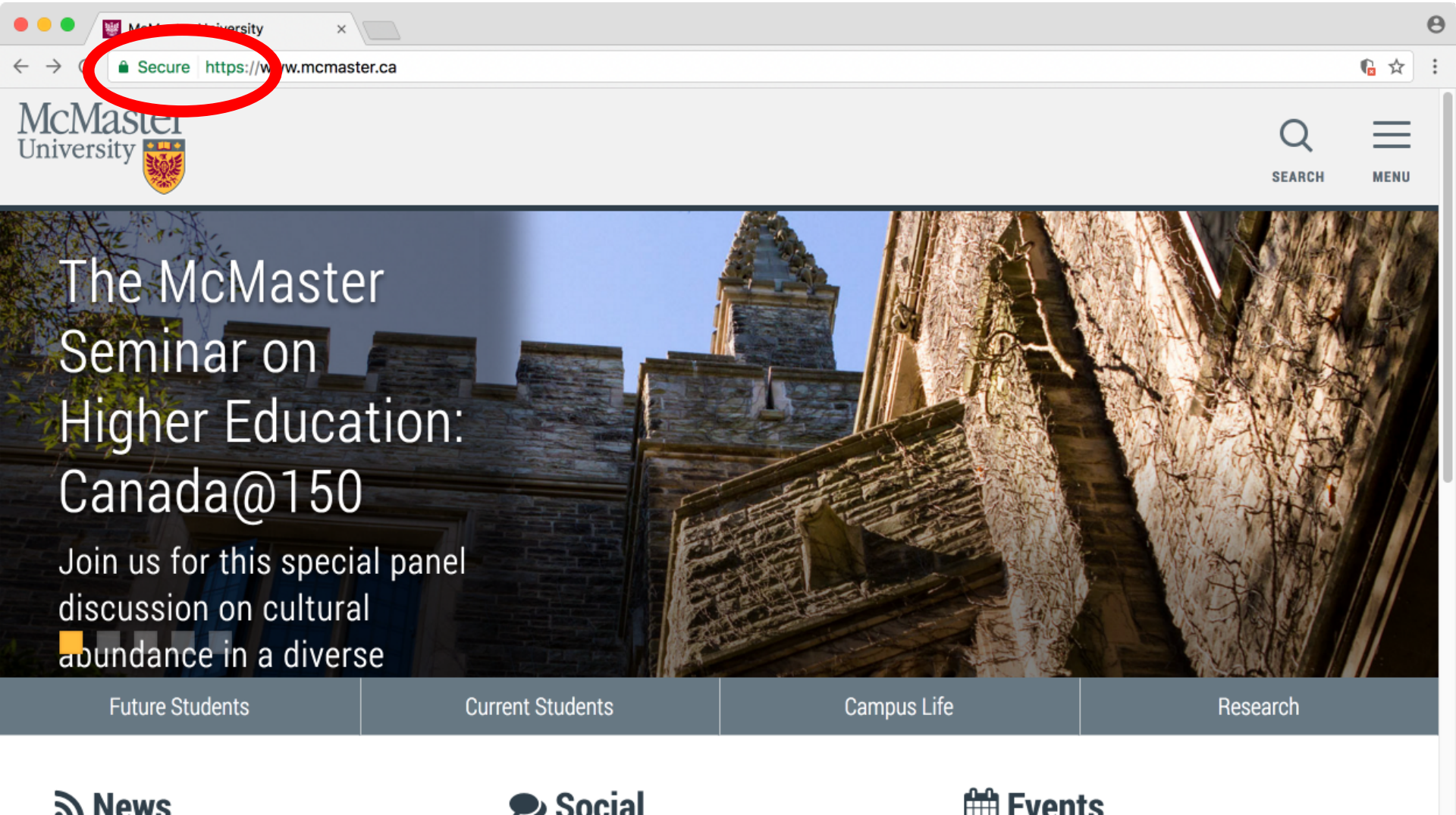
- But key derived from your password
  - Weak password => weak key
  - Forget password => locked out

- macOS: optional (FileVault)
- Windows: optional (BitLocker)
- Linux: optional

- iOS: automatic
- Android: versions 5+

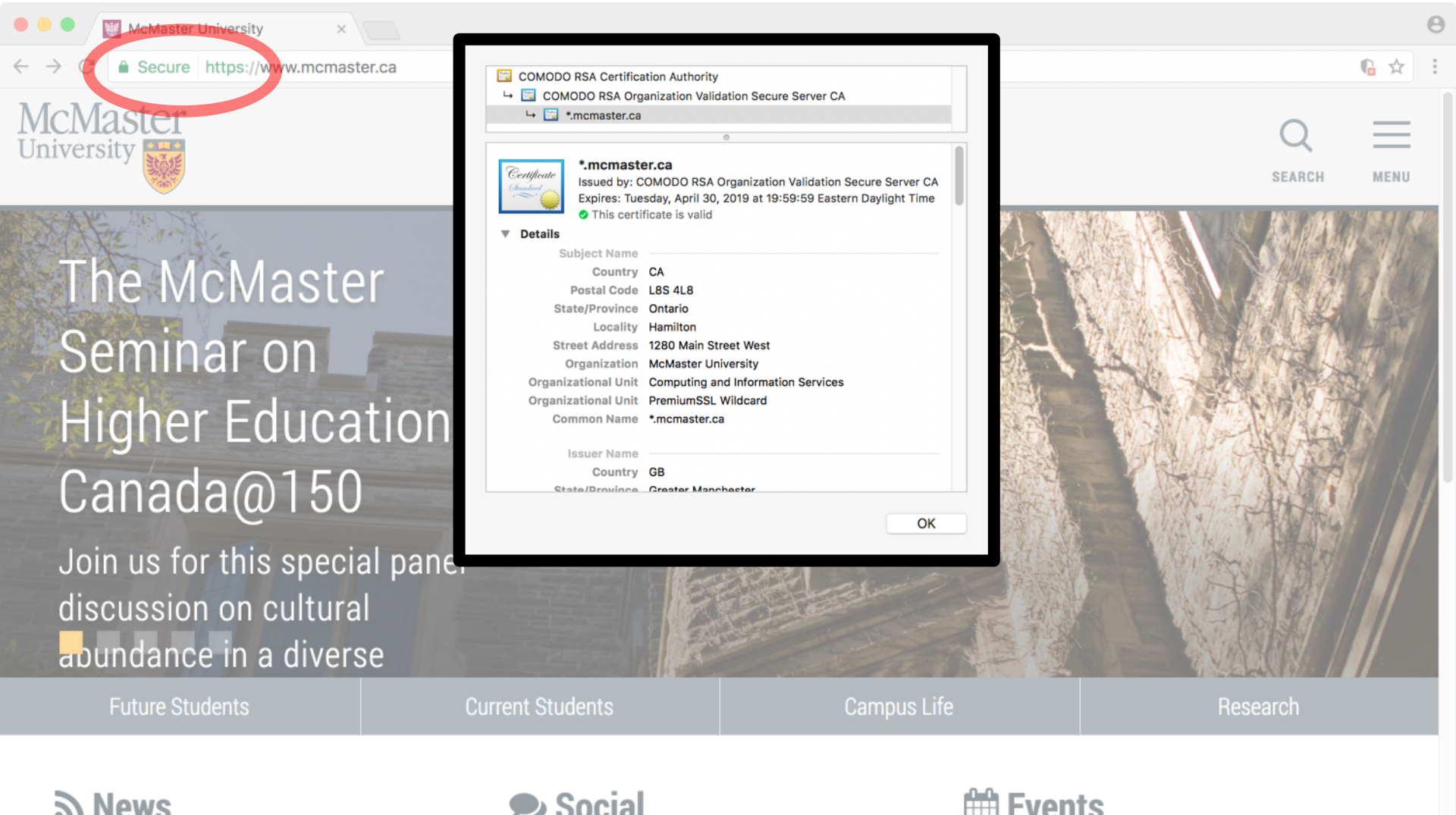
Transport Layer Security

a.k.a. HTTPS



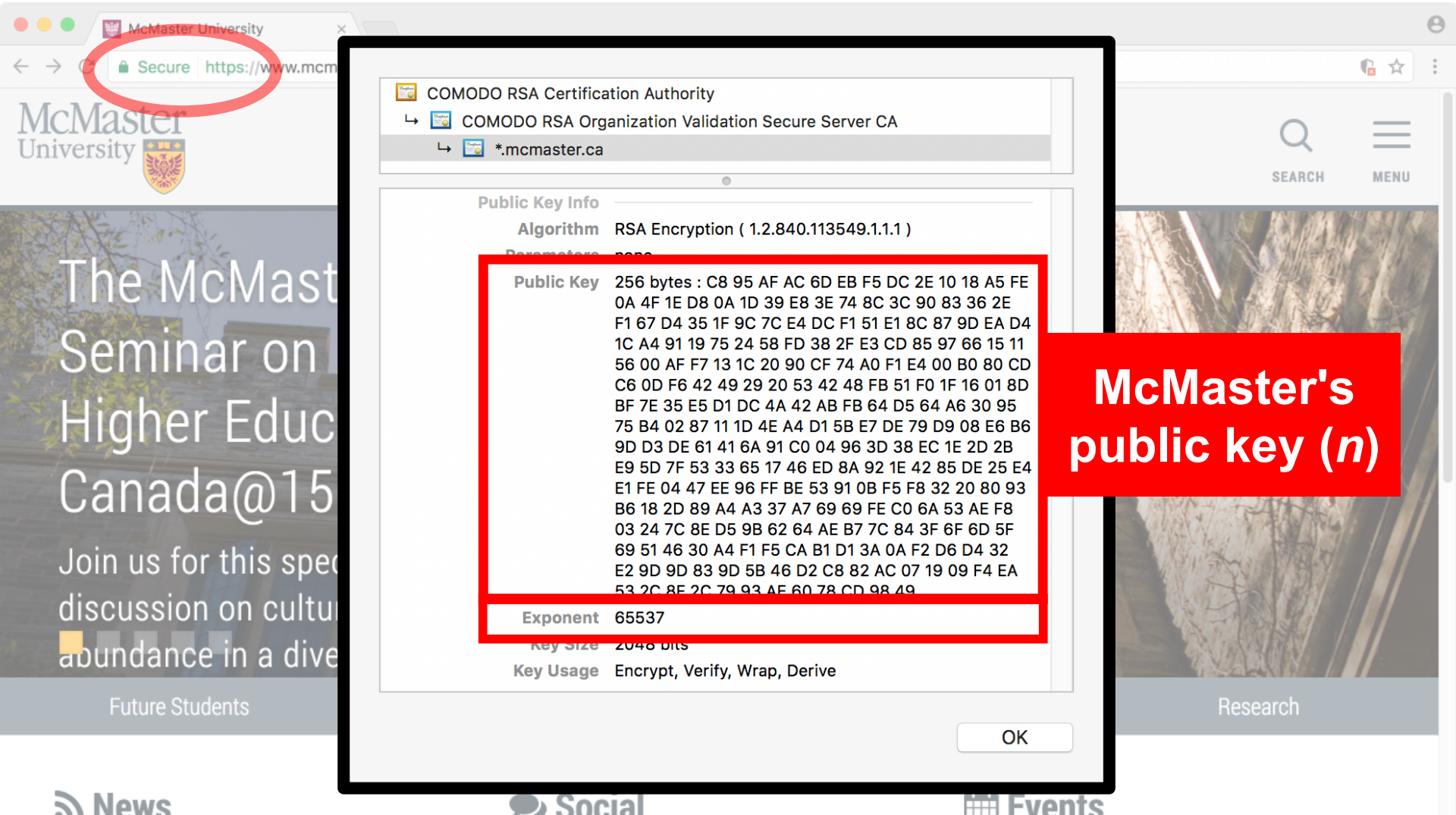
Transport Layer Security

a.k.a. HTTPS



Transport Layer Security

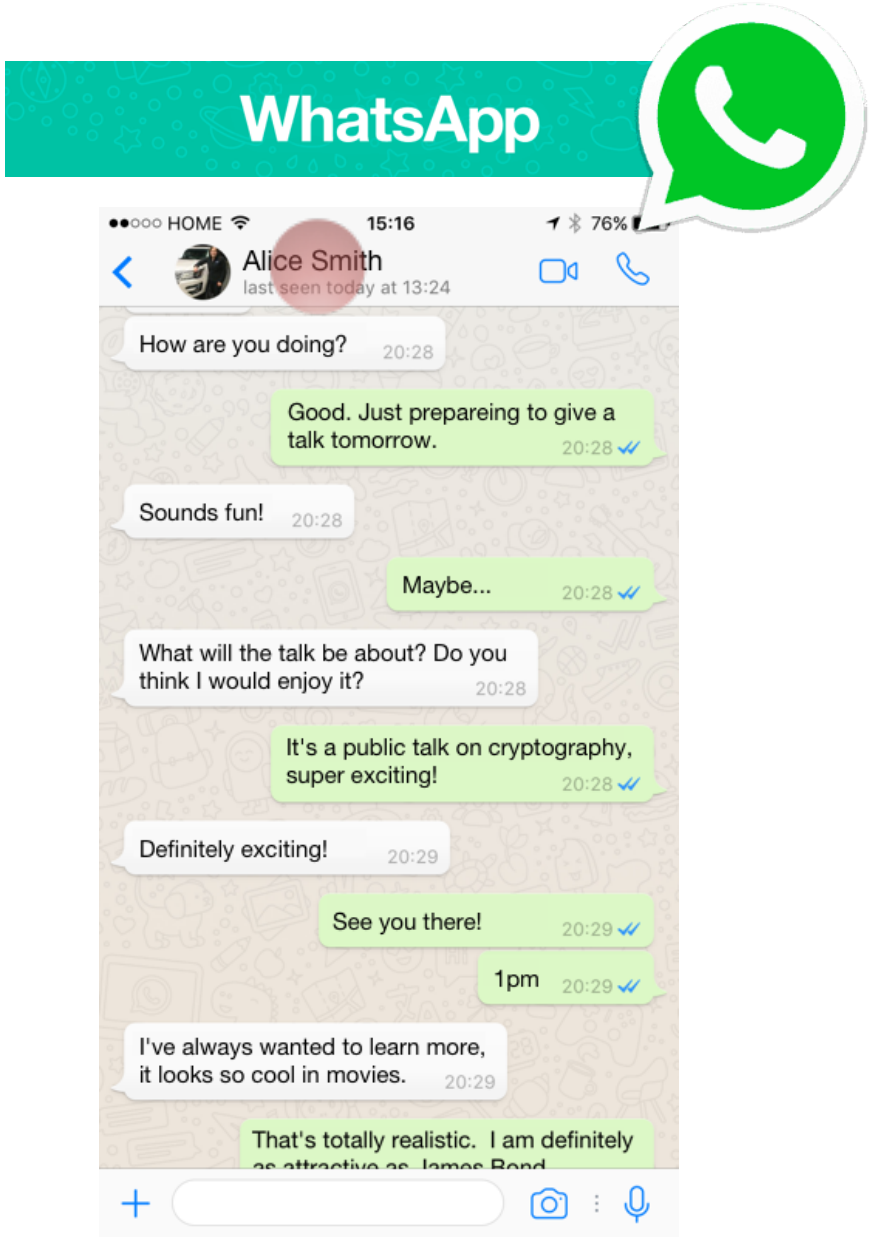
a.k.a. HTTPS



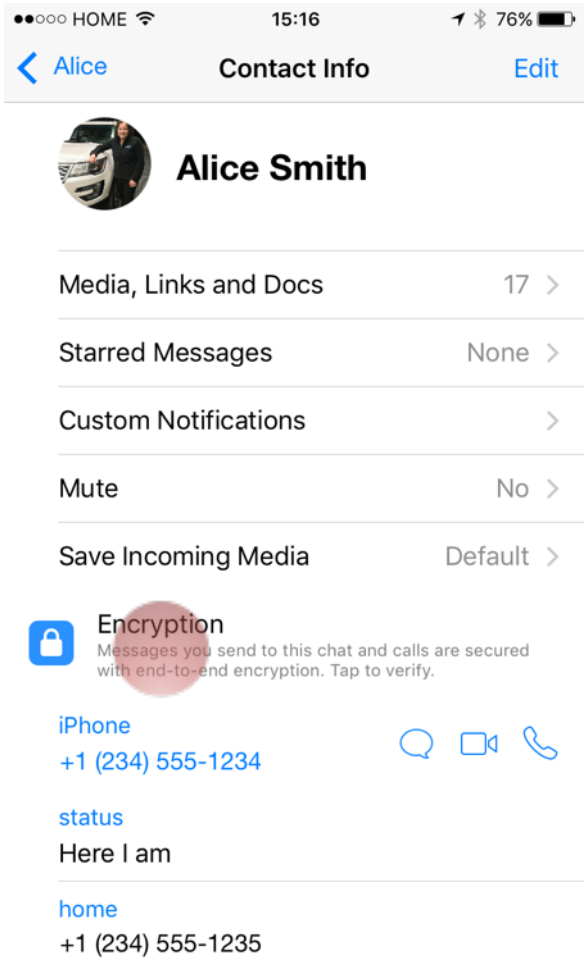
Encrypted instant messaging

Signal protocol

- Encrypts instant messaging for more than a billion users
  - Used in WhatsApp, Facebook Messenger, Google Allo, …



Encrypted instant messaging



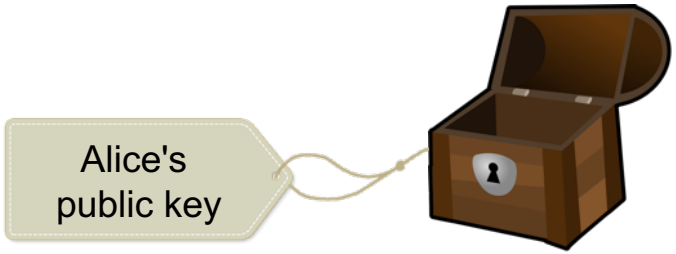
Alice's public key

Public key cryptography

public key

private key

How do you know this is really Alice's public key?

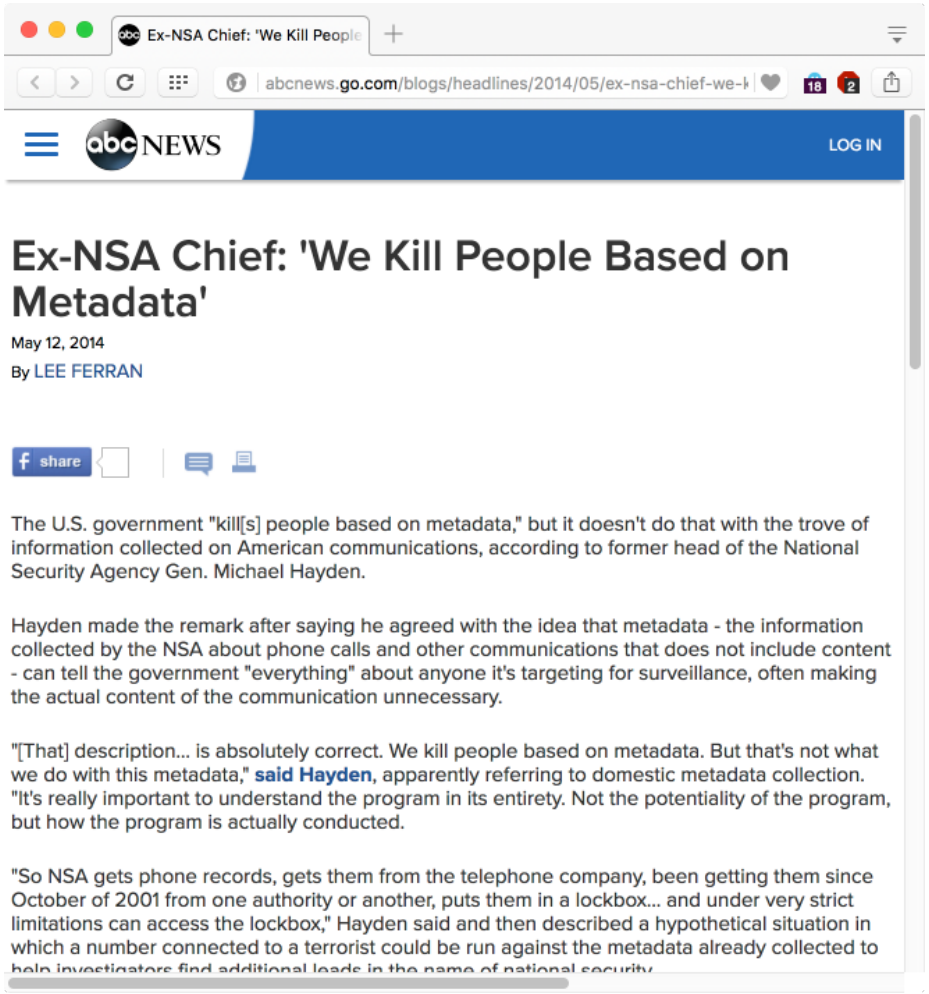


encrypt a message

Encrypted instant messaging

Metadata: "Data about data"

- Telephone
  - Who you're calling
  - When, how long, location (mobile)
  - => But not recording
- Email
  - Email address of recipient
  - When, size
  - => But not body of email
- Web
  - Address of server you're browsing
  - When, duration, size
  - => But not contents of web page



http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/
http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/

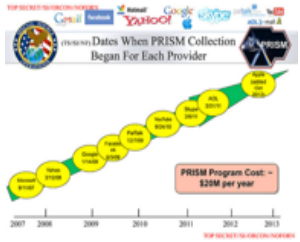
anonymity network

- Hides metadata and content
- Obscures traffic patterns

- Used by
  - journalists
  - whistleblowers
  - dissidents
  - activists
  - law enforcement
  - privacy-conscious citizens
  - … criminals

Metadata leakage on the Internet

131.181.46.152



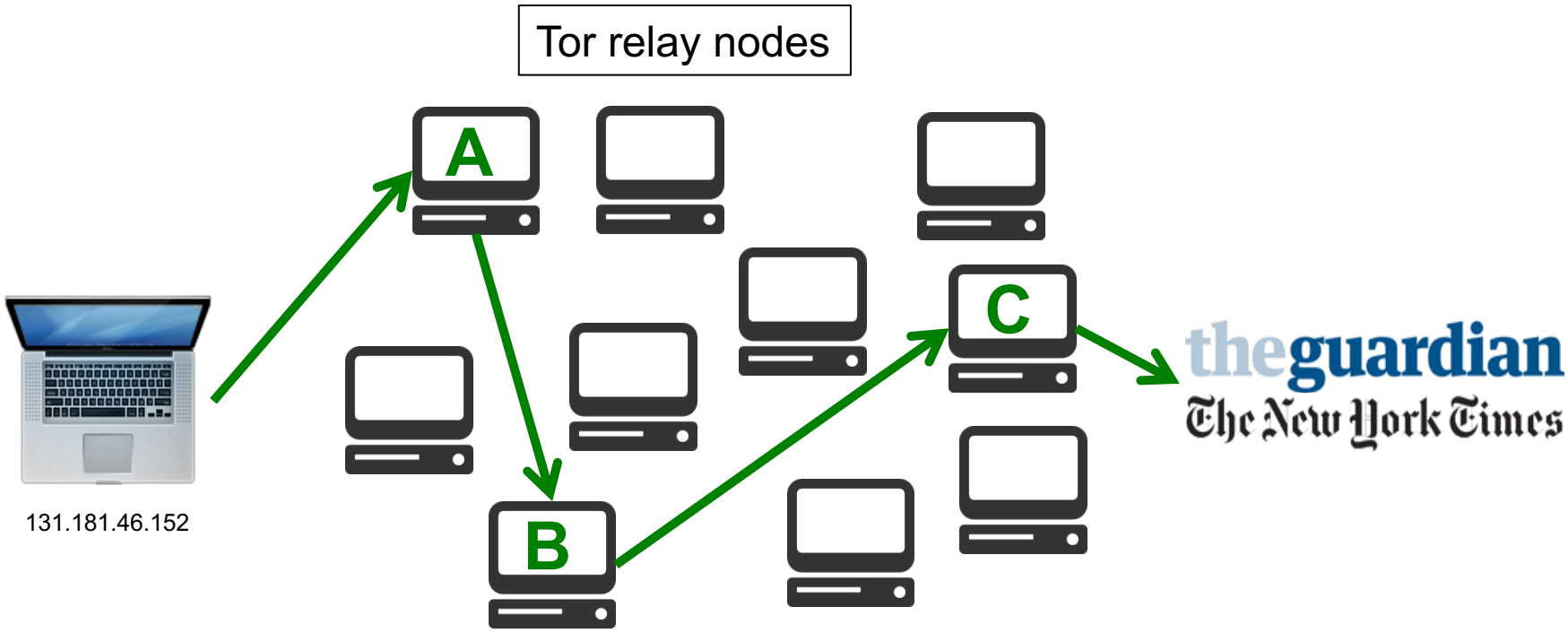
This came from 131.181.46.152

theguardian
The New York Times

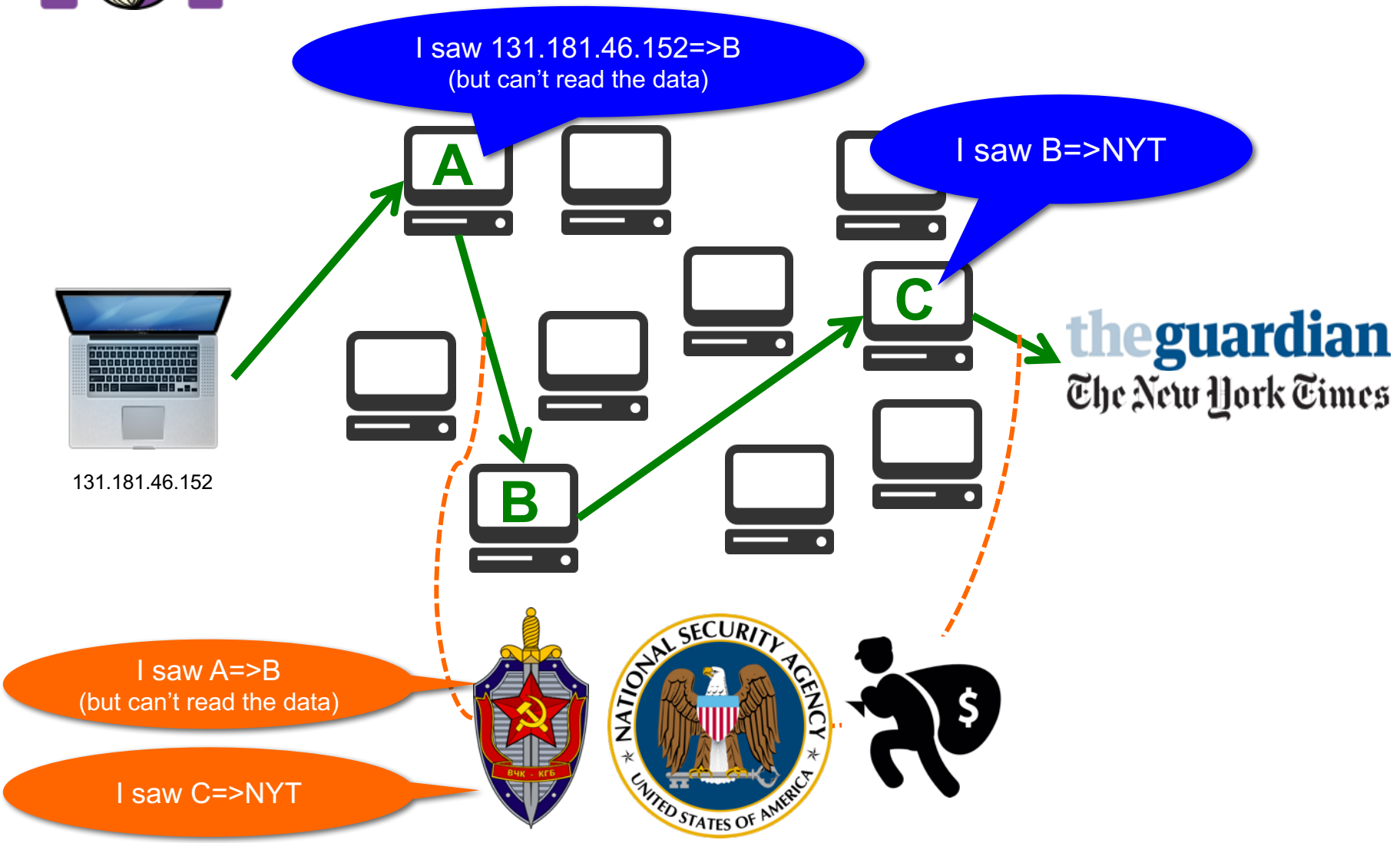
I saw 131.181.46.152 communicate with NYT

Bell
McMaster University

anonymity network



anonymity network



+ can't tell these two facts are linked

Things you can do to improve your privacy and security online

Things you can do

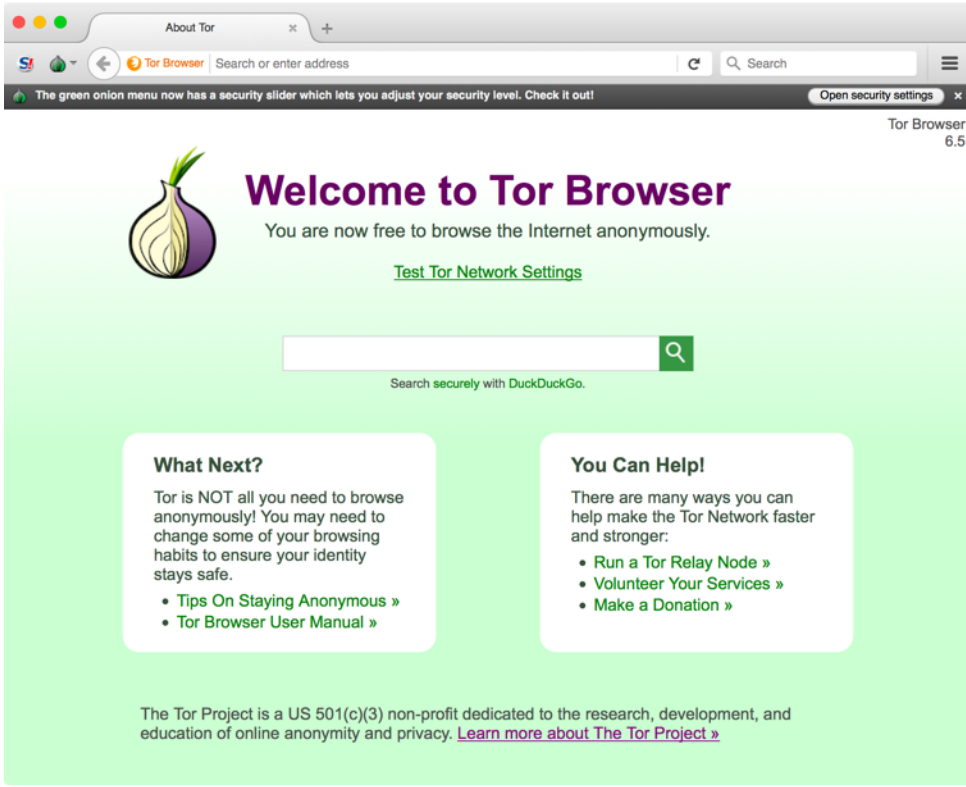
Passwords

- For really important sites (bank, email), pick completely random passwords and don't use them elsewhere.

Things you can do

Untrusted networks

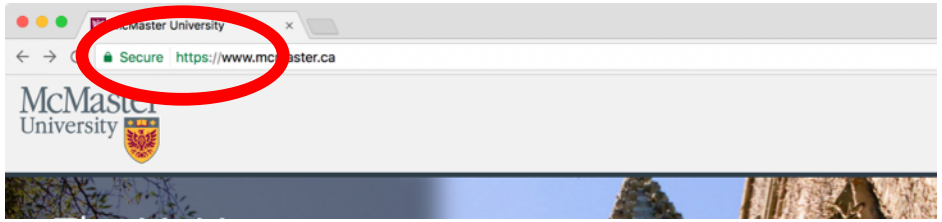
- On untrusted wi-fi networks (coffee shops, airports, hotels), consider using a **virtual private network** or the **Tor browser** for extra privacy.



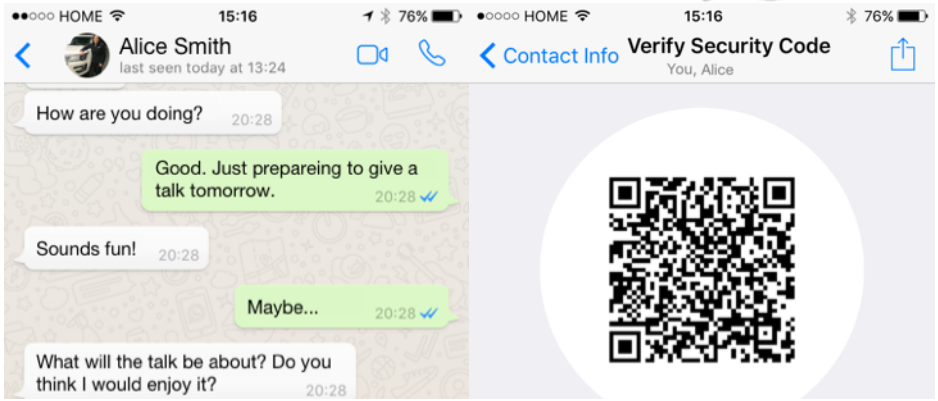
https://www.torproject.org

Things you can do

Web browsing



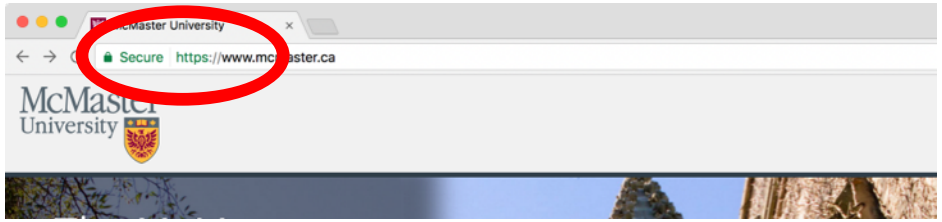
Instant messaging



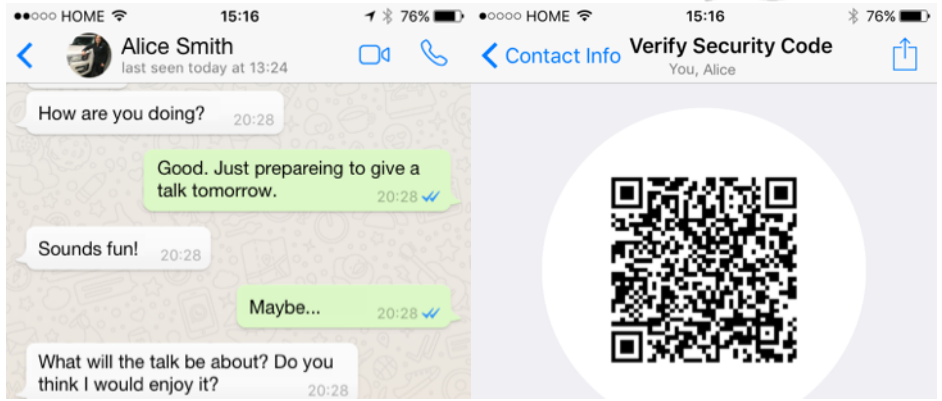
How cryptography protects your information every day

Douglas Stebila
McMaster University
https://www.cas.mcmaster.ca/~stebilad/

Web browsing



Instant messaging



The Code Book

- http://simonsingh.net/books/the-code-book/

'I've Got Nothing to Hide' and Other Misunderstandings of Privacy

- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

Surveillance Self-Defense

- https://ssd.eff.org

Schneier on Security

- https://www.schneier.com