

# How cryptography protects your information every day

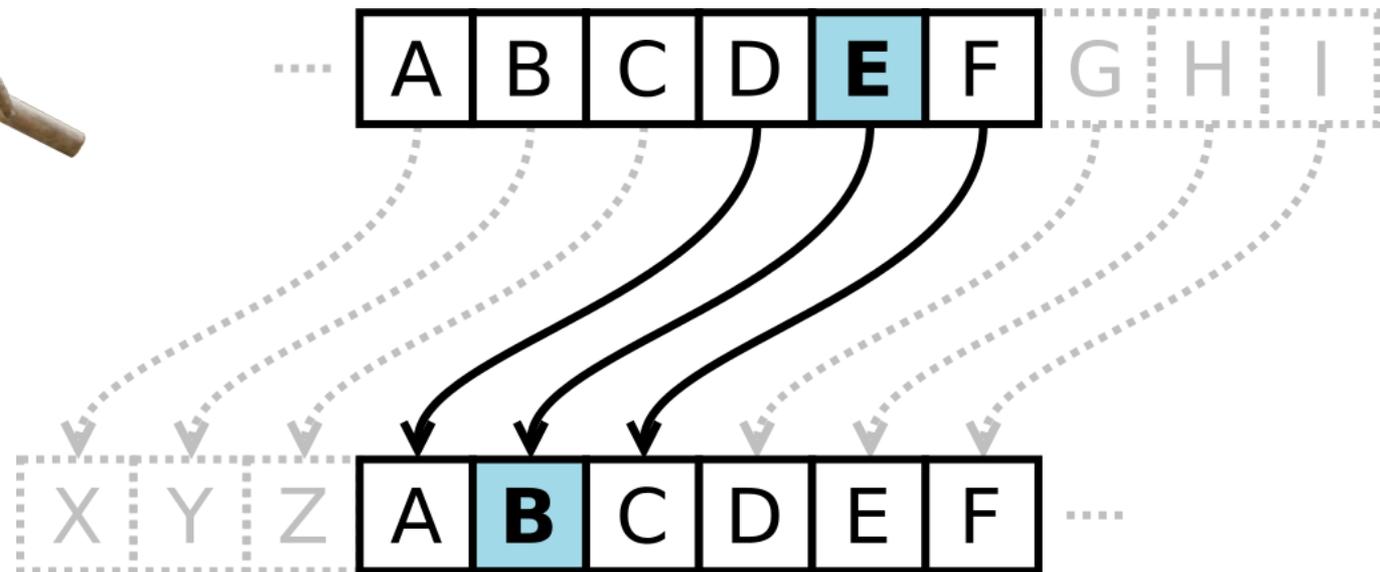
---

**Douglas Stebila**  McMaster University

Funding acknowledgements:



# Caesar cipher





# Caesar cipher

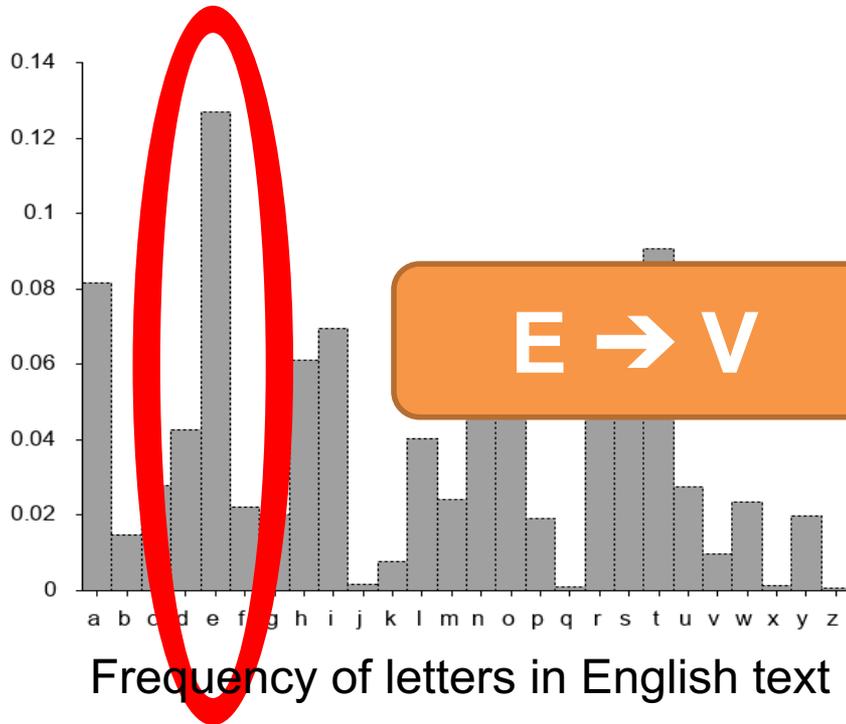
**ATTACK AT DAWN**



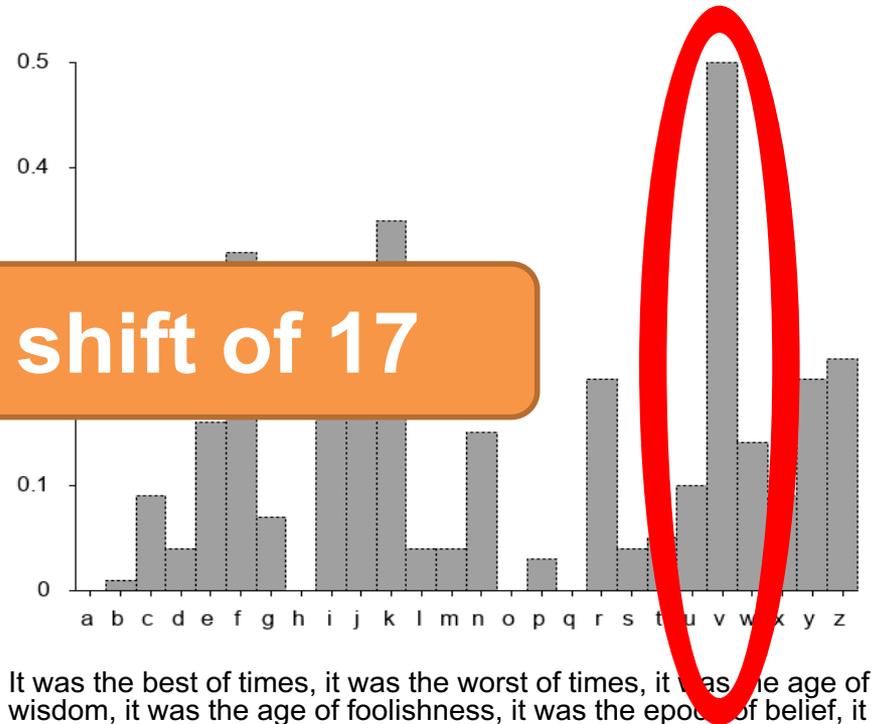
**XQQXZH XQ AXTK**

# 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 wfczjyevjj, 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 swwfv lj, nv yru efkyzex swwfv 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 efzjzvj rkyfizkzvj zejzjkvu fe zkj svzex ivtvzmvu, wfi xffu fi wfi vmzc, ze kyv jlgvicrkzmv uvxivv fw tfdgrizjfe fecp.



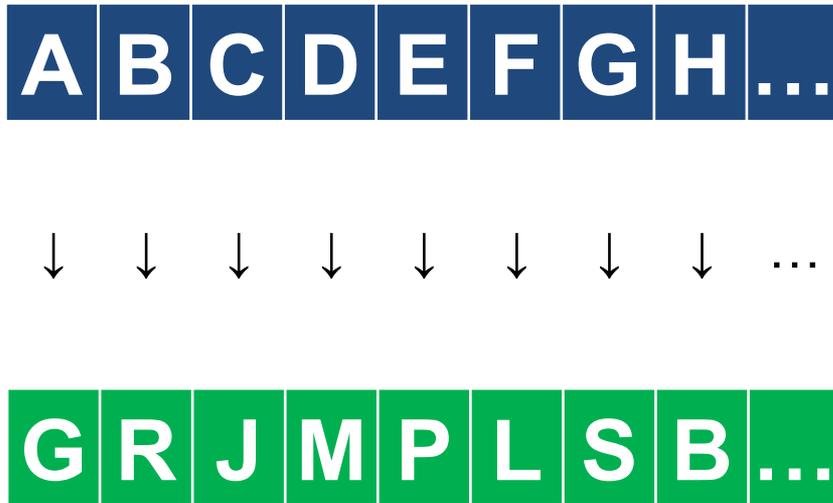
**E → V**      **shift of 17**



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.

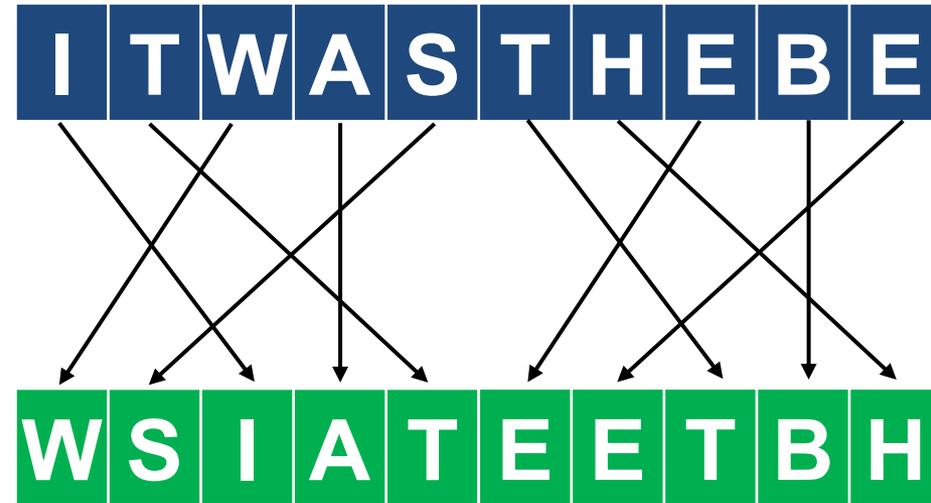
# Substitutions

- **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-defined substitution

# Permutations

- **Rearrange the letters** according to a

**Still vulnerable to statistical analysis**

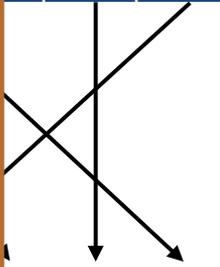
A B



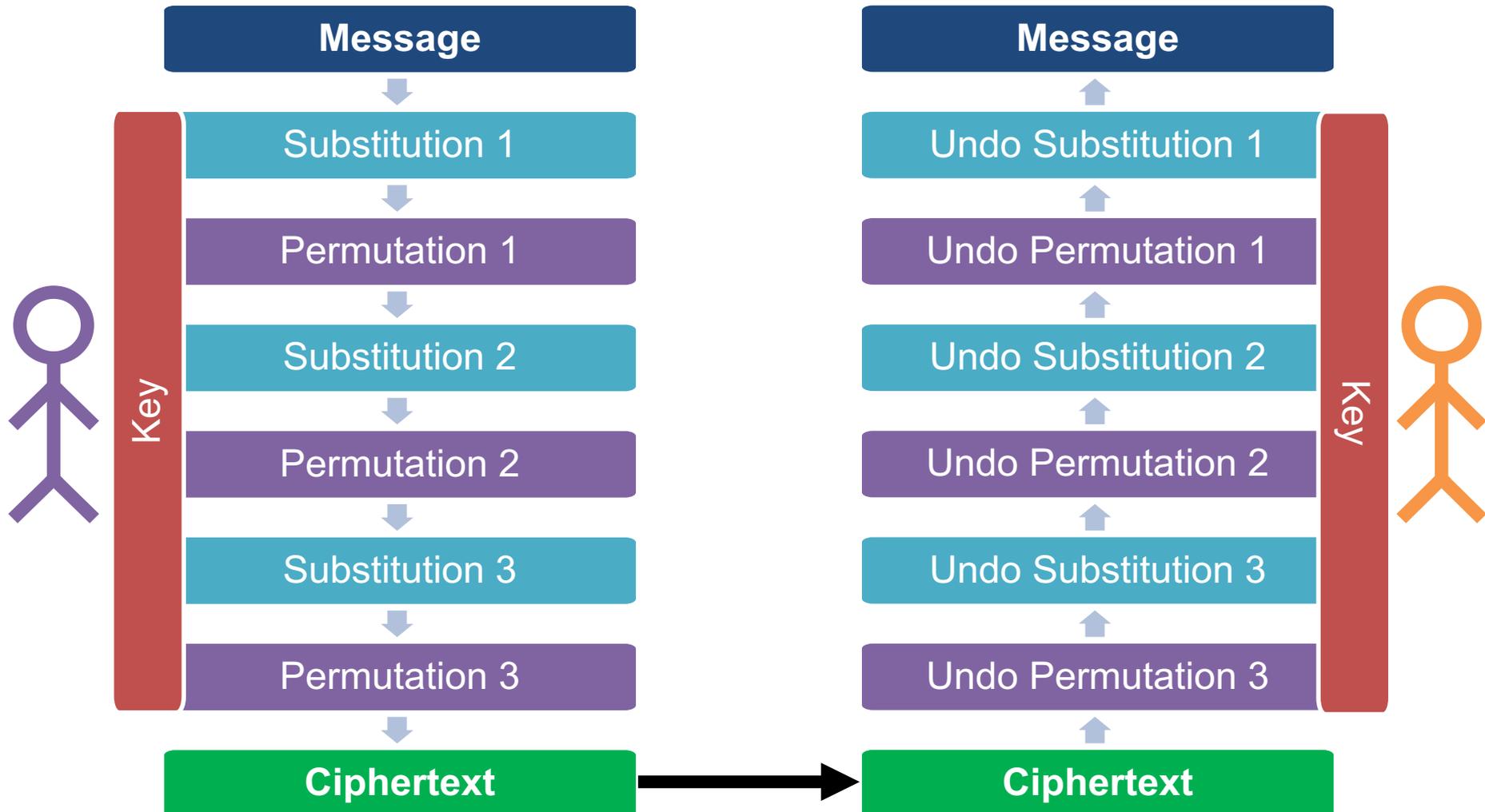
G R

E B E

F B H



# 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 Enigma Machine



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

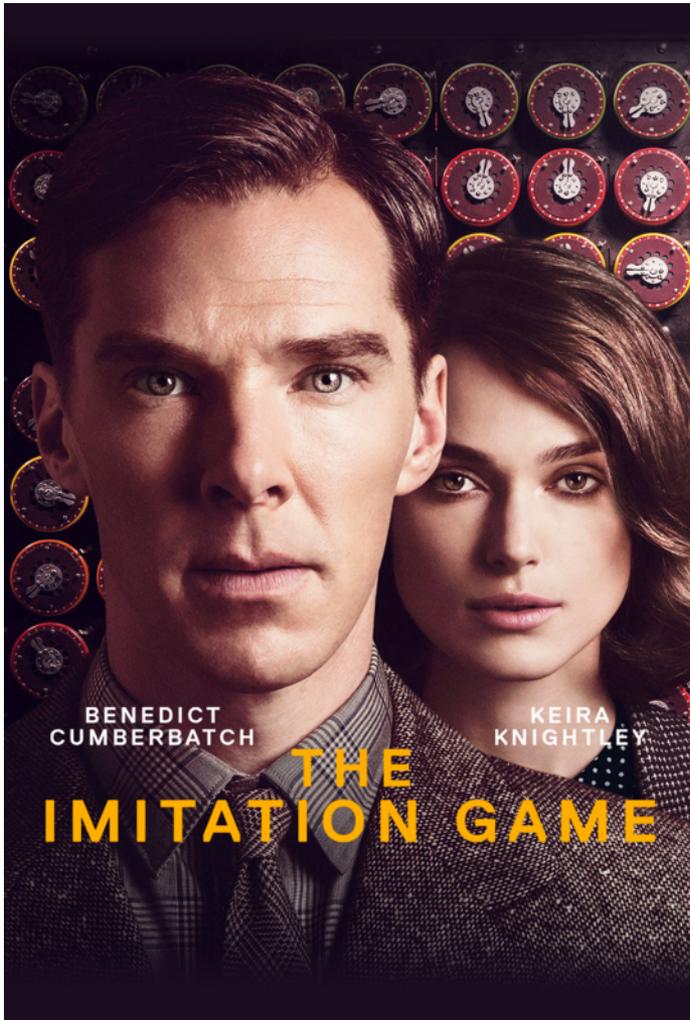
# World War II – The Enigma Machine



- 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



# 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

$$9 + 5 = 14$$



$$9\text{am} + 5 \text{ hrs} = 2\text{pm}$$

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

## 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

The screenshot shows the GitHub repository page for 'open-quantum-safe/liboqs'. The browser address bar shows 'github.com/open-quantum-safe/liboqs'. The repository name is 'open-quantum-safe / liboqs'. It has 14 Unwatch, 75 Star, and 12 Fork actions. The repository is a C library for quantum-resistant cryptographic algorithms, with a link to 'https://openquantumsafe.org/'. The repository has 120 commits, 4 branches, 0 releases, and 8 contributors. The current branch is 'master'. There are buttons for 'New pull request', 'Create new file', 'Upload files', 'Find file', and 'Clone or download'. The file list includes:

File/Folder	Description	Last Commit
Shravan Mishra clang-format showing format change		Latest commit 42d38a5 5 hours ago
.travis	Clang format instead of astyle (#84)	a month ago
VisualStudio	Enable ntru on windows (#95)	17 days ago
config	Autotools (#99)	7 days ago
docs/Algorithm data sheets	Add algorithm datasheet for Frodo.	a month ago
m4/macros	Autotools (#99)	7 days ago
src	clang-format showing format change	5 hours ago
.clang-format	Fix windows build after clang format refactoring (#94)	20 days ago
.gitignore	Autotools (#99)	7 days ago
.travis-tests.sh	ntru download already happening in .travis.yml	a day ago

# 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



The screenshot shows a web browser window with the address bar containing "Secure https://www.mcmaster.ca". A red circle highlights the "Secure" text. The page header includes the McMaster University logo and navigation links for "SEARCH" and "MENU".

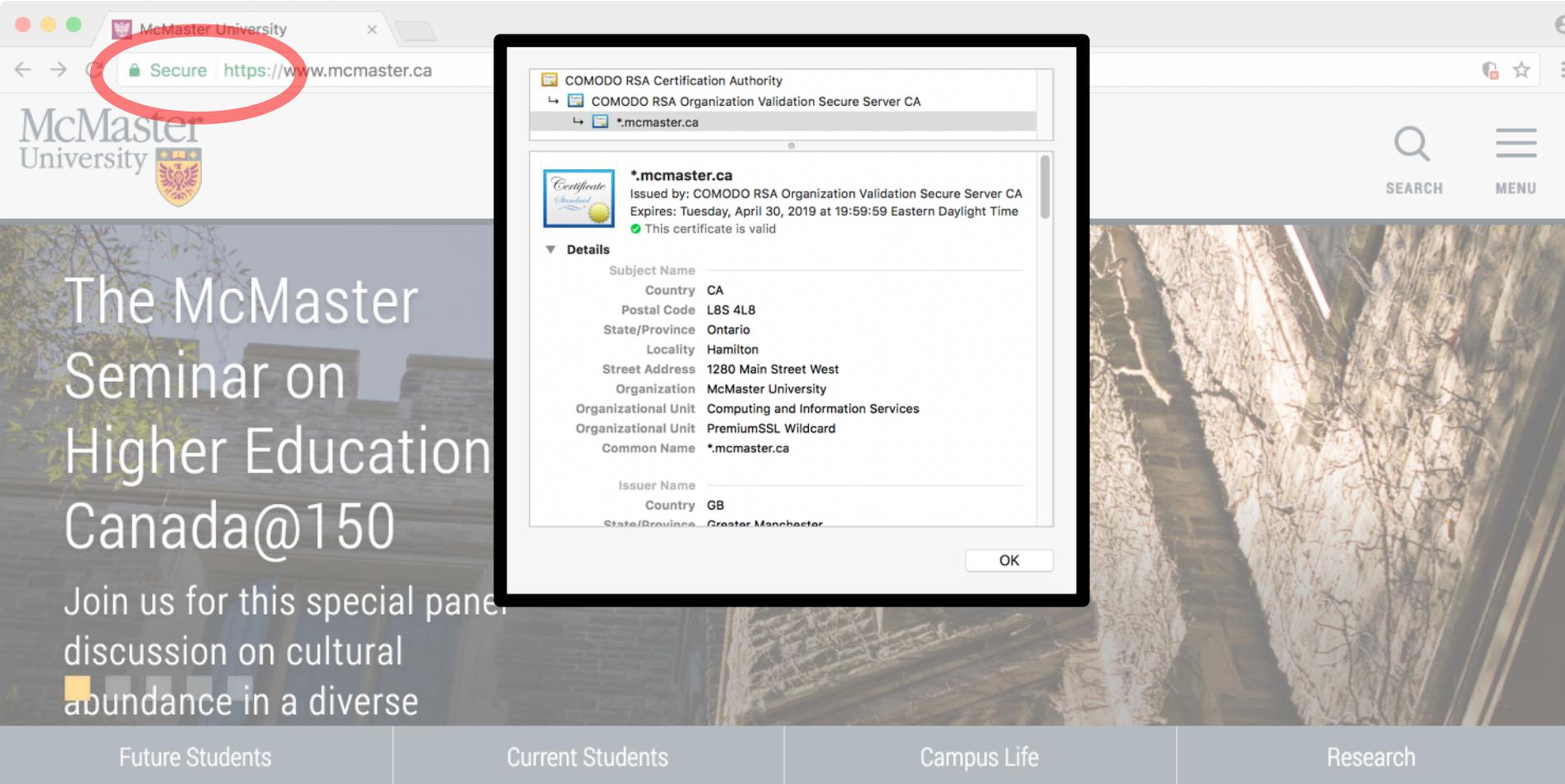
## The McMaster Seminar on Higher Education: Canada@150

Join us for this special panel discussion on cultural abundance in a diverse

Future Students    Current Students    Campus Life    Research

# Transport Layer Security

a.k.a. HTTPS



The image shows a web browser window with the address bar displaying "Secure https://www.mcmaster.ca". A red circle highlights the "Secure" and "https" parts of the address bar. A certificate details popup is overlaid on the browser, showing the following information:

**COMODO RSA Certification Authority**  
COMODO RSA Organization Validation Secure Server CA  
\*.mcmaster.ca

**\*.mcmaster.ca**  
Issued by: COMODO RSA Organization Validation Secure Server CA  
Expires: Tuesday, April 30, 2019 at 19:59:59 Eastern Daylight Time  
This certificate is valid

**Details**

Subject Name	
Country	CA
Postal Code	L8S 4L8
State/Province	Ontario
Locality	Hamilton
Street Address	1280 Main Street West
Organization	McMaster University
Organizational Unit	Computing and Information Services
Organizational Unit	PremiumSSL Wildcard
Common Name	*.mcmaster.ca
Issuer Name	
Country	GB
State/Province	Greater Manchester

OK

The background of the browser window shows the McMaster University logo and a banner for "The McMaster Seminar on Higher Education Canada@150". The banner text reads: "Join us for this special panel discussion on cultural abundance in a diverse". At the bottom of the browser window, there are navigation links for "Future Students", "Current Students", "Campus Life", and "Research".

# Transport Layer Security

a.k.a. HTTPS

McMaster University

Secure https://www.mcm...

COMODO RSA Certification Authority

COMODO RSA Organization Validation Secure Server CA

\*.mcmaster.ca

Public Key Info

Algorithm	RSA Encryption ( 1.2.840.113549.1.1.1 )
Parameters	none
Public Key	256 bytes : C8 95 AF AC 6D EB F5 DC 2E 10 18 A5 FE 0A 4F 1E D8 0A 1D 39 E8 3E 74 8C 3C 90 83 36 2E F1 67 D4 35 1F 9C 7C E4 DC F1 51 E1 8C 87 9D EA D4 1C A4 91 19 75 24 58 FD 38 2F E3 CD 85 97 66 15 11 56 00 AF F7 13 1C 20 90 CF 74 A0 F1 E4 00 B0 80 CD C6 0D F6 42 49 29 20 53 42 48 FB 51 F0 1F 16 01 8D BF 7E 35 E5 D1 DC 4A 42 AB FB 64 D5 64 A6 30 95 75 B4 02 87 11 1D 4E A4 D1 5B E7 DE 79 D9 08 E6 B6 9D D3 DE 61 41 6A 91 C0 04 96 3D 38 EC 1E 2D 2B E9 5D 7F 53 33 65 17 46 ED 8A 92 1E 42 85 DE 25 E4 E1 FE 04 47 EE 96 FF BE 53 91 0B F5 F8 32 20 80 93 B6 18 2D 89 A4 A3 37 A7 69 69 FE C0 6A 53 AE F8 03 24 7C 8E D5 9B 62 64 AE B7 7C 84 3F 6F 6D 5F 69 51 46 30 A4 F1 F5 CA B1 D1 3A 0A F2 D6 D4 32 E2 9D 9D 83 9D 5B 46 D2 C8 82 AC 07 19 09 F4 EA 53 2C 8E 2C 79 93 AF 60 78 CD 98 49
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive

McMaster's public key ( $n$ )

OK

Future Students

Research

News

Social

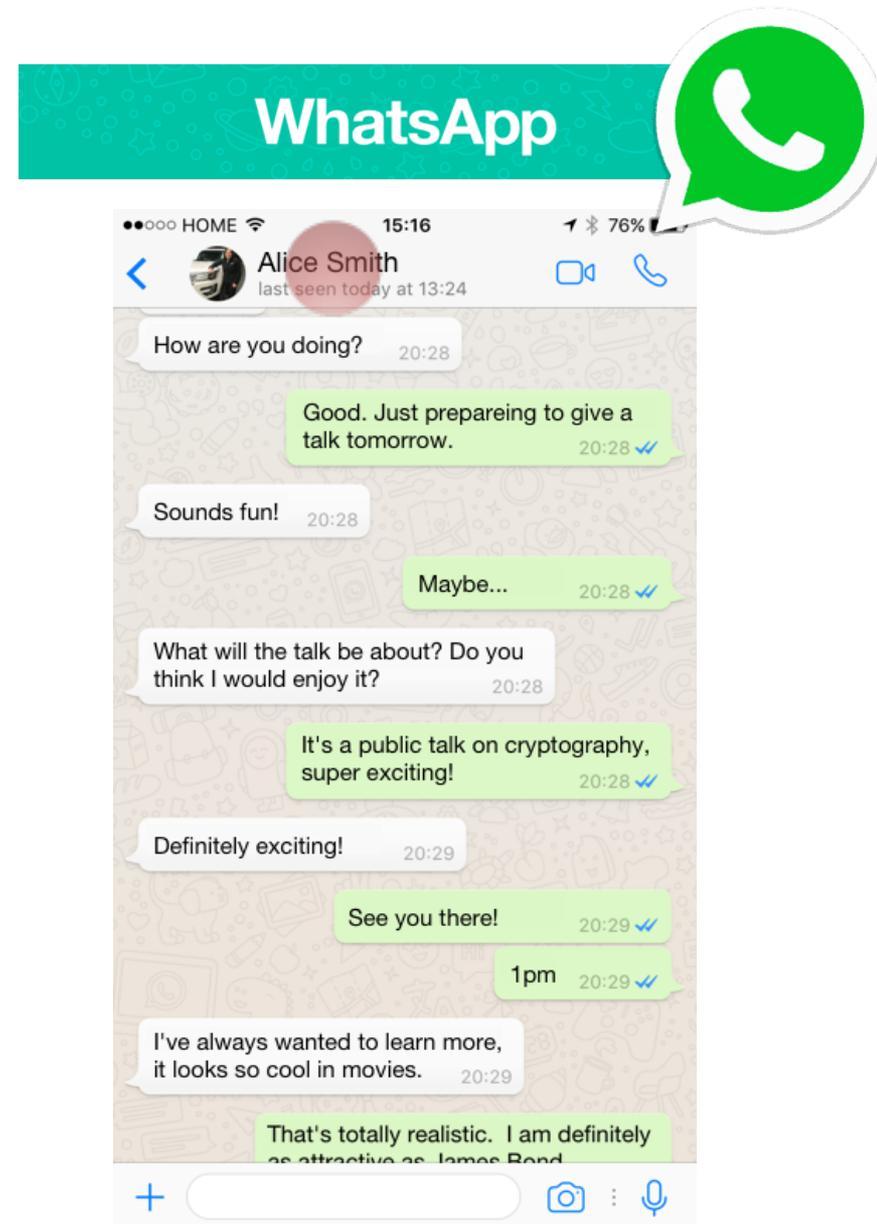
Events

# Encrypted instant messaging

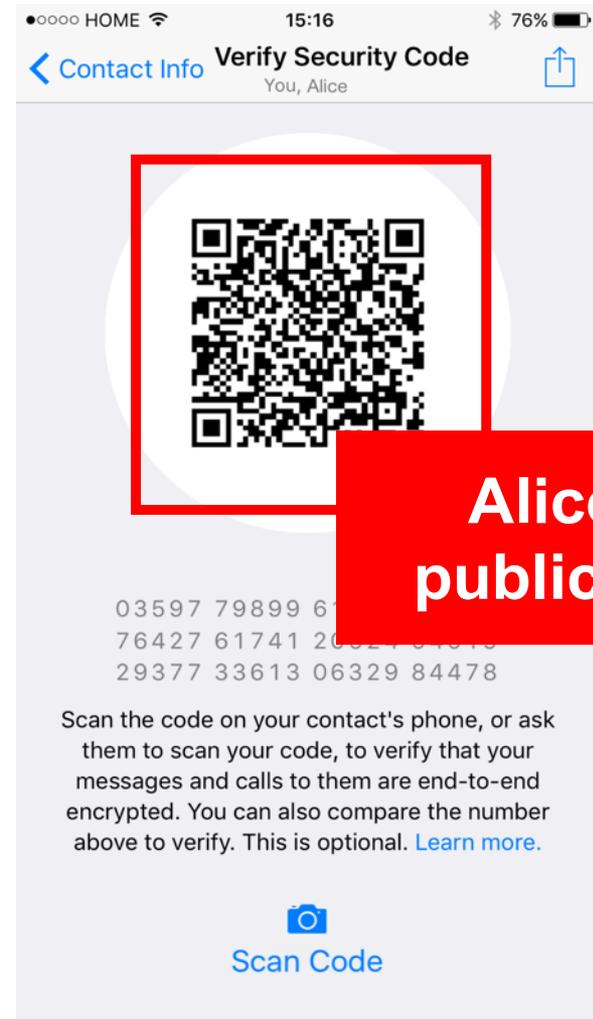
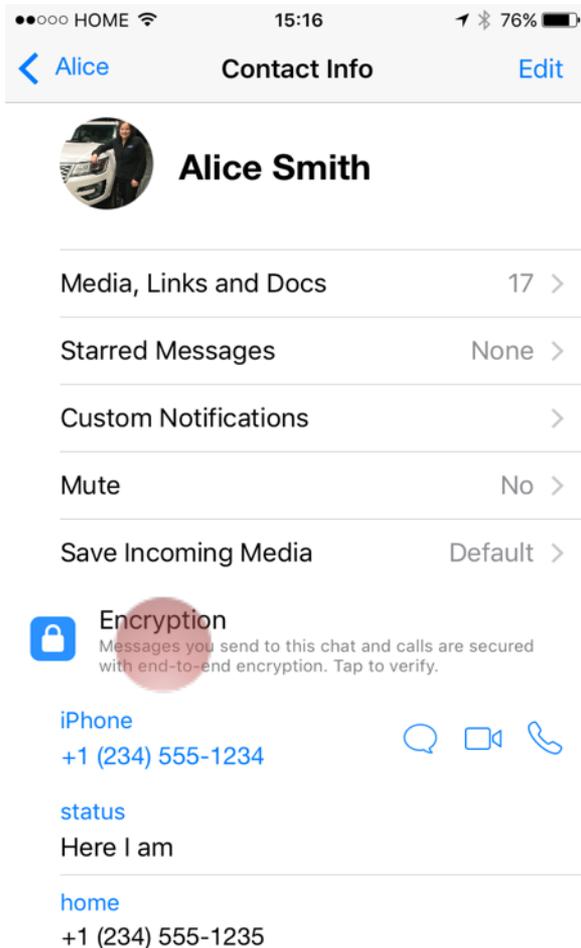
## Signal protocol



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



# Encrypted instant messaging



# Public key cryptography



public key



private key

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

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

The screenshot shows a web browser window displaying an ABC News article. The browser's address bar shows the URL: [abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/](http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/). The article title is "Ex-NSA Chief: 'We Kill People Based on Metadata'", dated May 12, 2014, by Lee Ferran. The article text discusses the U.S. government's use of metadata for surveillance, quoting former NSA head Michael Hayden. The text states: "The U.S. government 'kill[s] people based on metadata,' but it doesn't do that with the trove of information collected on American communications, according to former head of the National Security Agency Gen. Michael Hayden." It further explains that metadata can reveal "everything" about a target without the need for the actual communication content. A quote from Hayden is also included: "[That] description... is absolutely correct. We kill people based on metadata. But that's not what we do with this metadata," said Hayden, apparently referring to domestic metadata collection. "It's really important to understand the program in its entirety. Not the potentiality of the program, but how the program is actually conducted." The article concludes with another quote from Hayden: "So NSA gets phone records, gets them from the telephone company, been getting them since October of 2001 from one authority or another, puts them in a lockbox... and under very strict limitations can access the lockbox," Hayden said and then described a hypothetical situation in which a number connected to a terrorist could be run against the metadata already collected to help investigators find additional leads in the name of national security.

<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/>

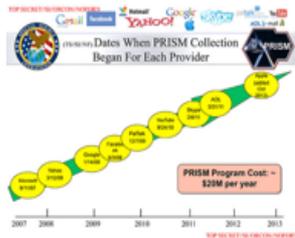
# anonymity network

- 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

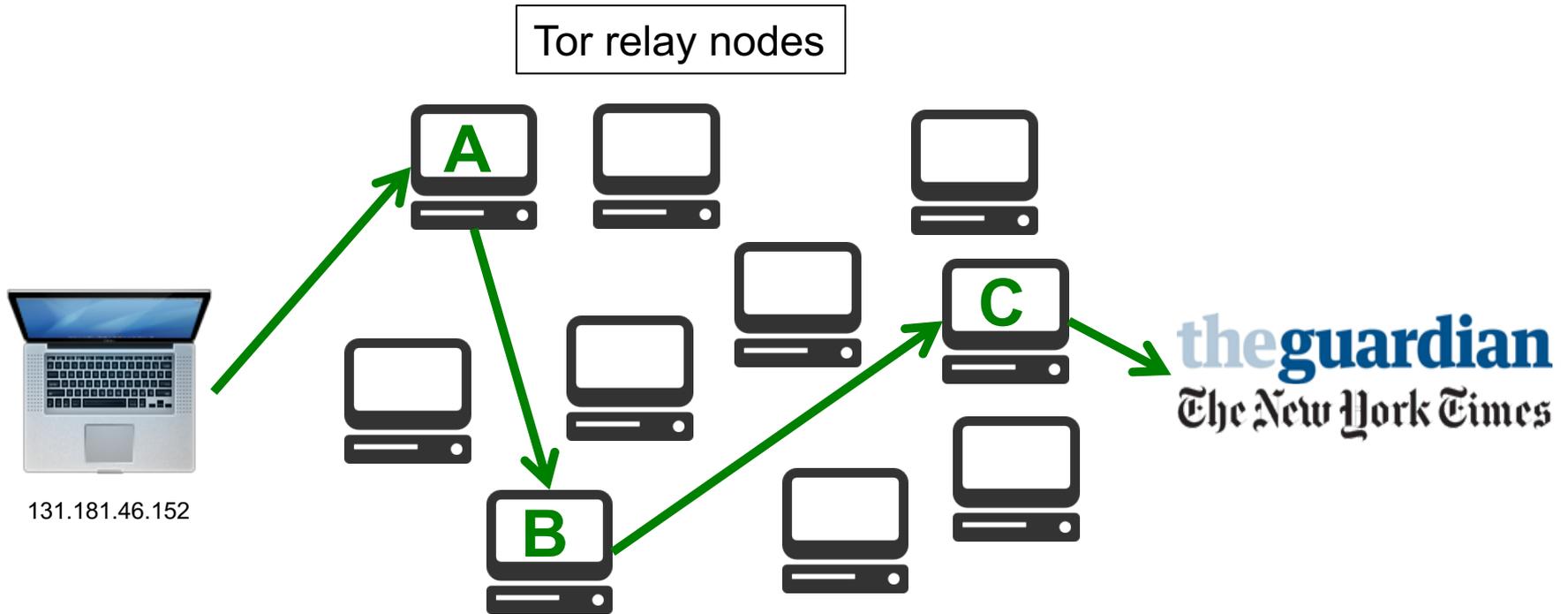
the guardian  
The New York Times



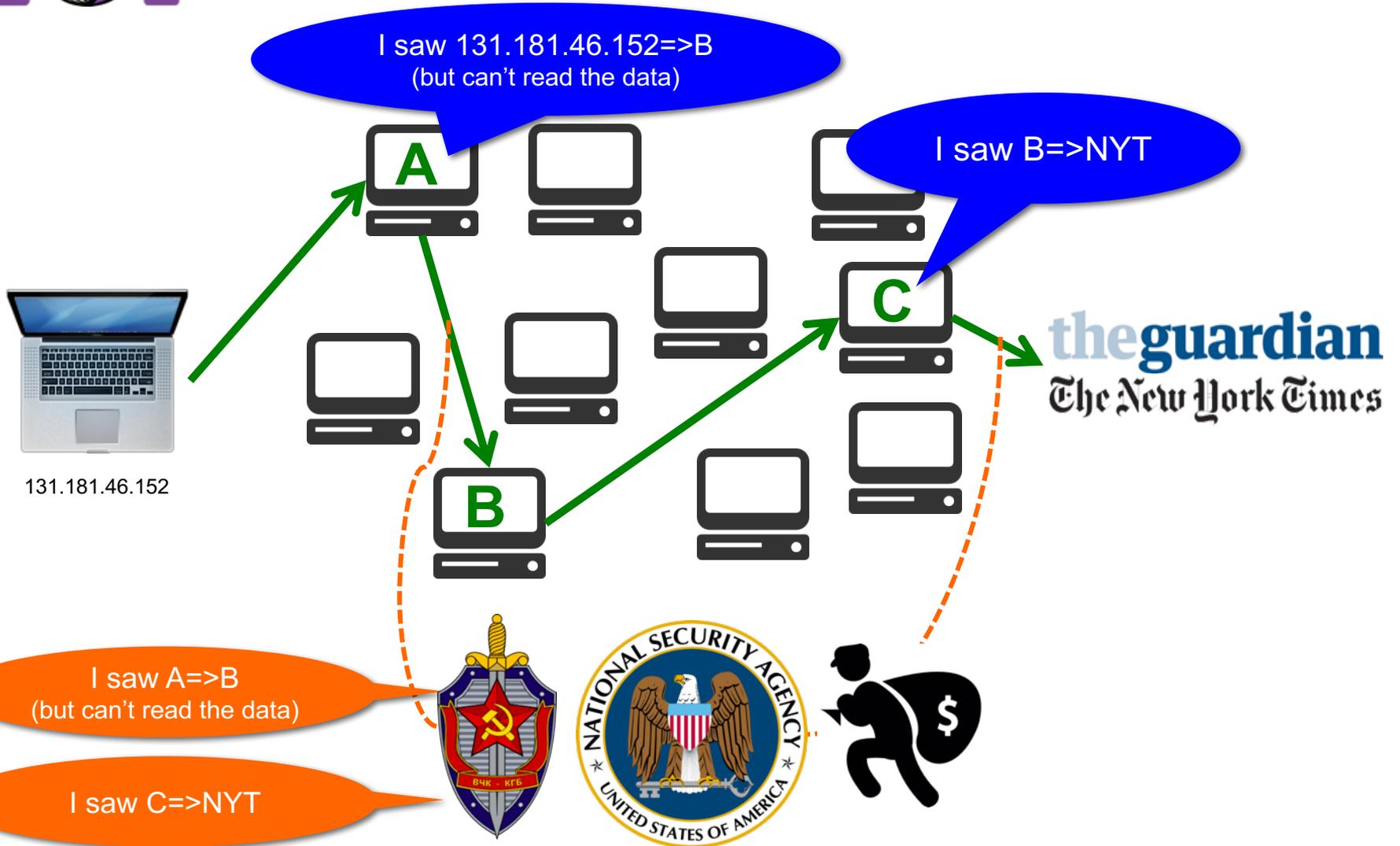
I saw 131.181.46.152 communicate with NYT



# anonymity network



# Tor anonymity network



I saw 131.181.46.152=>B  
(but can't read the data)

I saw B=>NYT

I saw A=>B  
(but can't read the data)

I saw C=>NYT

+ can't tell these two facts are linked

# Things you can do to improve your privacy and security online

---

# Things you can do

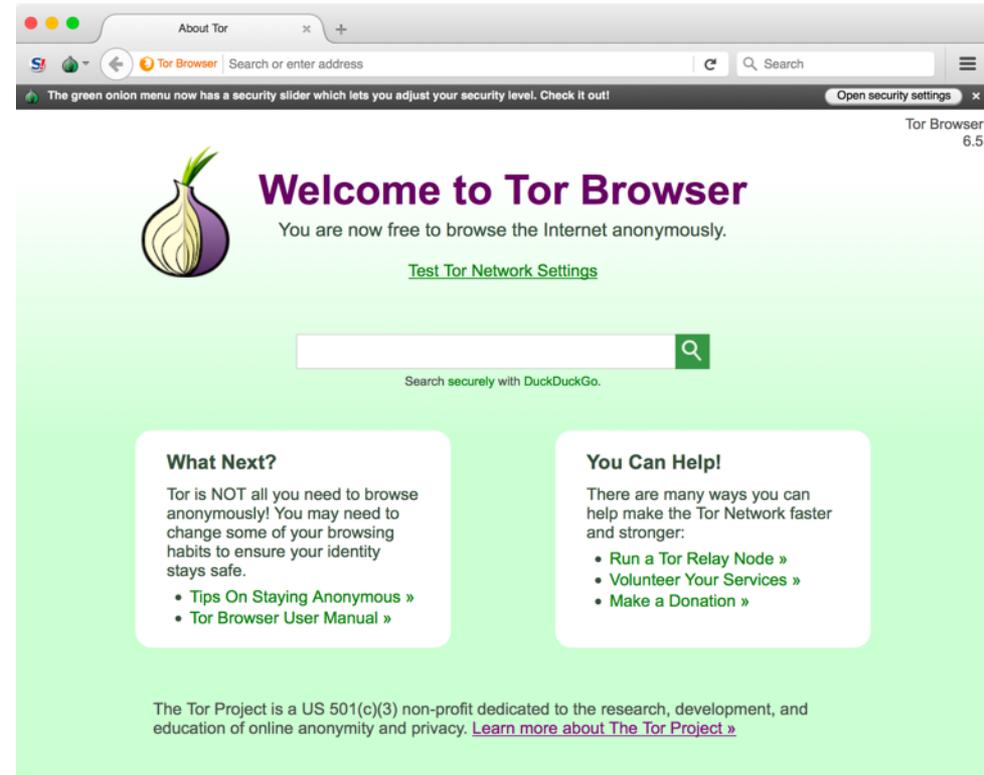
## Passwords

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

# Things you can do

## Untrusted networks

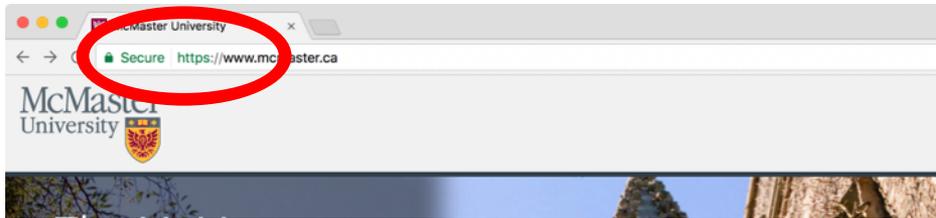
- On untrusted wi-fi networks (coffee shops, airports, hotels), consider using a **virtual private network** or the **Tor browser** for extra privacy.



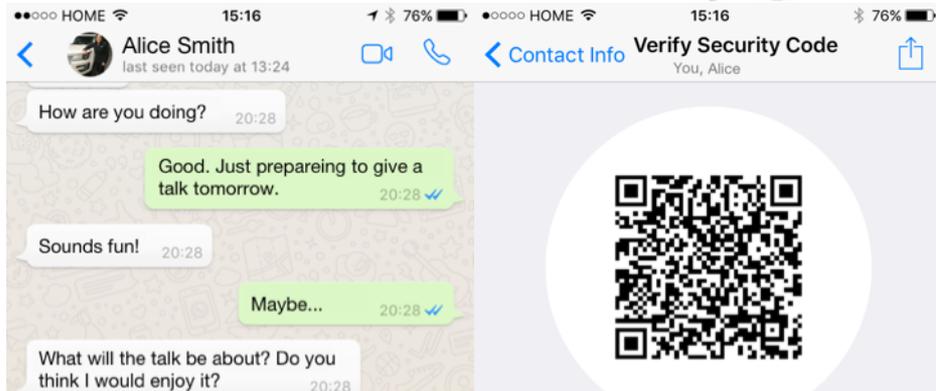
<https://www.torproject.org>

# Things you can do

## Web browsing



## Instant messaging

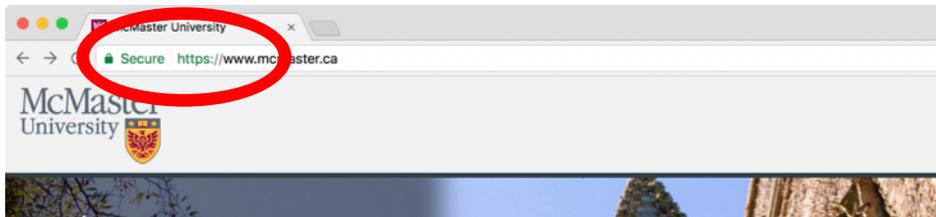


# How cryptography protects your information every day

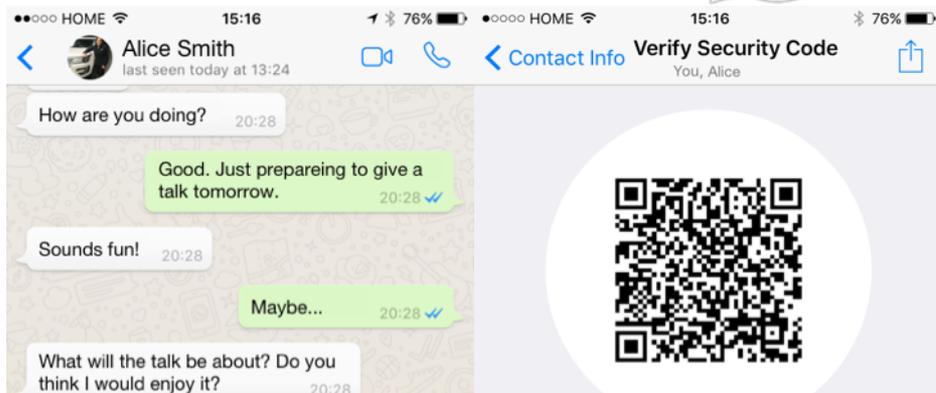
Douglas Stebila 

<https://www.cas.mcmaster.ca/~stebila/>

## 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](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565)

### Surveillance Self-Defense

- <https://ssd.eff.org>

### Schneier on Security

- <https://www.schneier.com>