CS 568: Applied Cryptography

Prof. Mayank Varia

Syllabus

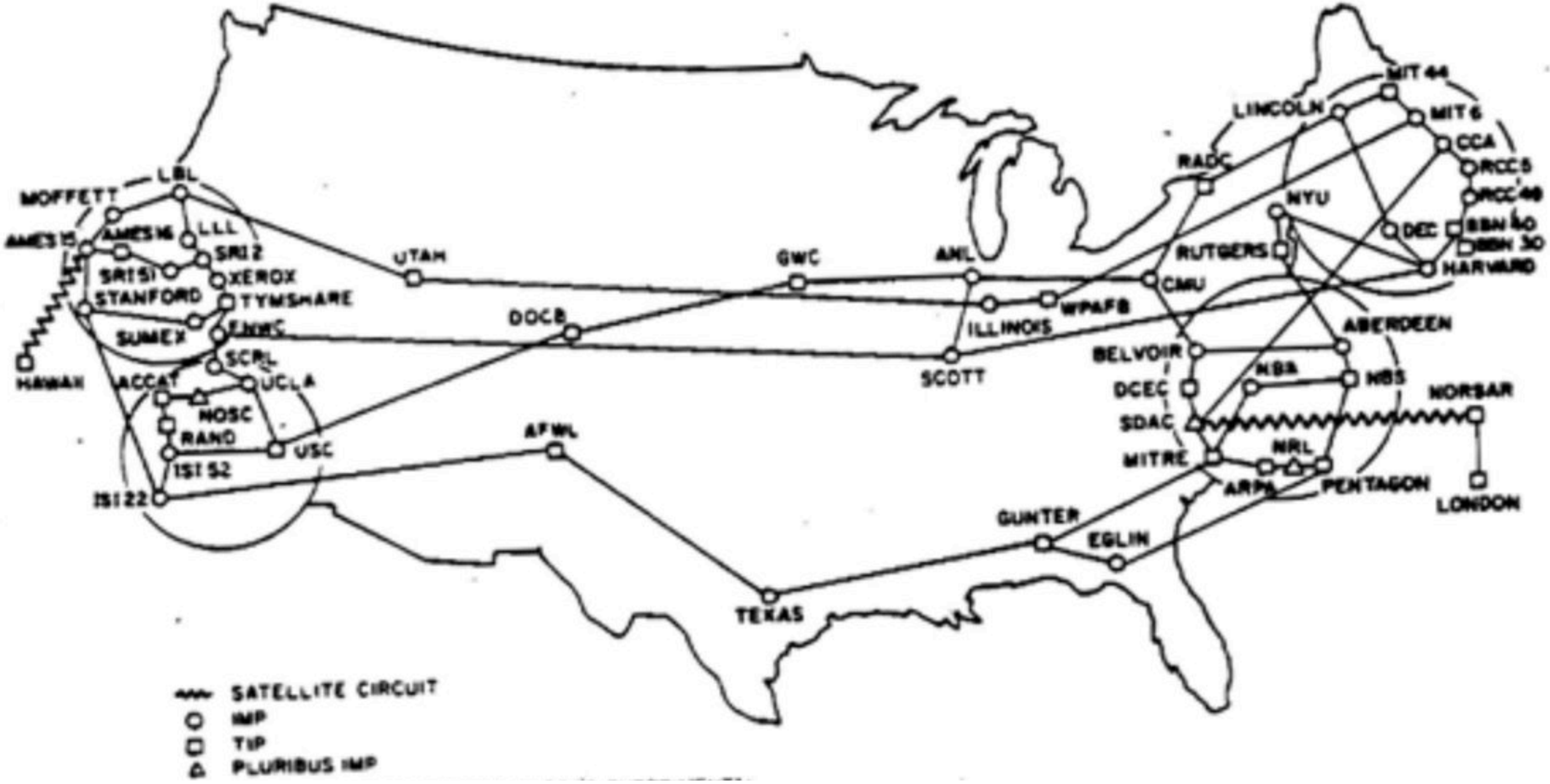
- Instructor: Mayank Varia, TA: Nicolas Alhaddad
- Course sites: piazza.com for discussion, gradescope.com for homework
- Exam dates: 2/20, 3/31, and 5/5 (mark on your calendar now!)
- Weekly assignments: programming homework + textbook reading
- Textbook: no purchase required, all reading is available online
- Grading: 40% homework, 20% midterm1, 20% midterm2, 25% final
- *Always follow the BU academic conduct code & collaboration policy!*

What is cryptography?

> “**Cryptography** is how people get things done when they need one another, don’t fully trust one another, and have adversaries actively trying to screw things up.”

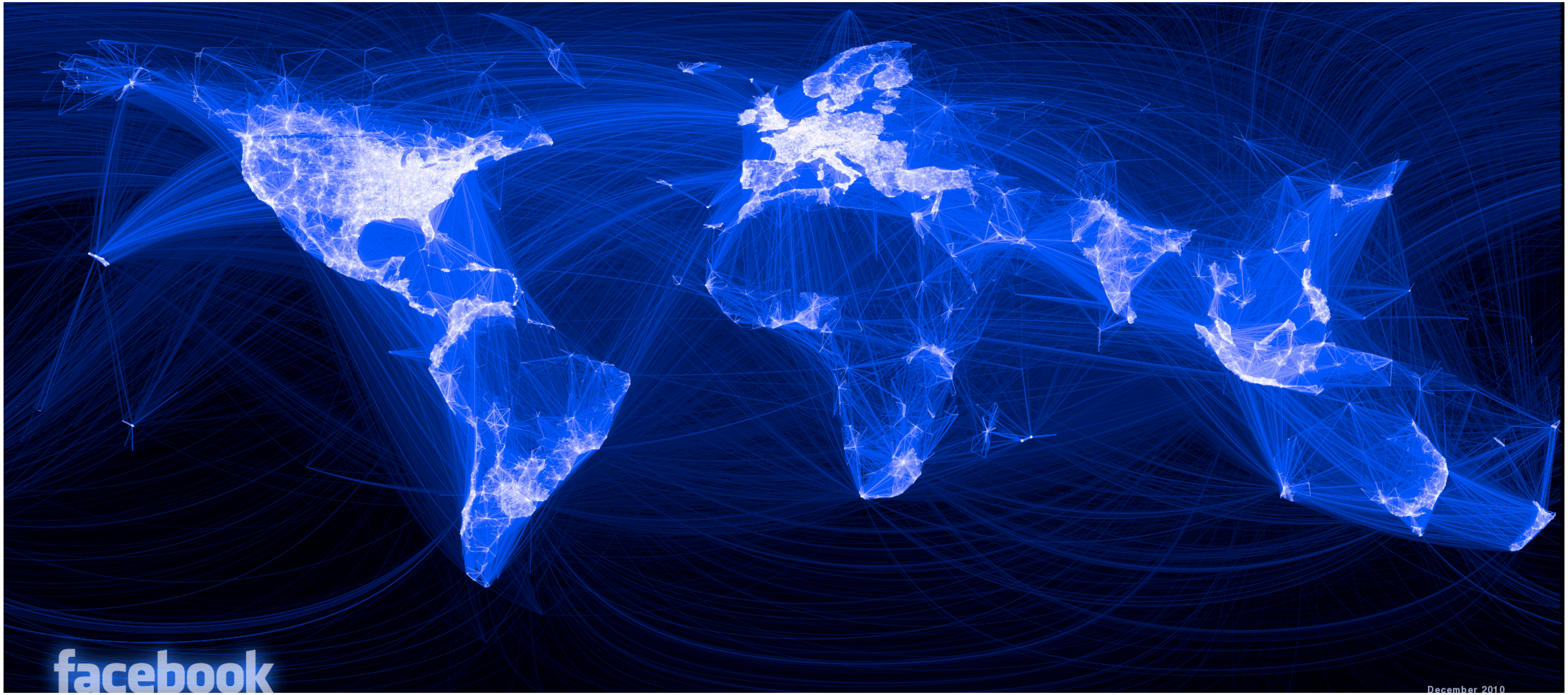
–Ben Adida

The Internet, 1968



Source: twitter.com/pwnallthethings/status/935395453482520576

Facebook friendship graph, 2010



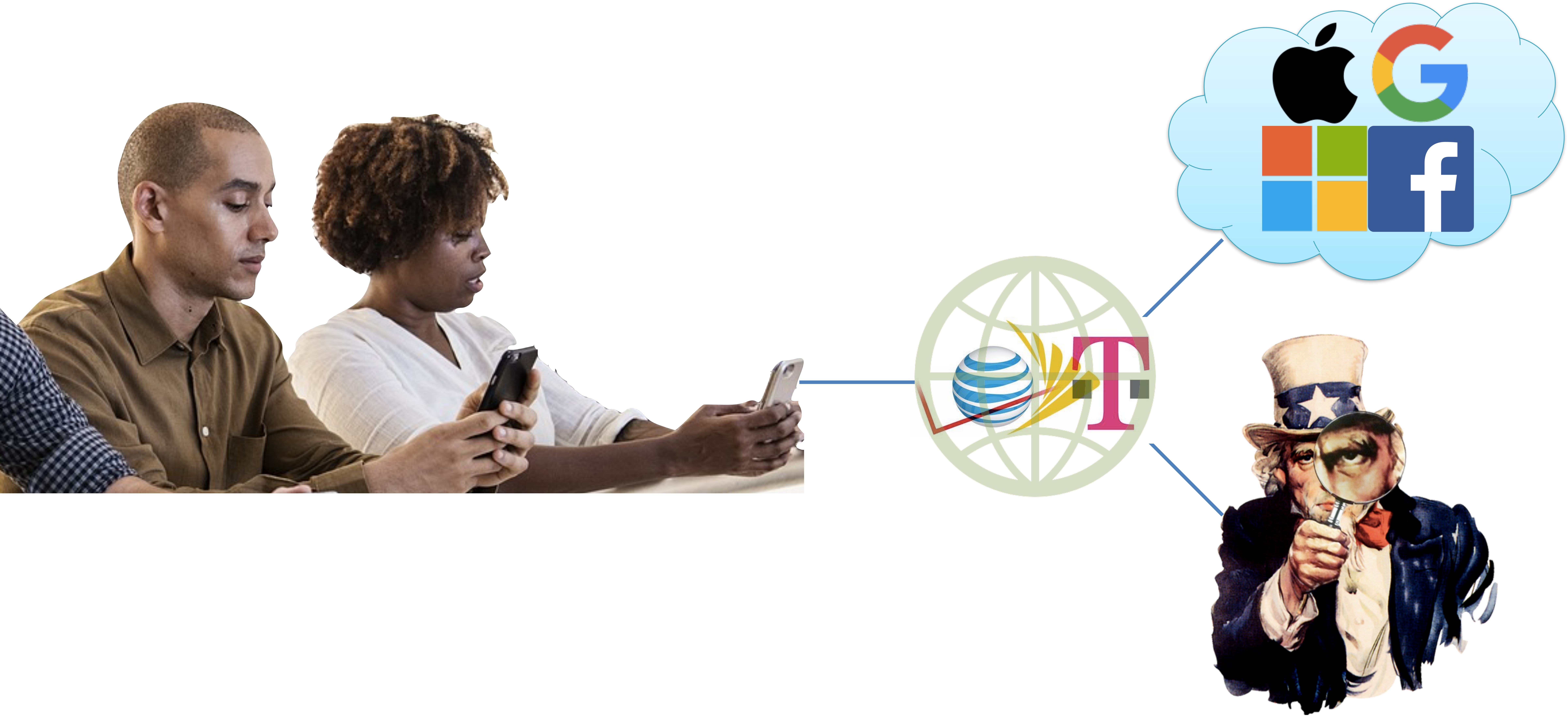
Source: www.facebook.com/note.php?note_id=469716398919

“The Internet is just the world passing notes in a classroom.”

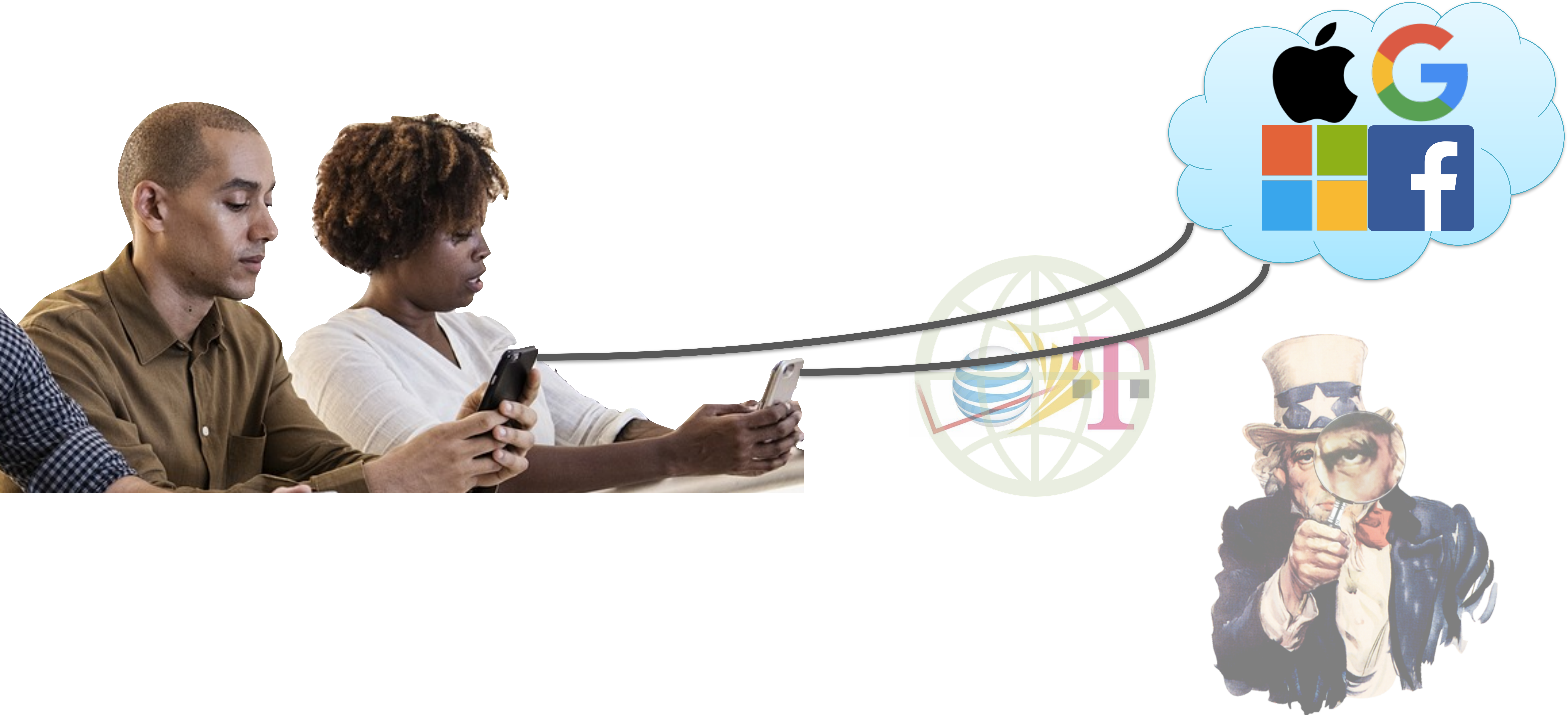
–Jon Stewart

Source: news.bbcimg.co.uk/media/images/75643000/jpg/_75643557_passing-notes.jpg

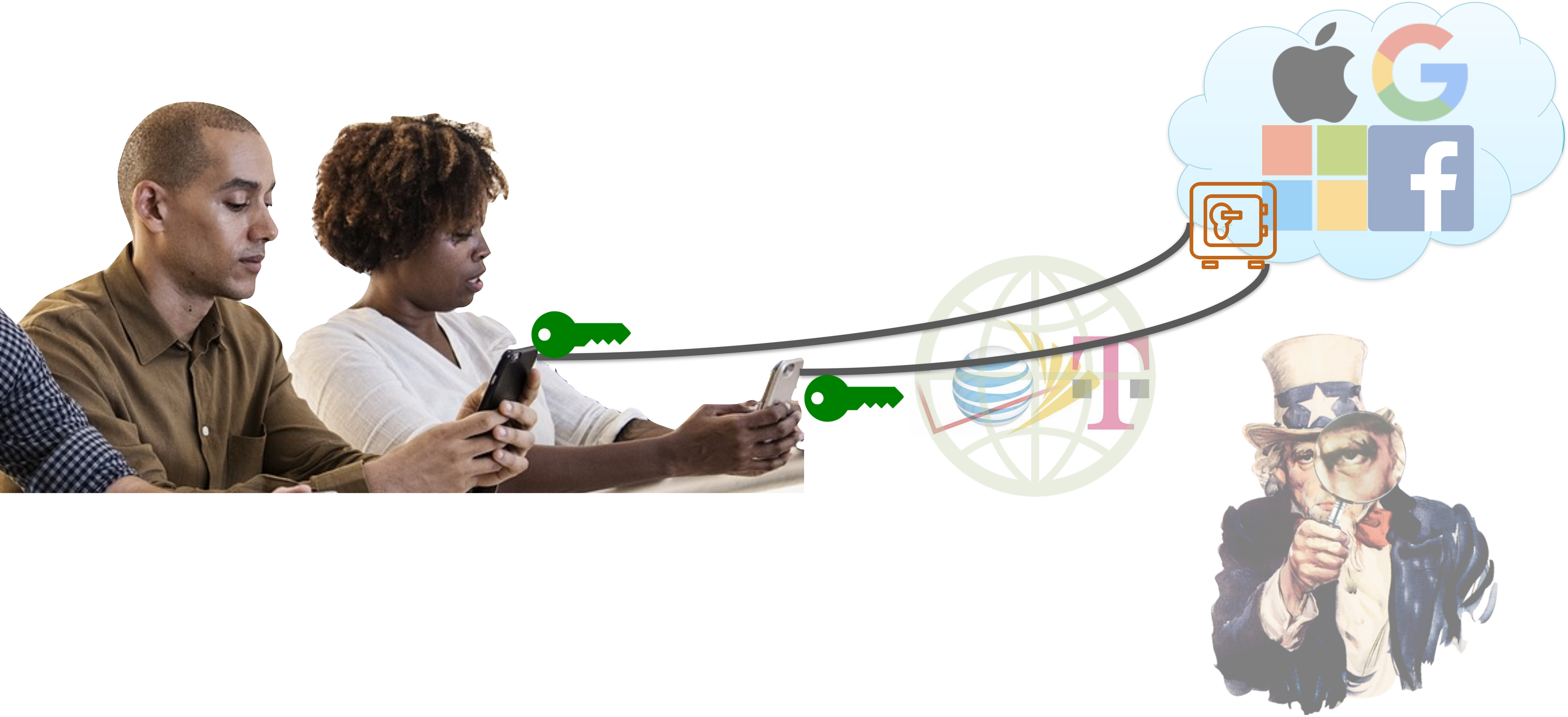
Talking over the Internet



Client-server cryptography



End-to-end cryptography

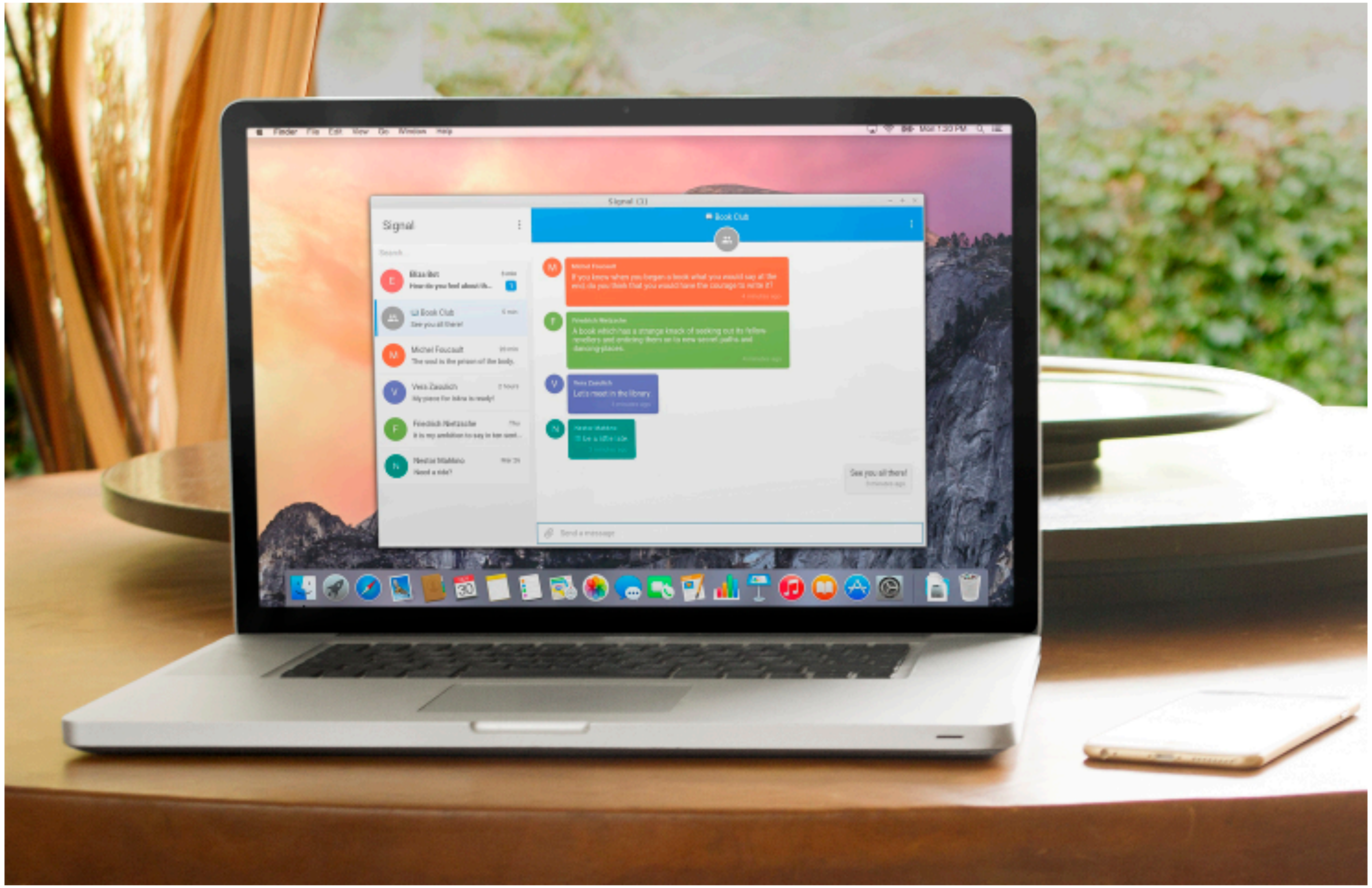


Why does crypto matter?

Why does crypto matter?

1. We use it all the time, so it must be automatic + fast

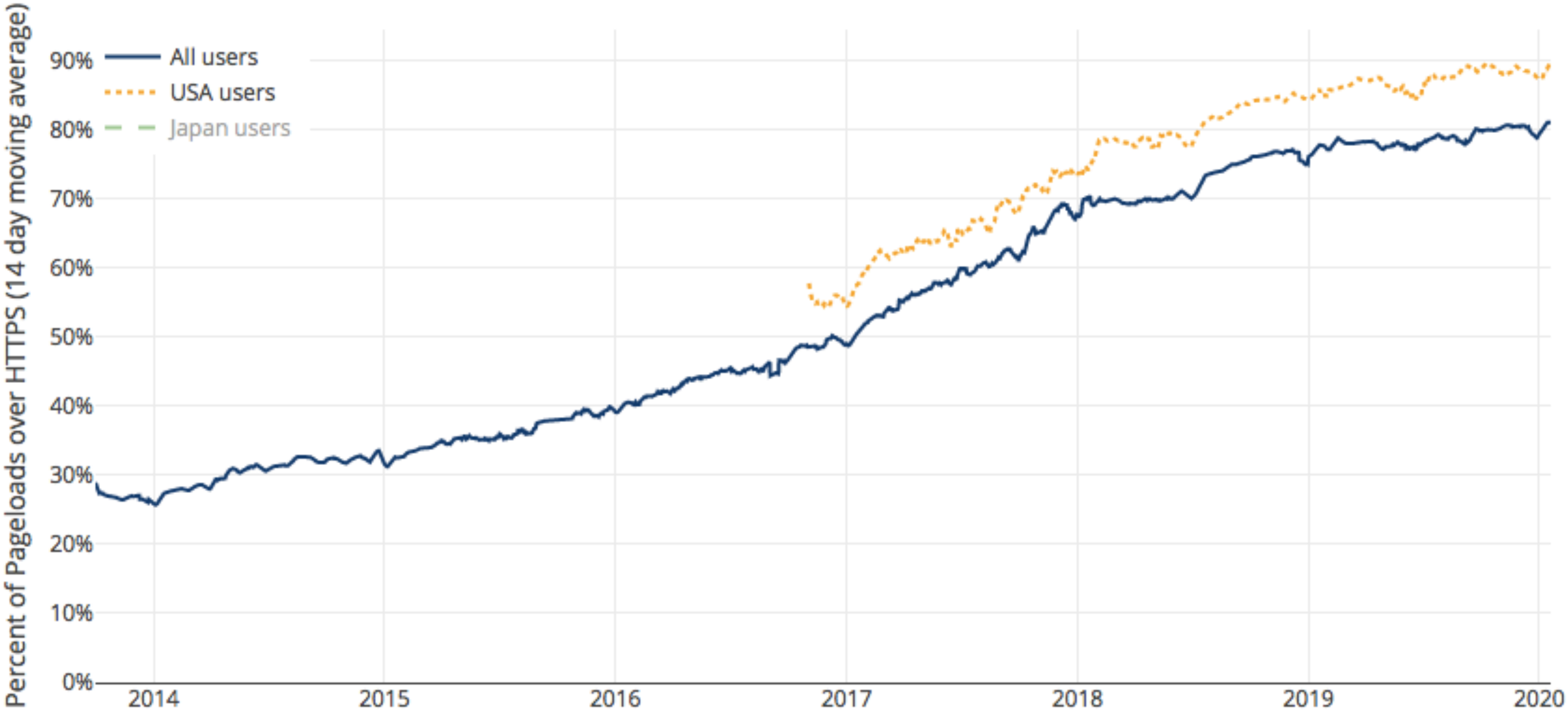
Source: signal.org



Why does crypto matter?

1. We use it all the time, so it must be automatic + fast

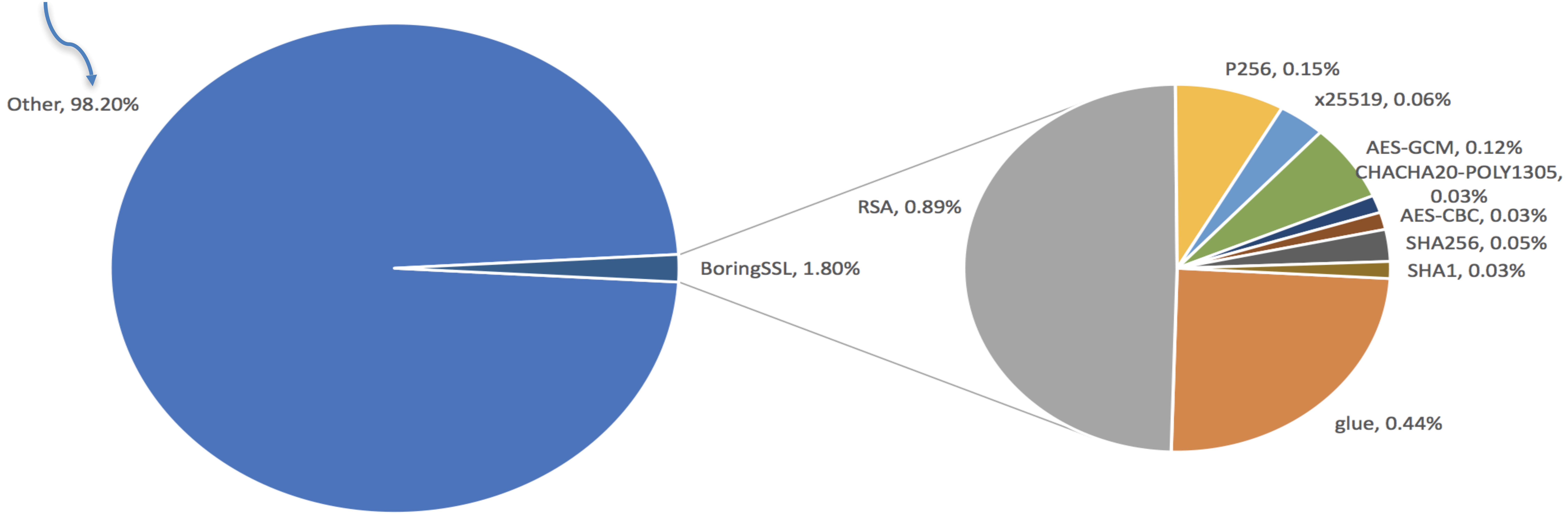
Source: letsencrypt.org/stats



Why does crypto matter?

1. We use it all the time, so it must be automatic + fast

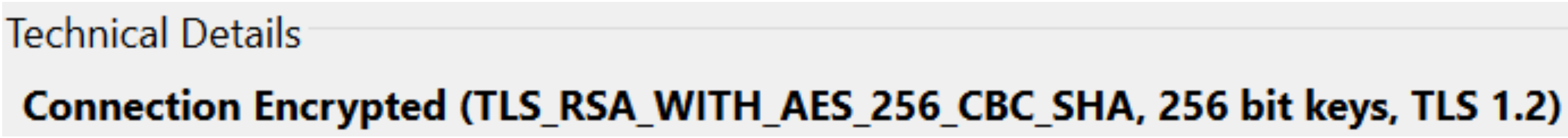
everything else the server does



Why does crypto matter?

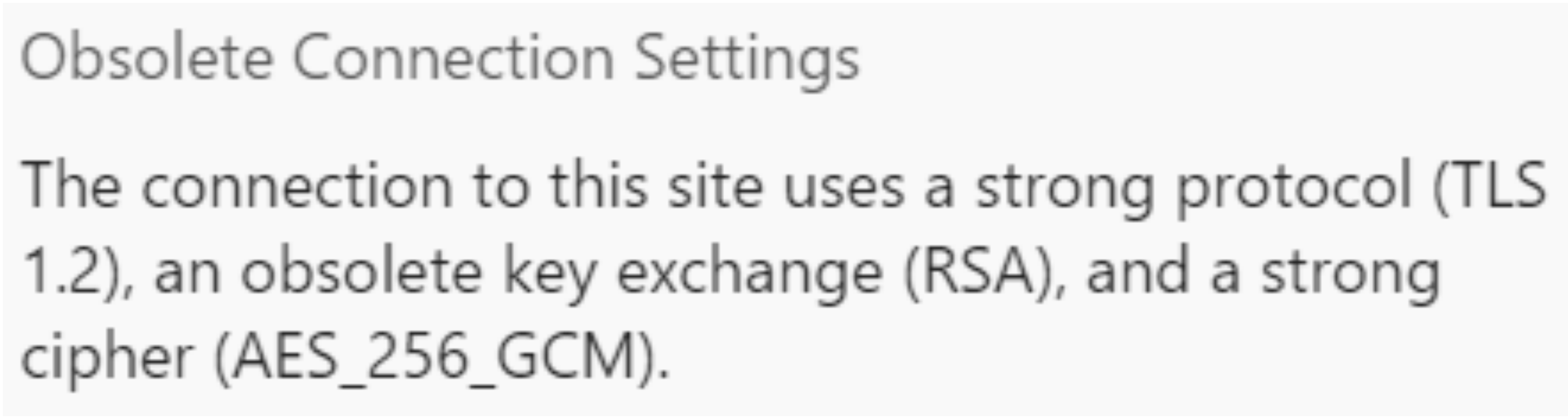
1. We use it all the time, so it must be automatic + fast
2. Bad crypto can lead to universal, covert breaches of digital security

bu.edu login page



Technical Details

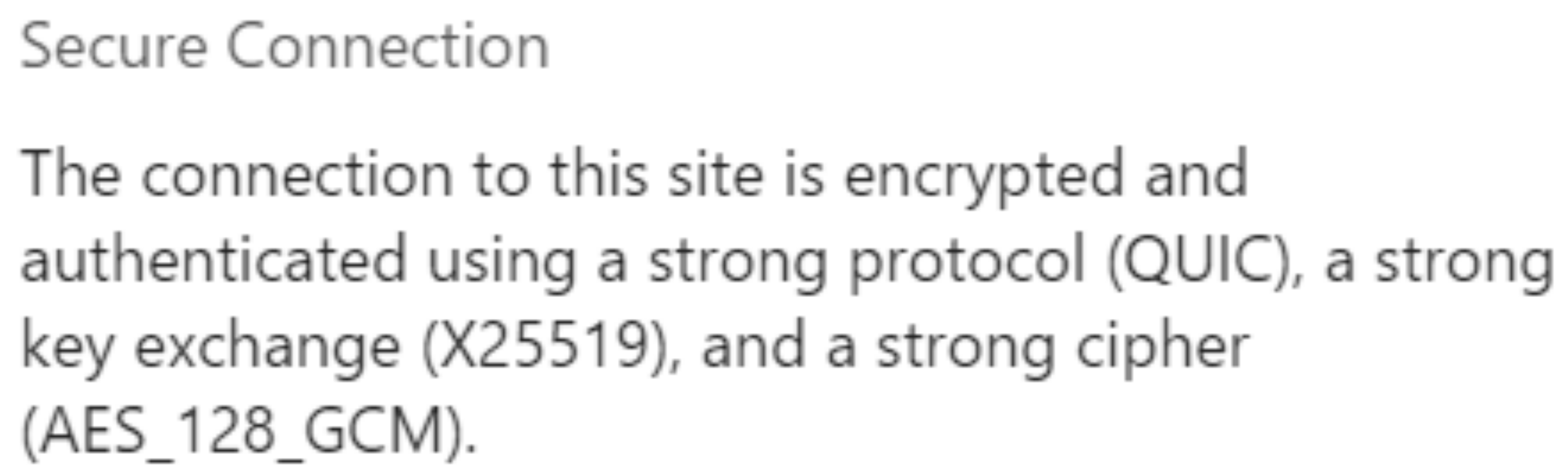
Connection Encrypted (TLS_RSA_WITH_AES_256_CBC_SHA, 256 bit keys, TLS 1.2)



Obsolete Connection Settings

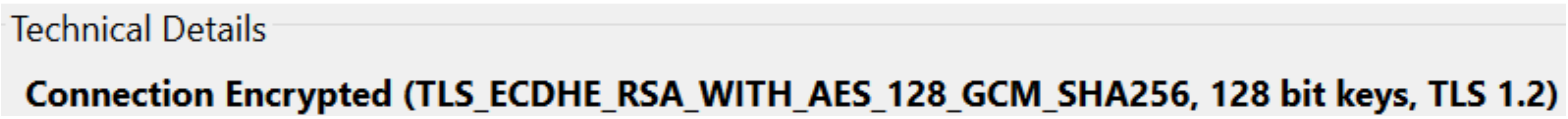
The connection to this site uses a strong protocol (TLS 1.2), an obsolete key exchange (RSA), and a strong cipher (AES_256_GCM).

google.com



Secure Connection

The connection to this site is encrypted and authenticated using a strong protocol (QUIC), a strong key exchange (X25519), and a strong cipher (AES_128_GCM).



Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

Why does crypto matter?

1. We use it all the time, so it must be automatic + fast
2. Bad crypto can lead to universal, covert breaches of digital security
3. Cryptography has social, legal, and political impacts
   (& conversely, crypto is influenced by society, the law, and politicians)

> “**Cryptography rearranges power:** it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension.”
>
> *–Prof. Phillip Rogaway (UC Davis)*

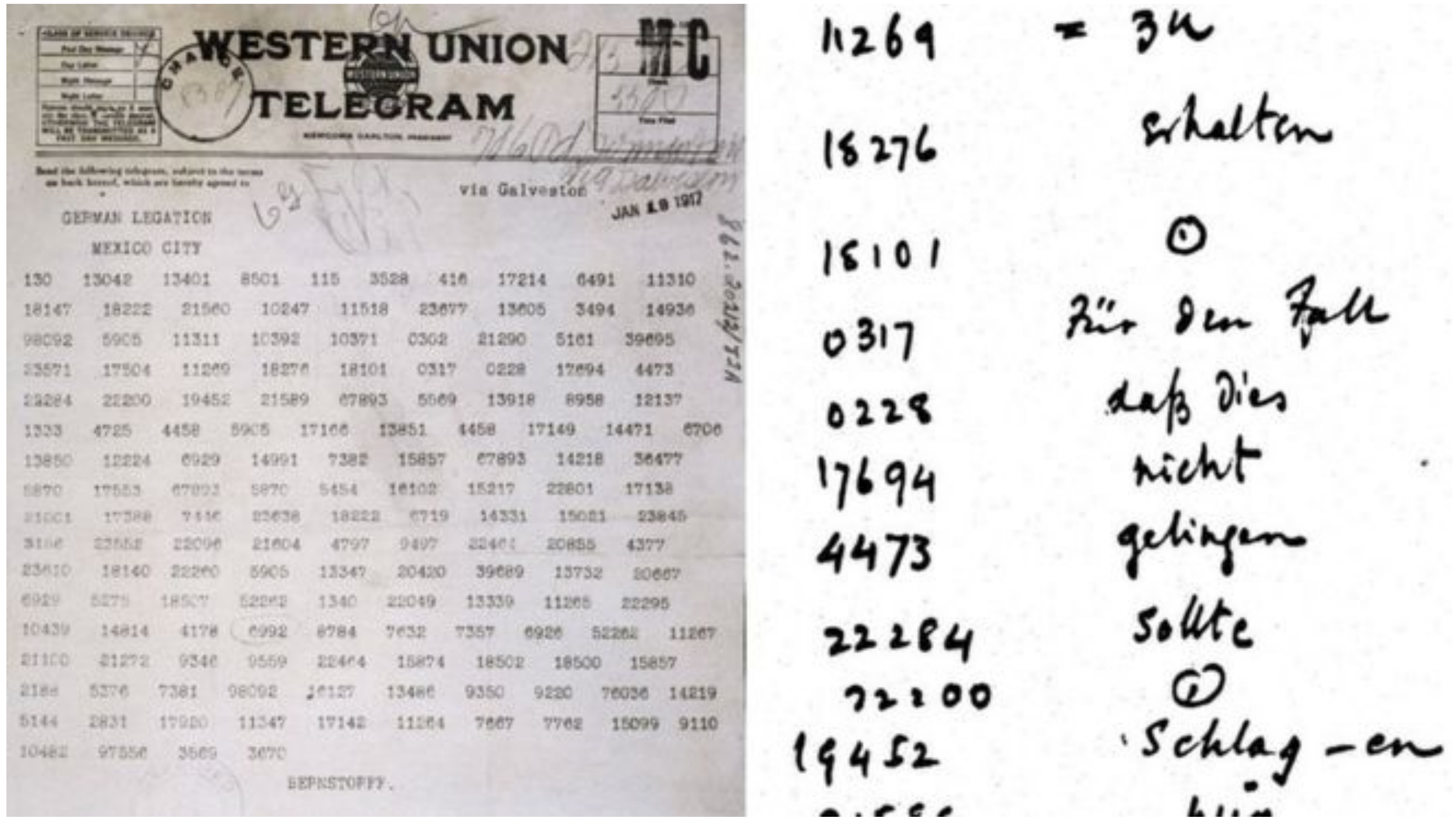
Source: web.cs.ucdavis.edu/~rogaway/papers/moral.html

Crypto meets the U.S. Bill of Rights

Amendment	Crypto relevance
1. Free speech++	*Bernstein v. United States* established code == speech
2. Right to bear arms	Crypto is regulated as a munition
3. No quartering of soldiers	1990s Clipper chip: government in all computers
4. Limits on law enforcement	Crypto → reasonable expectation of privacy?
5. Right against self-incrimination	Can government request your help to unlock phone?

Crypto Wars: early 20th century edition

World War I: Zimmerman telegram



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

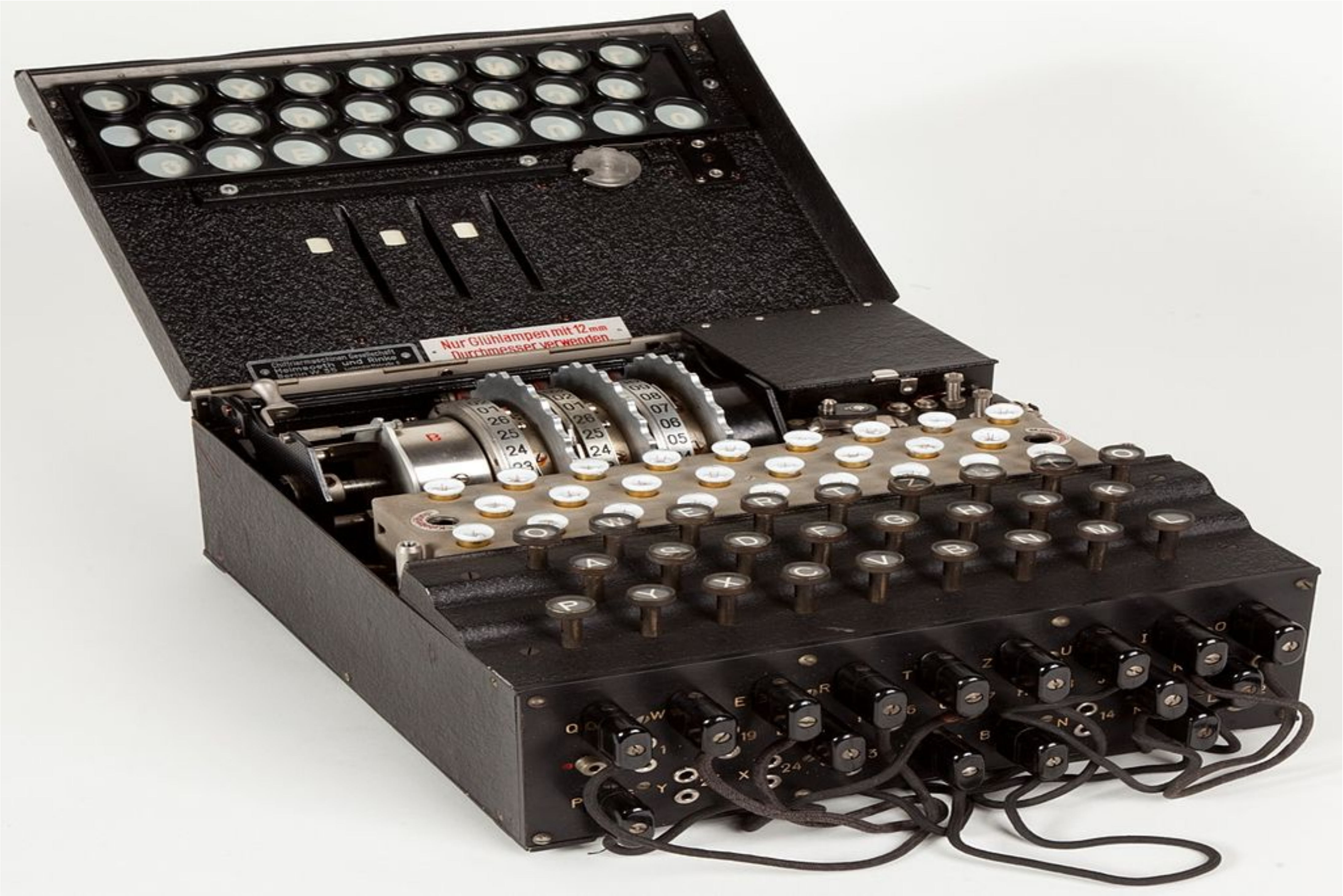
```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
22284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
23610  18140  22260  5905   13347  20420  39689  13732  20667
6929   5275   18507  52262  1340   22049  13339  11265  22295
10439  14814  4178   6992   8784   7632   7357   6926   52262  11267
21100  21272  9346   9559   22464  15874  18502  18500  15857
2188   5376   7381   98092  16127  13486  9350   9220   76036  14219
5144   2831   17920  11347  17142  11264  7667   7762   15099  9110
10482  97556  3569   3670
```

BERNSTORFF.

11269	= zu
18276	schalten
18101	⊙
0317	Für den Fall
0228	daß dies
17694	nicht
4473	gelingen
22284	sollte
22200	⊙
19452	Schlag-en

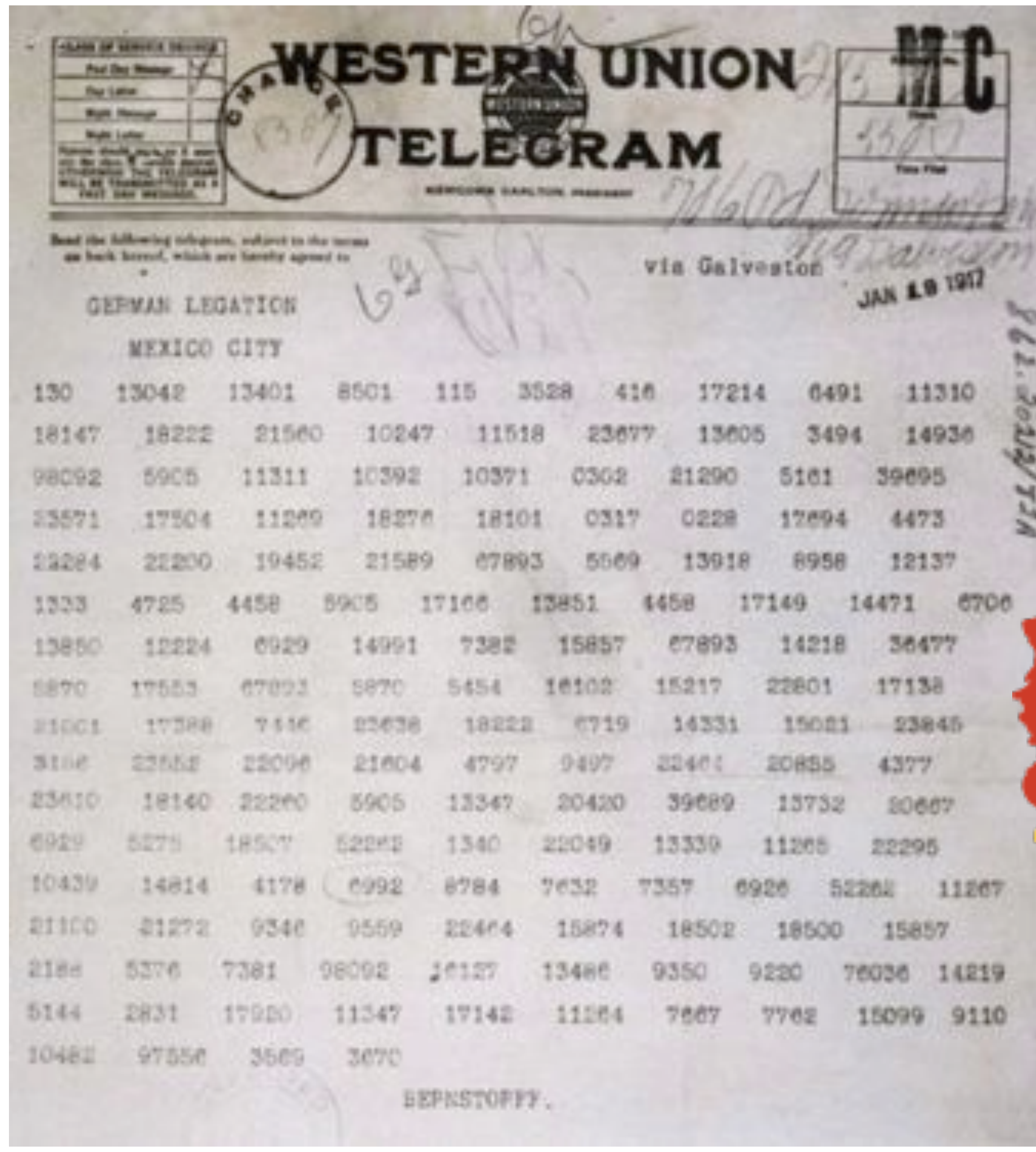
Source: www.bbc.com/news/uk-38581861

World War II: Enigma machine



Source: en.wikipedia.org/wiki/Enigma_machine

Zimmerman telegram



WESTERN UNION
TELEGRAM

via Galveston

JAN 19 1917

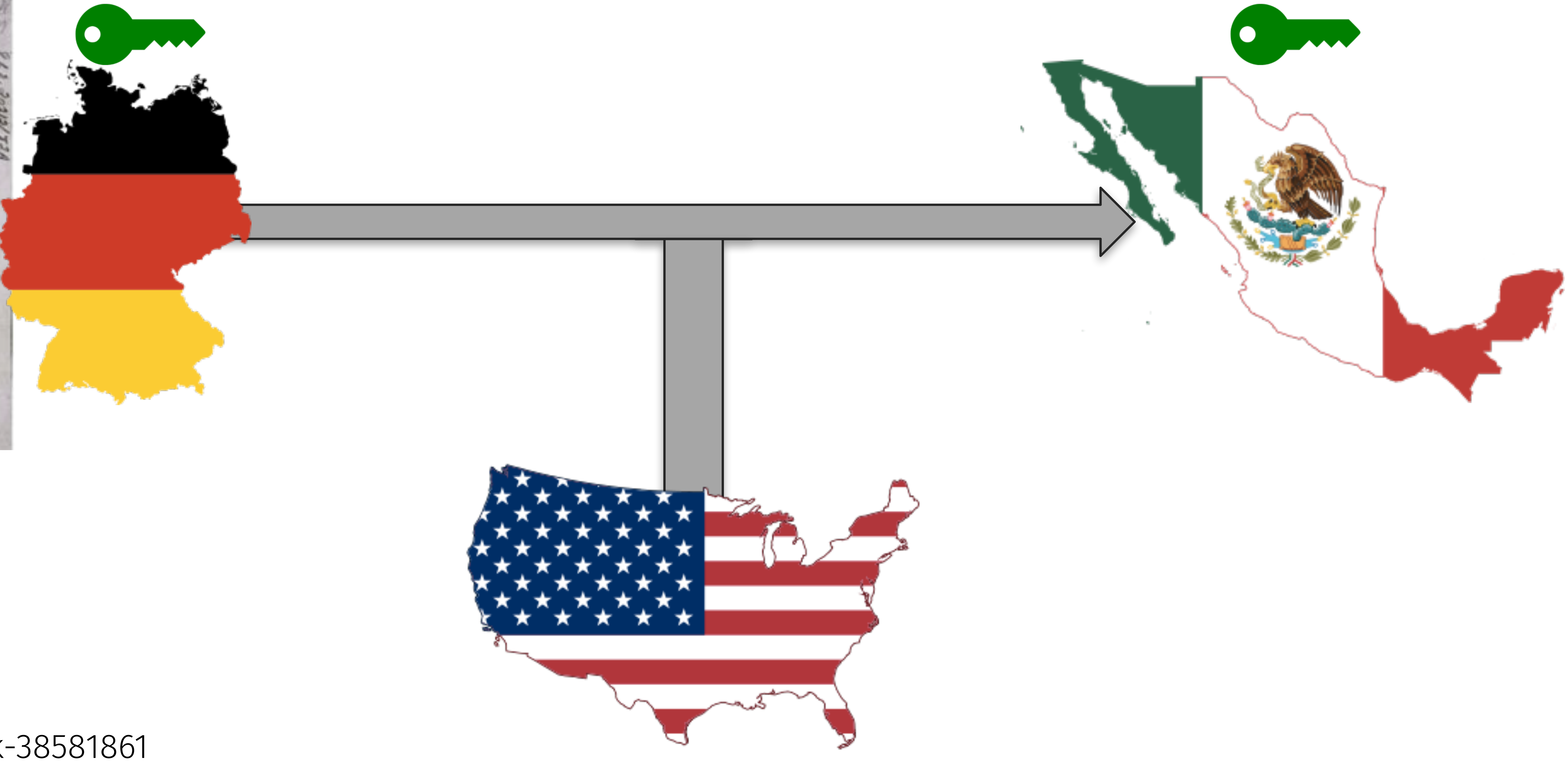
GERMAN LEGATION

MEXICO CITY

```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
22284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
23610  18140  22260  5905   13347  20420  39689  13732  20667
6929   5275   18507  52262  1340   22049  13339  11265  22295
10439  14814  4178   6992   8784   7632   7357   6926   52262  11267
21100  21272  9346   9559   22464  15874  18502  18500  15857
2188   5376   7381   98092  16127  13486  9350   9220   76036  14219
5144   2831   17920  11347  17142  11264  7667   7762   15099  9110
10482  97556  3569   3670
```

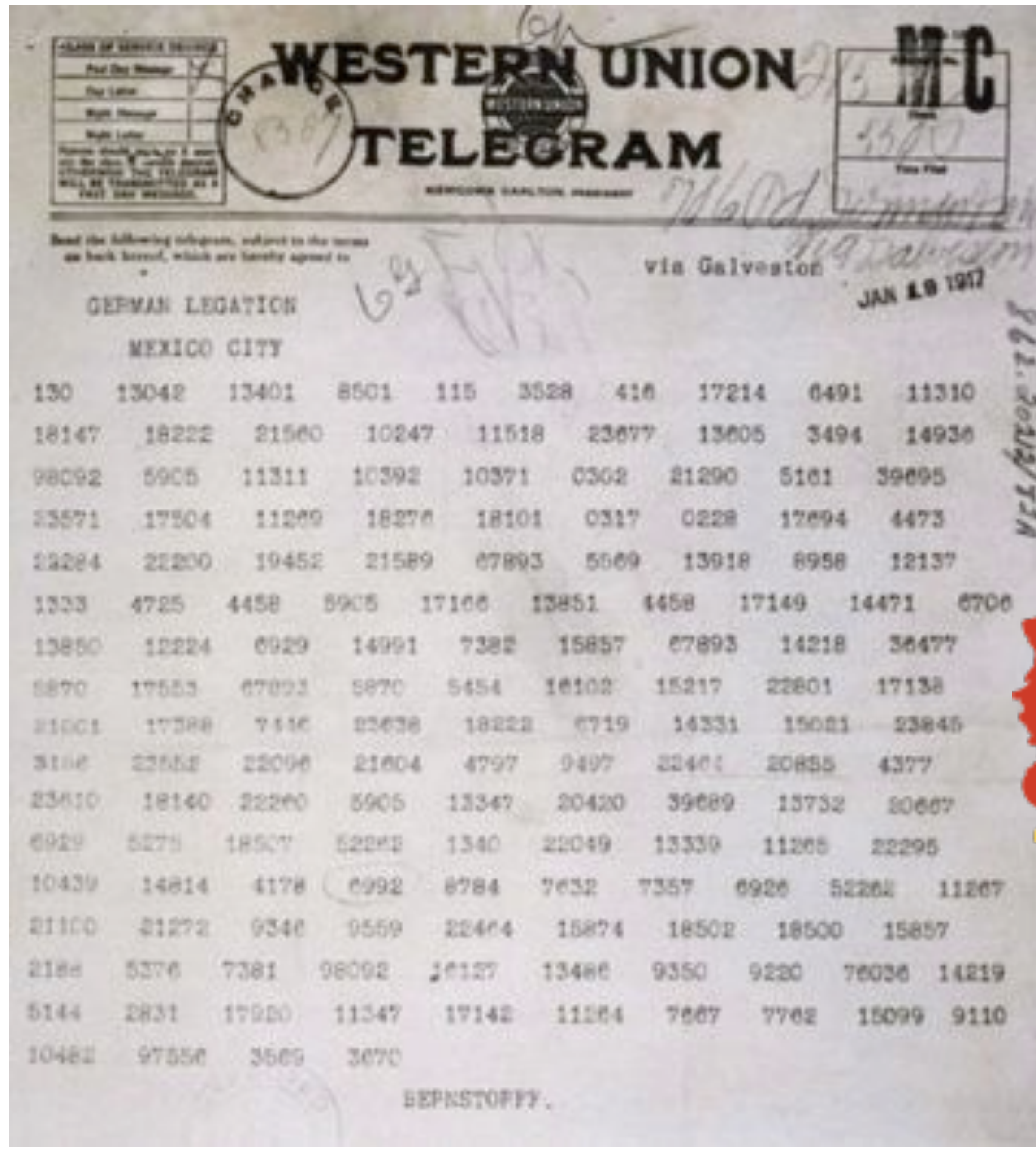
BERNSTORFF.

862.20212/82A



Source: www.bbc.com/news/uk-38581861

Zimmerman telegram



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

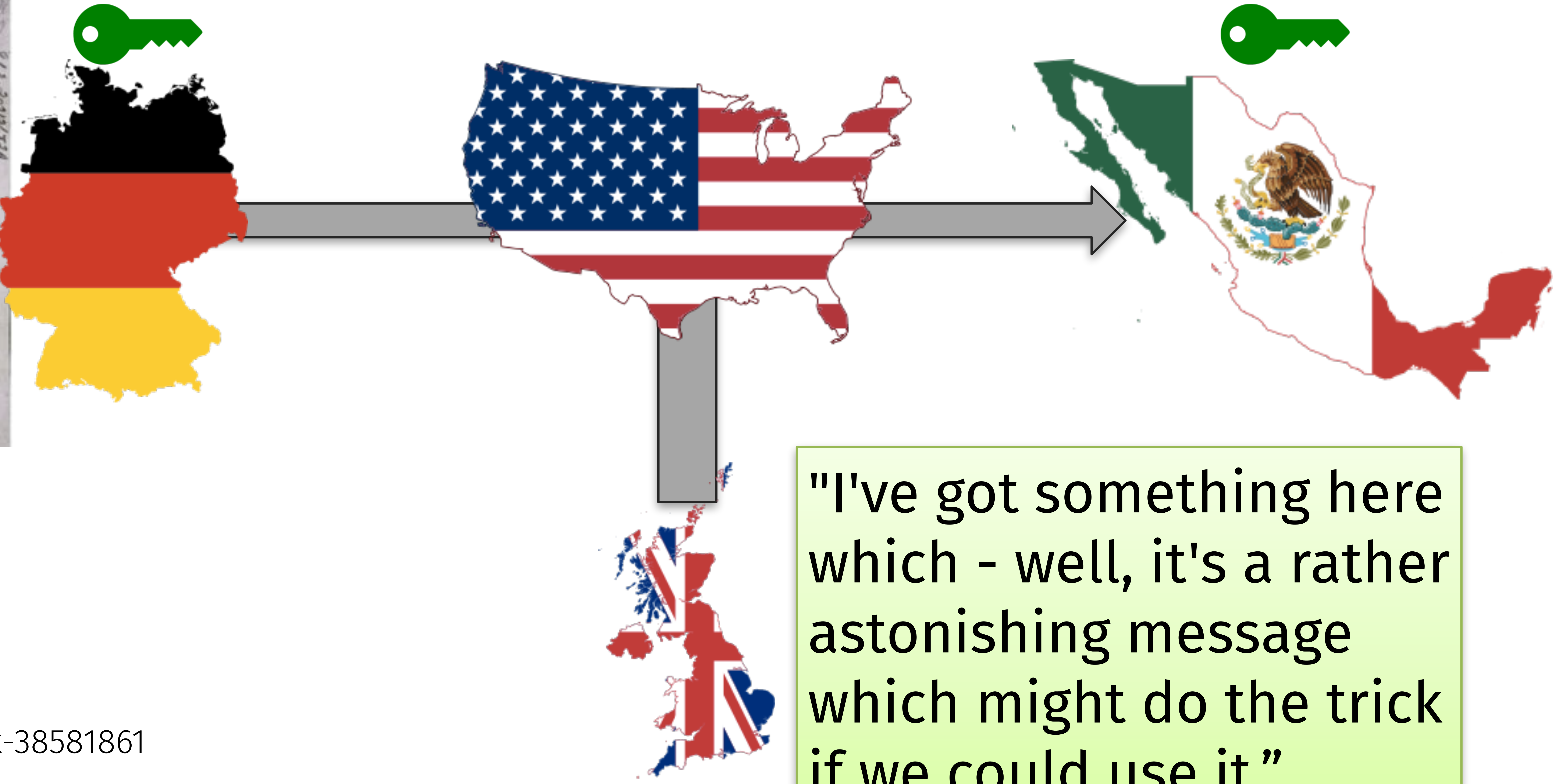
862.20212/71A

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

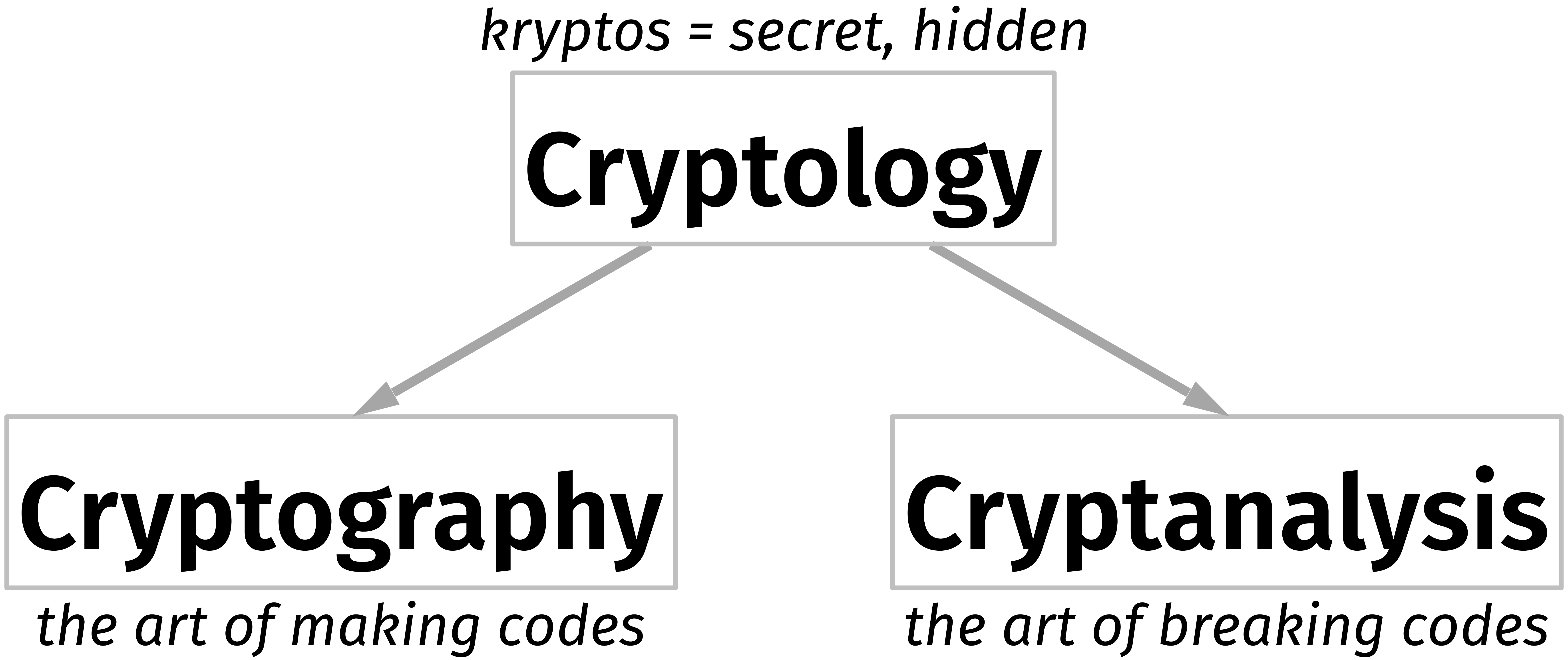
BERNSTORFF.



"I've got something here which - well, it's a rather astonishing message which might do the trick if we could use it."

Source: www.bbc.com/news/uk-38581861

What protections do we want cryptosystems to offer?



kryptos = secret, hidden

Cryptology

Cryptography

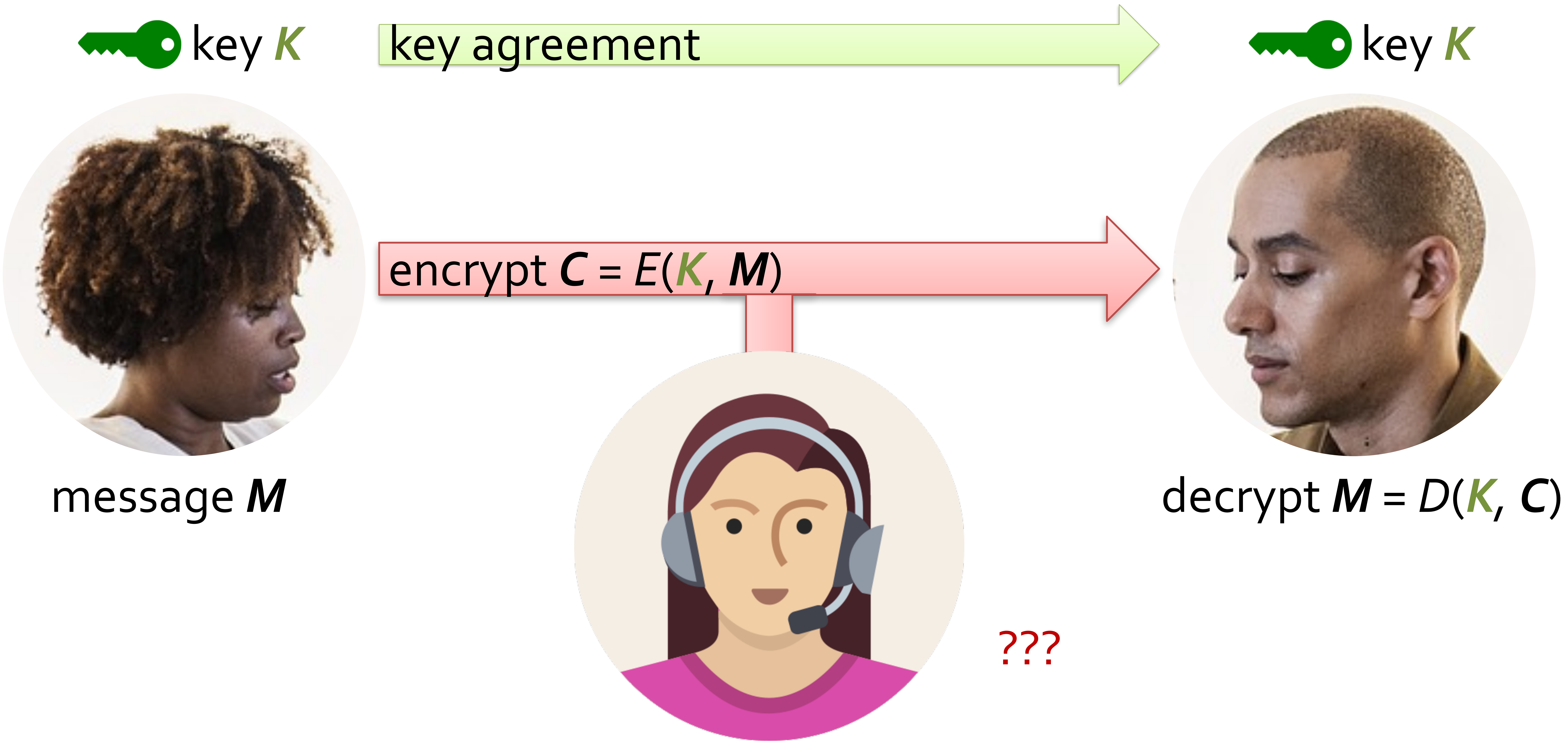
the art of making codes

Cryptanalysis

the art of breaking codes

Schneier's law: Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break.

Protecting data in transit



key K

key agreement

key K

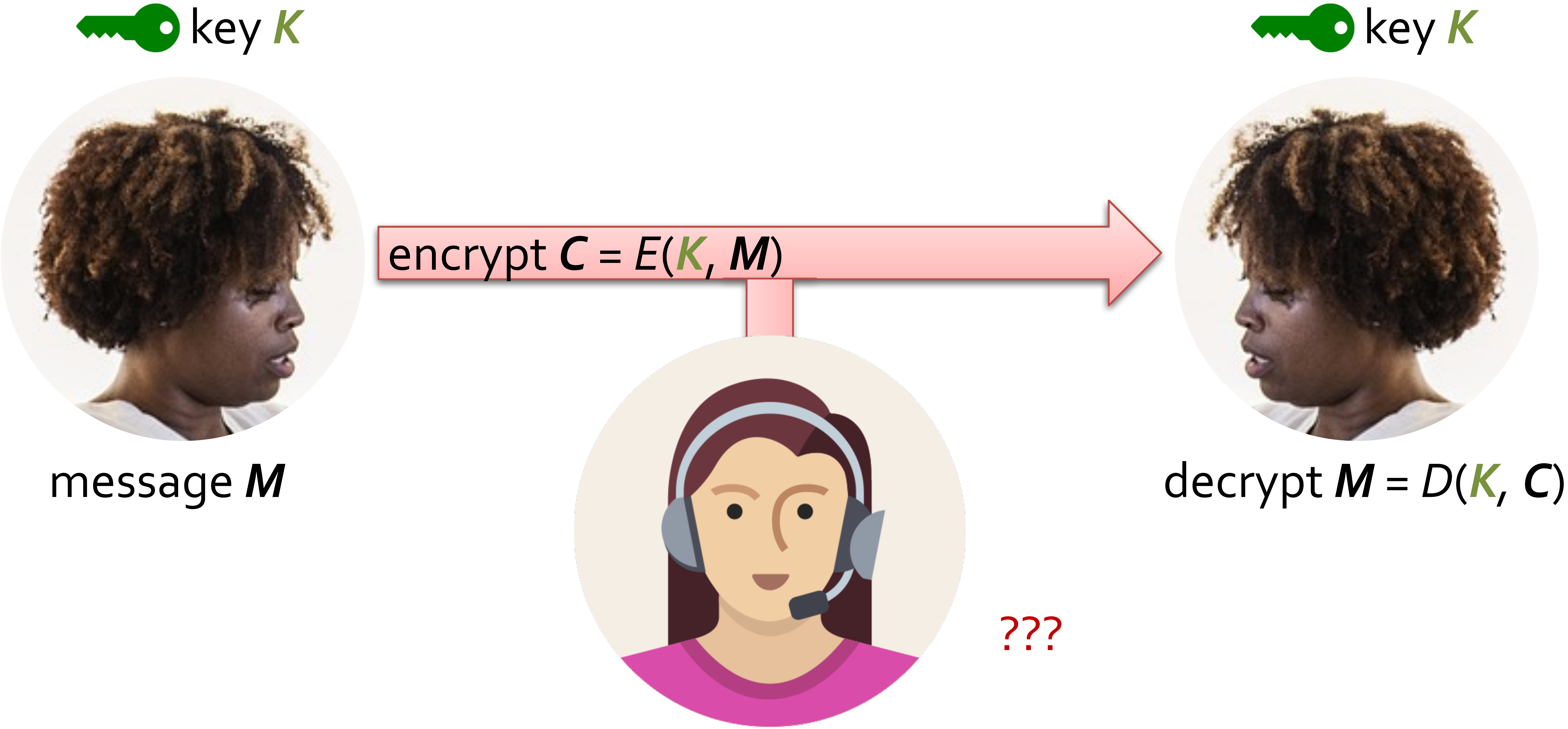
encrypt $\boldsymbol{C} = E(K, \boldsymbol{M})$

message $\boldsymbol{M}$

decrypt $\boldsymbol{M} = D(K, \boldsymbol{C})$

???

Protecting data at rest



key K

message $\boldsymbol{M}$

encrypt $\boldsymbol{C} = E(K, \boldsymbol{M})$

key K

decrypt $\boldsymbol{M} = D(K, \boldsymbol{C})$

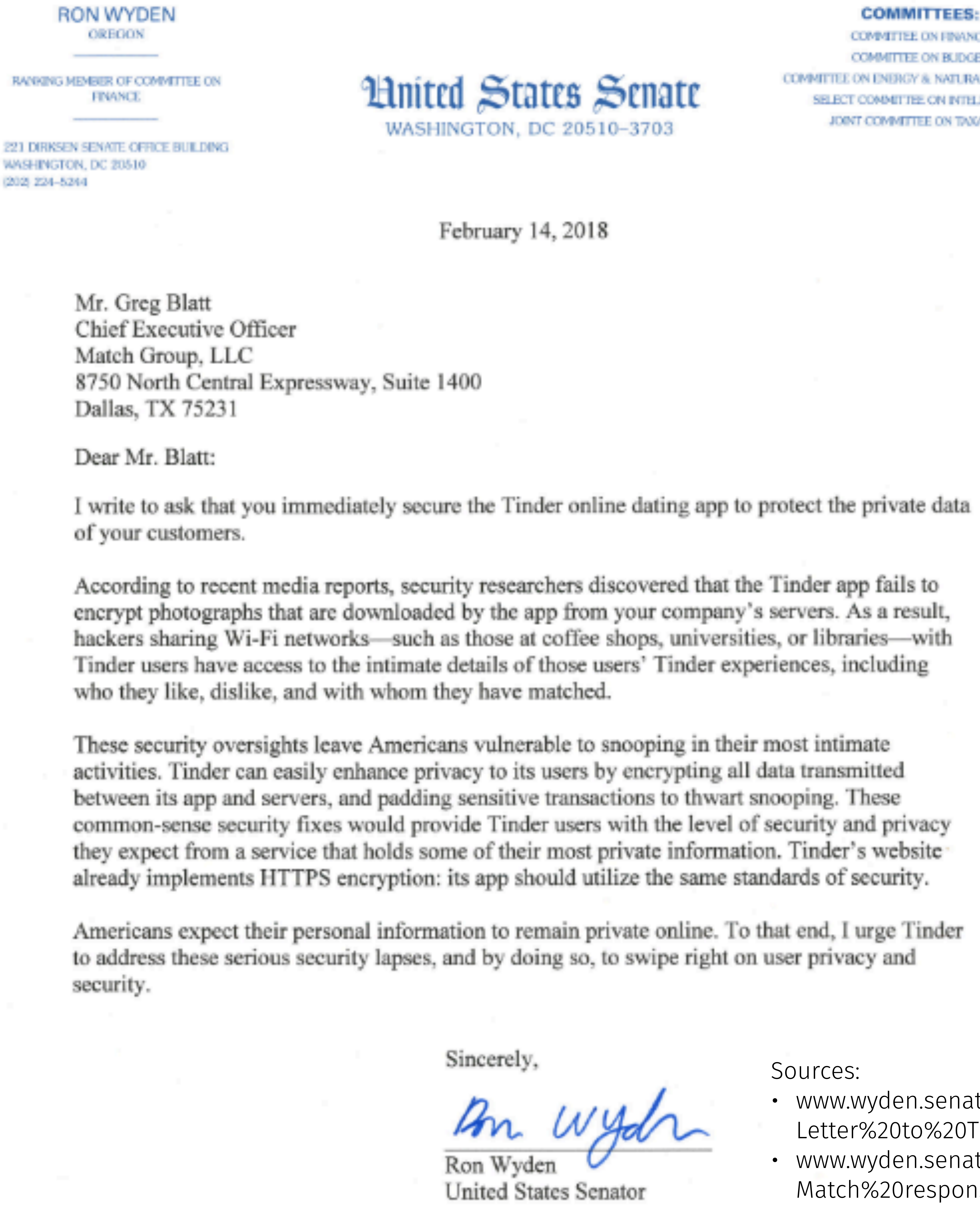
???

Eve’s powers we can handle

- Control over the network: add, drop, alter, re-order packets
- Intermittent control of an endpoint: we can still provide confidentiality at other times

Eve can still learn metadata

- No anonymity: Eve knows Alice and Bob are communicating
- No hiding message length: Eve sees how much data is flowing across the wire
- [Much more if you mess up…]



RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

February 14, 2018

Mr. Greg Blatt
Chief Executive Officer
Match Group, LLC
8750 North Central Expressway, Suite 1400
Dallas, TX 75231

Dear Mr. Blatt:

I write to ask that you immediately secure the Tinder online dating app to protect the private data of your customers.

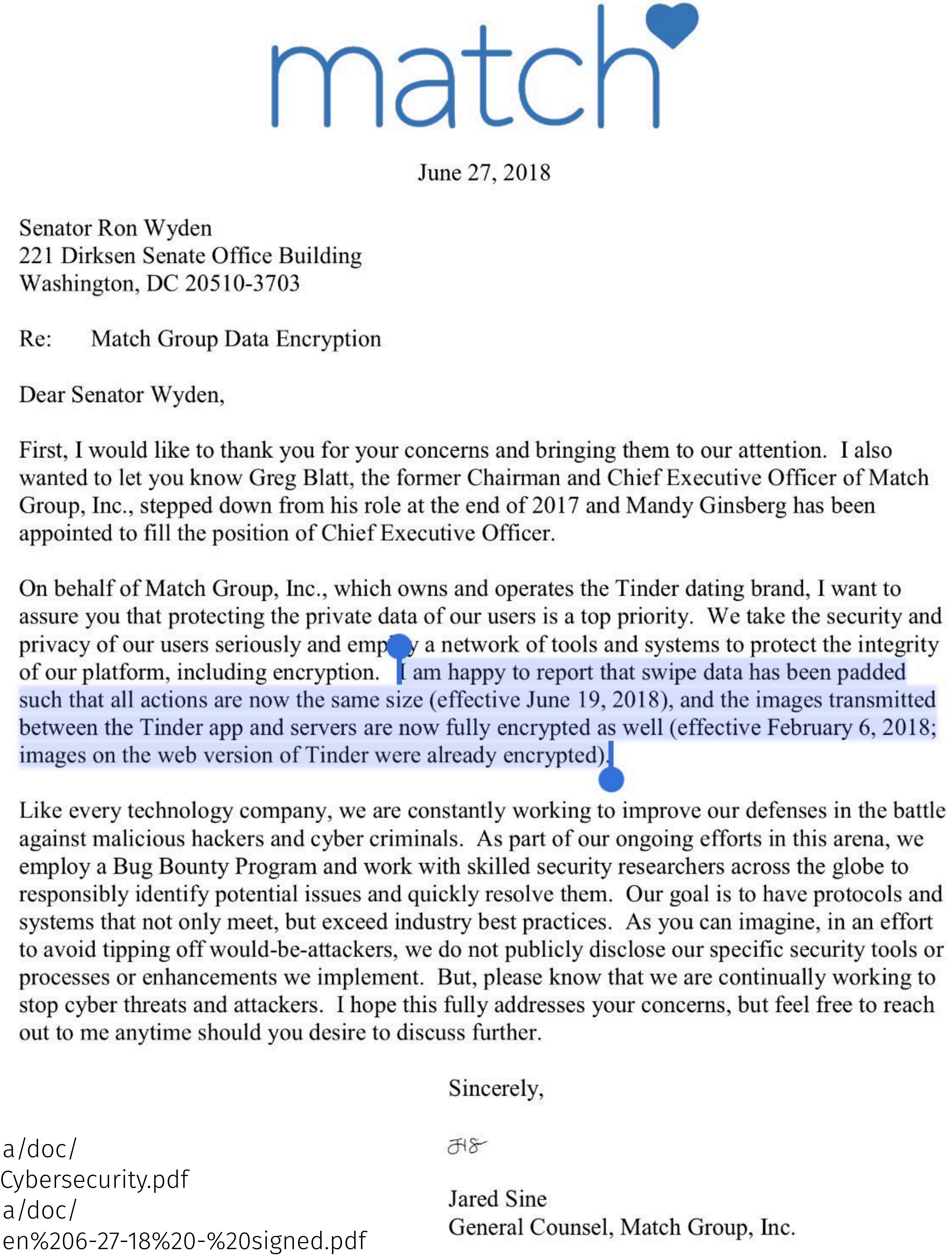
According to recent media reports, security researchers discovered that the Tinder app fails to encrypt photographs that are downloaded by the app from your company's servers. As a result, hackers sharing Wi-Fi networks—such as those at coffee shops, universities, or libraries—with Tinder users have access to the intimate details of those users' Tinder experiences, including who they like, dislike, and with whom they have matched.

These security oversights leave Americans vulnerable to snooping in their most intimate activities. Tinder can easily enhance privacy to its users by encrypting all data transmitted between its app and servers, and padding sensitive transactions to thwart snooping. These common-sense security fixes would provide Tinder users with the level of security and privacy they expect from a service that holds some of their most private information. Tinder's website already implements HTTPS encryption: its app should utilize the same standards of security.

Americans expect their personal information to remain private online. To that end, I urge Tinder to address these serious security lapses, and by doing so, to swipe right on user privacy and security.

Sincerely,

Ron Wyden
United States Senator



match

June 27, 2018

Senator Ron Wyden
221 Dirksen Senate Office Building
Washington, DC 20510-3703

Re: Match Group Data Encryption

Dear Senator Wyden,

First, I would like to thank you for your concerns and bringing them to our attention. I also wanted to let you know Greg Blatt, the former Chairman and Chief Executive Officer of Match Group, Inc., stepped down from his role at the end of 2017 and Mandy Ginsberg has been appointed to fill the position of Chief Executive Officer.

On behalf of Match Group, Inc., which owns and operates the Tinder dating brand, I want to assure you that protecting the private data of our users is a top priority. We take the security and privacy of our users seriously and employ a network of tools and systems to protect the integrity of our platform, including encryption. I am happy to report that swipe data has been padded such that all actions are now the same size (effective June 19, 2018), and the images transmitted between the Tinder app and servers are now fully encrypted as well (effective February 6, 2018; images on the web version of Tinder were already encrypted).

Like every technology company, we are constantly working to improve our defenses in the battle against malicious hackers and cyber criminals. As part of our ongoing efforts in this arena, we employ a Bug Bounty Program and work with skilled security researchers across the globe to responsibly identify potential issues and quickly resolve them. Our goal is to have protocols and systems that not only meet, but exceed industry best practices. As you can imagine, in an effort to avoid tipping off would-be-attackers, we do not publicly disclose our specific security tools or processes or enhancements we implement. But, please know that we are continually working to stop cyber threats and attackers. I hope this fully addresses your concerns, but feel free to reach out to me anytime should you desire to discuss further.

Sincerely,

Jared Sine
General Counsel, Match Group, Inc.

Sources:

- www.wyden.senate.gov/imo/media/doc/Letter%20to%20Tinder%20on%20Cybersecurity.pdf
- www.wyden.senate.gov/imo/media/doc/Match%20response%20to%20wyden%206-27-18%20-%20signed.pdf

Confidentiality

Integrity

Availability

Confidentiality

- Message privacy
- Entity privacy (aka anonymity)
- Deniability of transmission
- Withstand device compromise

Integrity

- Message authenticity
- Entity authenticity
- Message binding / non-malleability
- Message freshness

Availability

> “Confidentiality xor authenticity is **not possible**. If you don't have both, often you don't have either.”

–Prof. Matthew Green, Johns Hopkins

Nevertheless, we start by focusing on privacy without authenticity...

Objectives of this course

Crypto = Scientific field at intersection of many disciplines

Algorithms

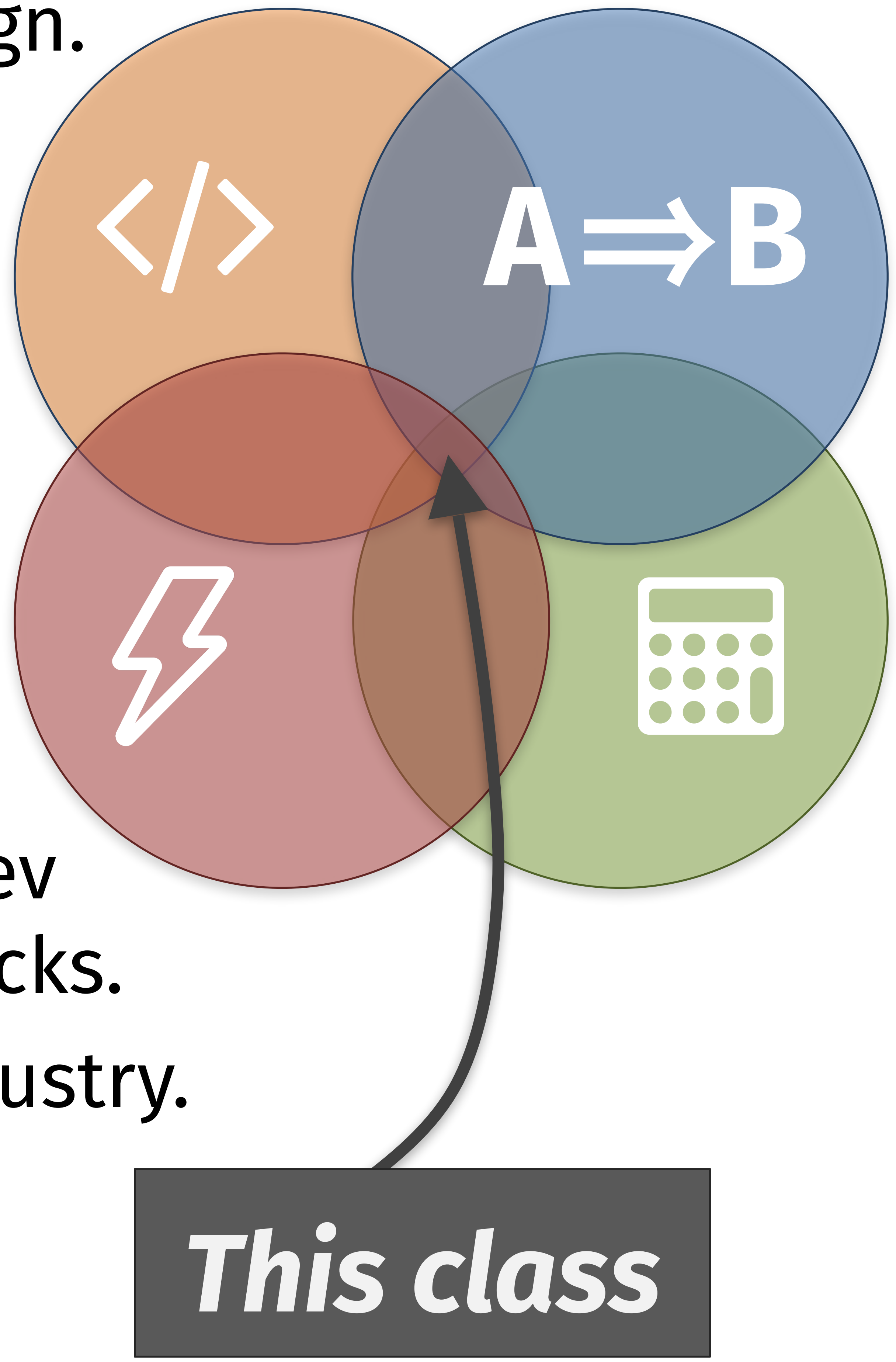
Known for cipher design.

Primarily found in European academia.

Complexity theory

Known for reductions.

Primarily found in American academia.



Engineering

Known for software dev and side channel attacks.

Primarily found in industry.

Mathematics

Known for cryptanalysis.

Primarily found in government.

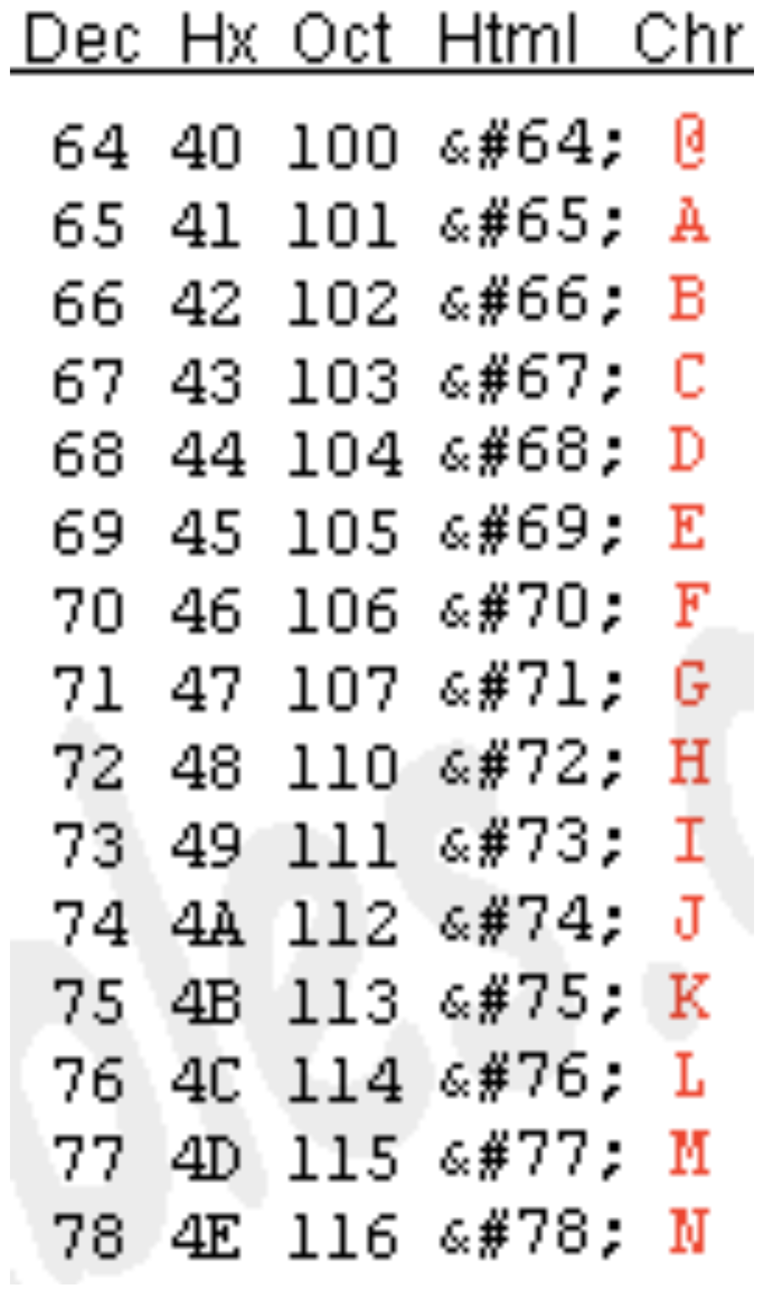
Representations of data

Quantities

- bit $\in \{0,1\}$
- byte $\in \{0,1\}^8$

Data types to encode bytes

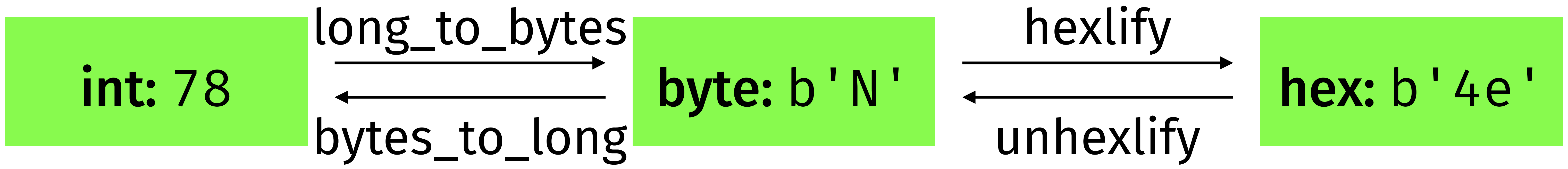
- Decimal integer
- Hex character string
- Raw bytes
  (some are ASCII printable)



Dec	Hx	Oct	Html	Chr
64	40	100	&#64;	@
65	41	101	&#65;	A
66	42	102	&#66;	B
67	43	103	&#67;	C
68	44	104	&#68;	D
69	45	105	&#69;	E
70	46	106	&#70;	F
71	47	107	&#71;	G
72	48	110	&#72;	H
73	49	111	&#73;	I
74	4A	112	&#74;	J
75	4B	113	&#75;	K
76	4C	114	&#76;	L
77	4D	115	&#77;	M
78	4E	116	&#78;	N

Useful Python3 methods

- from binascii import hexlify, unhexlify
- from Crypto.Util.strxor import strxor
- from Crypto.Util.number import bytes_to_long, long_to_bytes



int: 78

long_to_bytes

bytes_to_long

byte: `b'N'`

hexlify

unhexlify

hex: `b'4e'`

Warnings when completing homework assignments!

- Keep track of data formats during homework! If your output length is double/half what you expected, then you have a format bug

- Don't use strings with UTF-8 encoding! (contrary to the name, this encoding doesn't guarantee that each char is represented with 8 bits)

- The goal of homework is to explore crypto done well/poorly, so the code from the homework usually should *not* be used in practice