02. Usable Encryption

Blase Ur

April 4th, 2019

CMSC 23210 / 33210

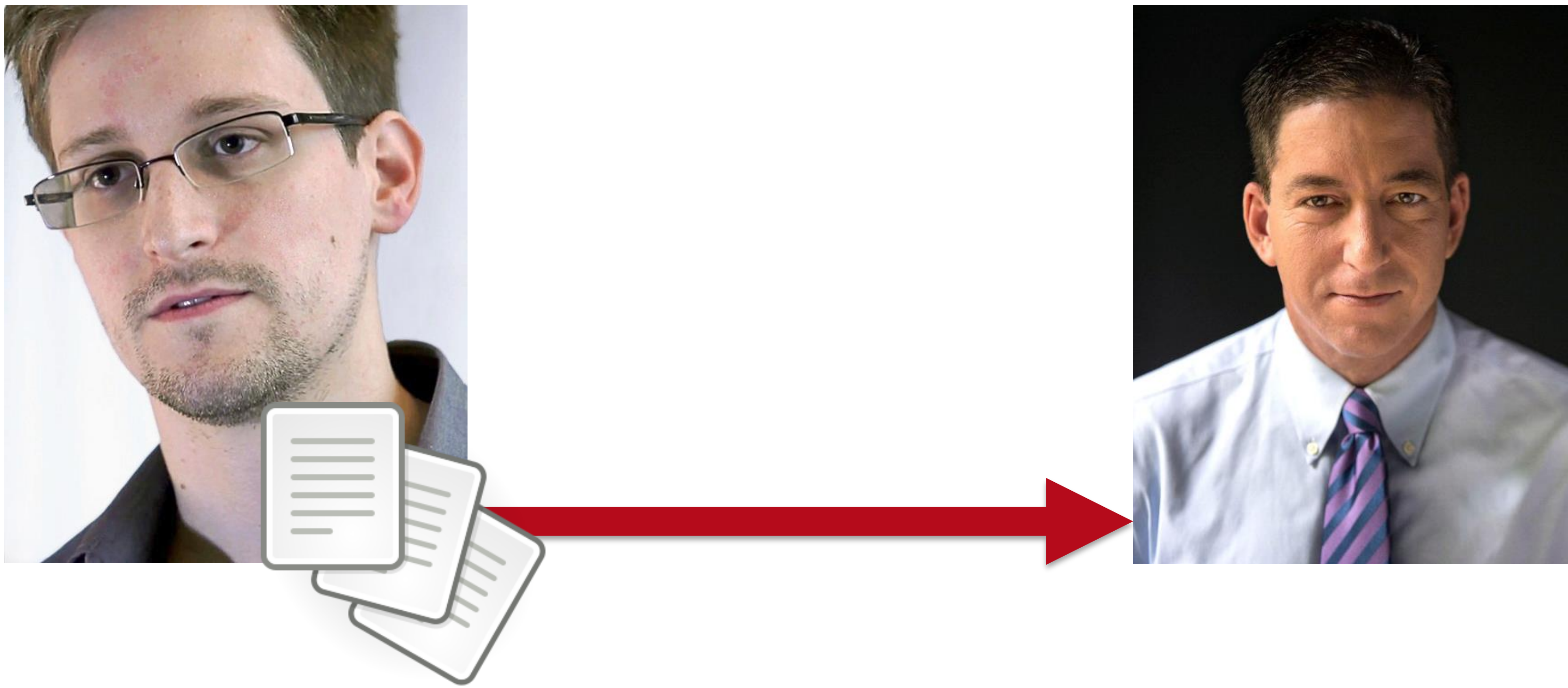
THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy Education & Research

Why Glenn couldn't encrypt

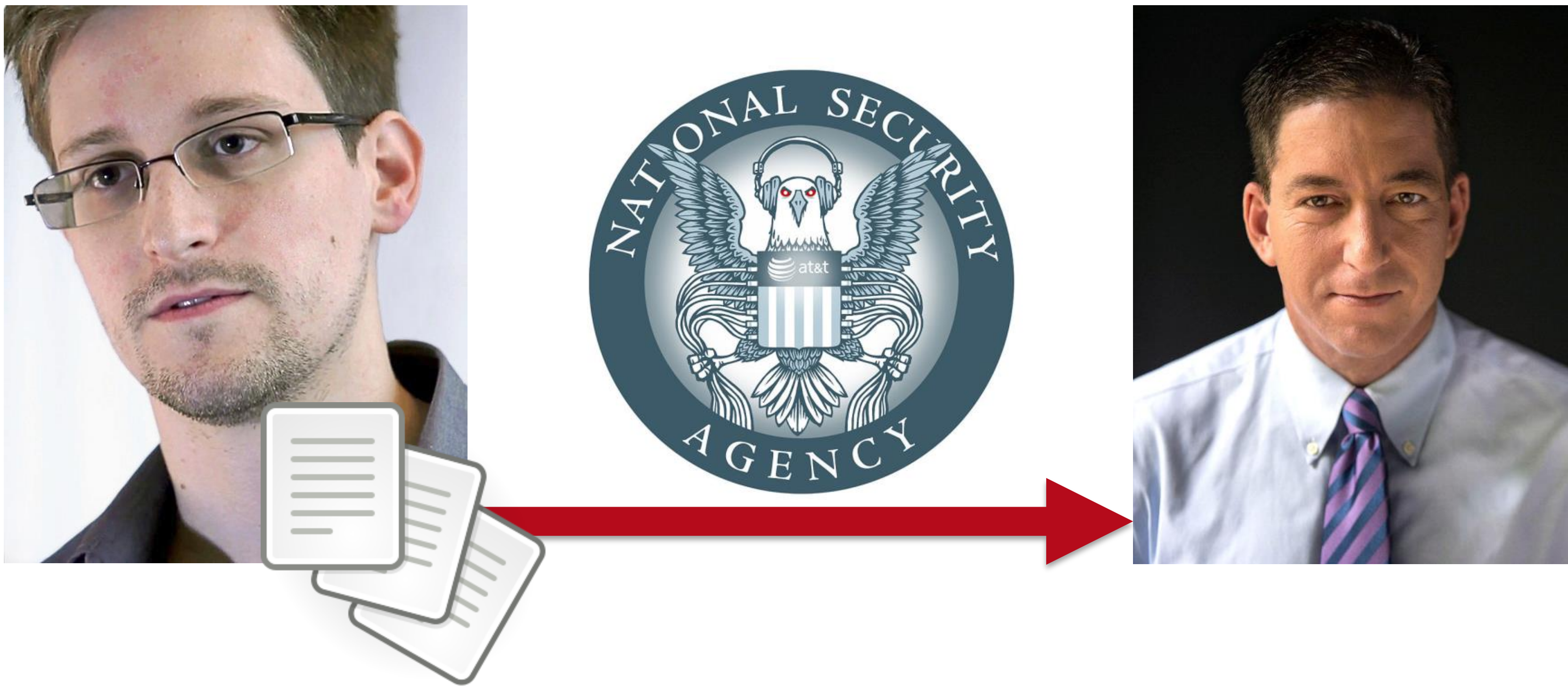
Why Glenn couldn't encrypt

Why Glenn couldn't encrypt



Snowden image public domain from Laura Poitras. Document image CC by GNOME icon authors
Greenwald image CC by David dos Dantos - mynewsdesk, https://commons.wikimedia.org/w/index.php?curid=36965640
NSA logo CC by the Electronic Frontier Foundation

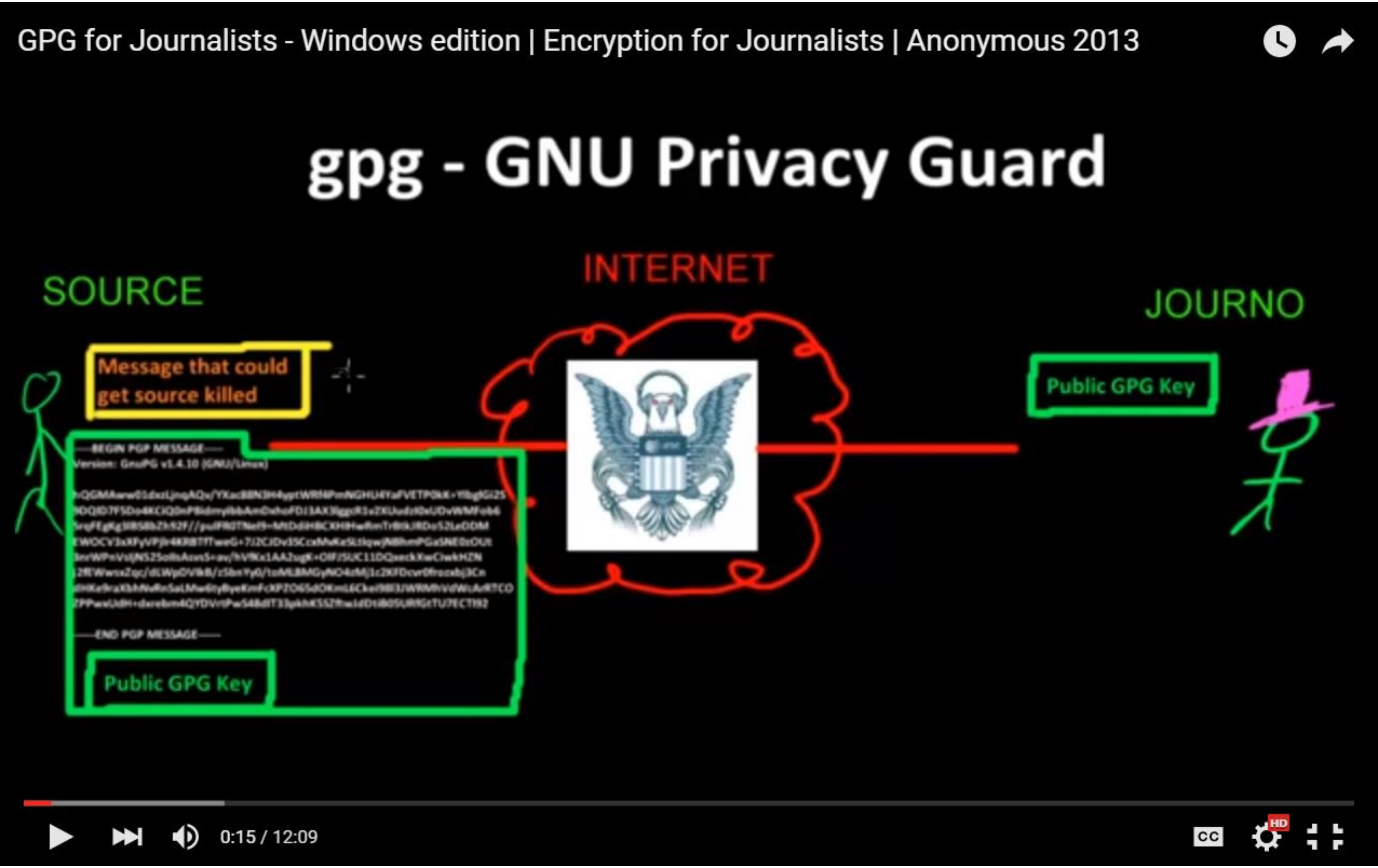
Why Glenn couldn't encrypt



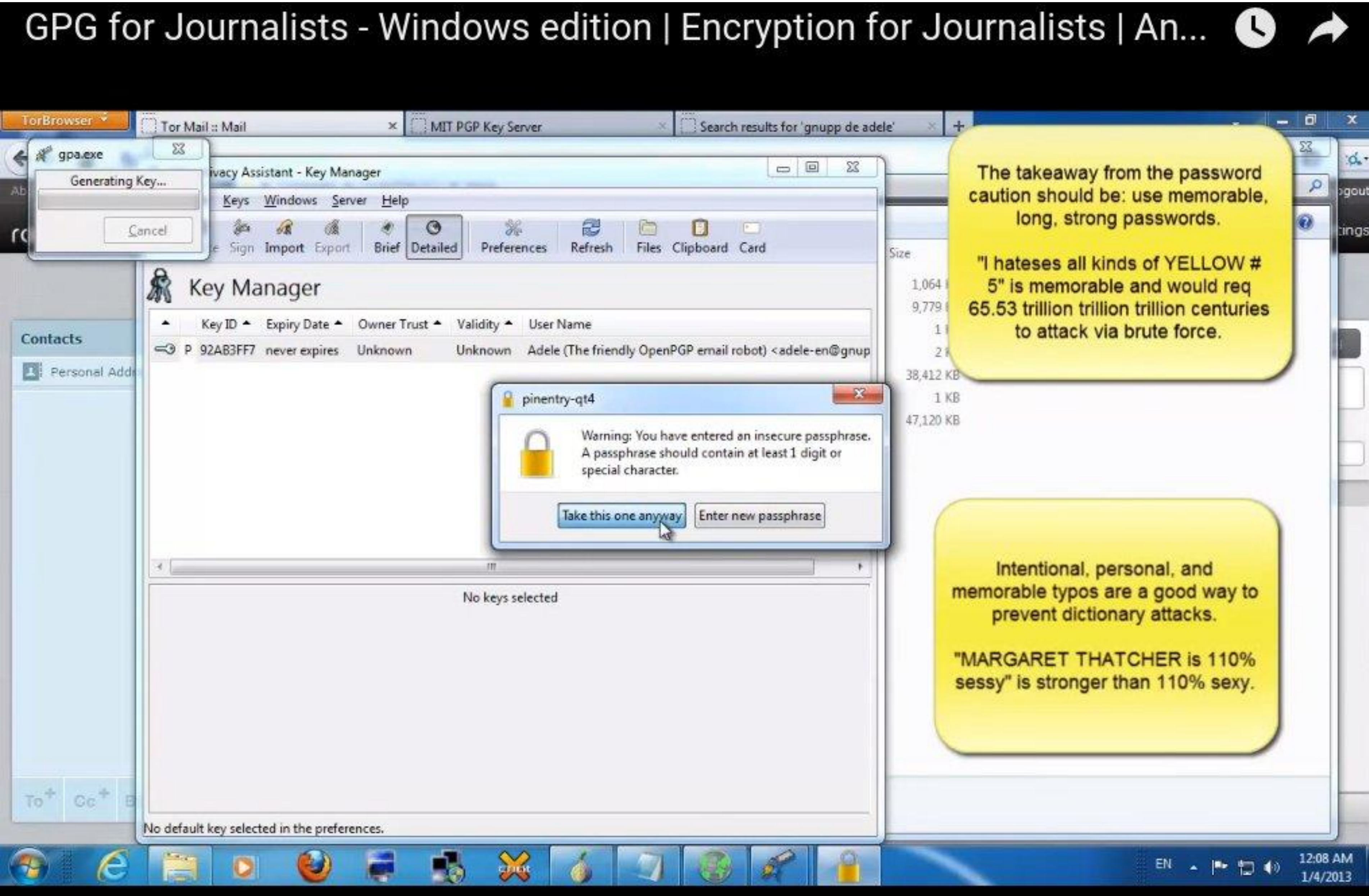
Why Glenn couldn't encrypt

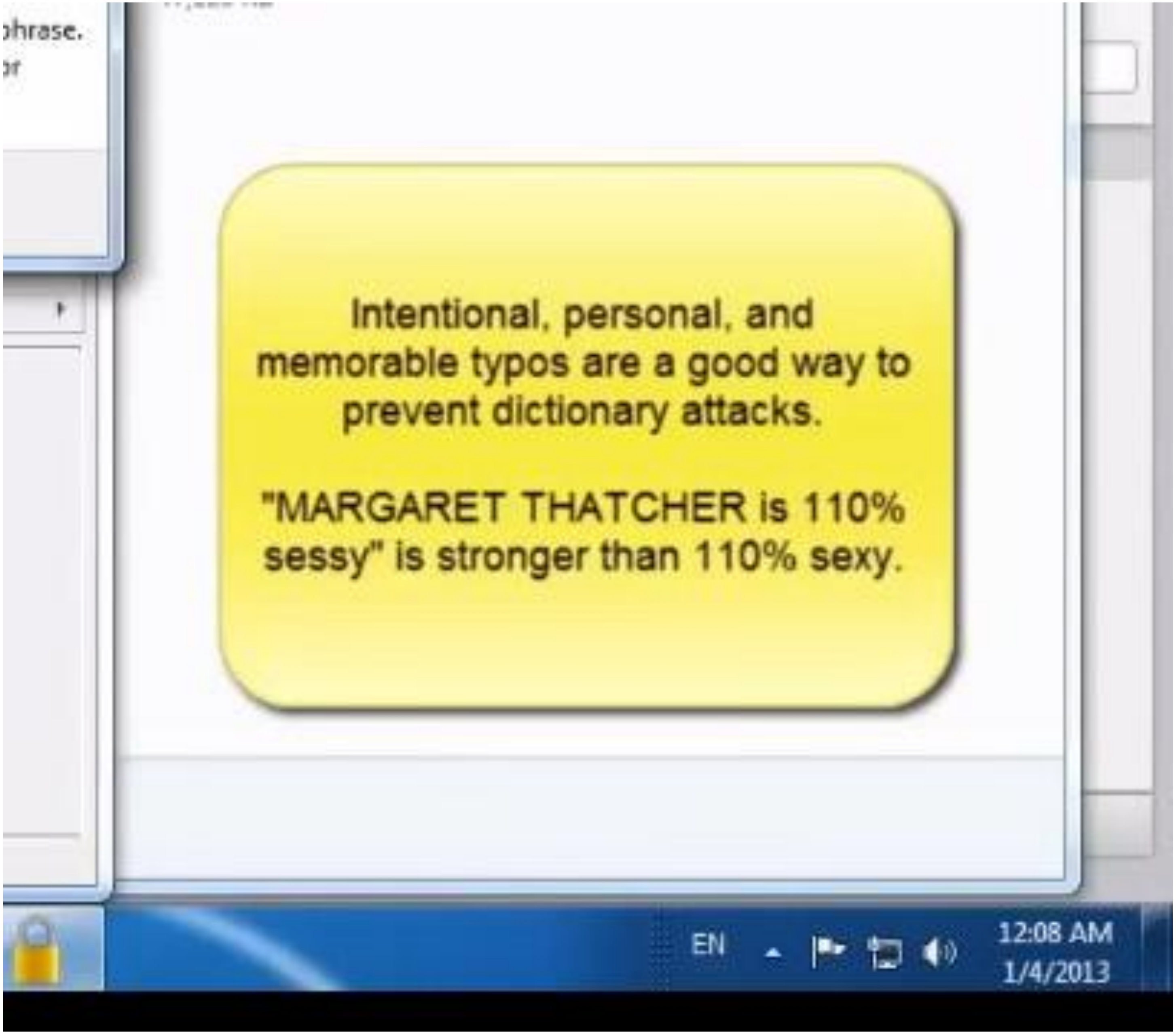
- http://vimeo.com/56881481
  - 1:50 – 3:37, 4:10 – 4:58, 11:15 – 11:43
- "And yet, Greenwald still didn't bother learning security protocols. 'The more he sent me, the more difficult it seemed,' he says. 'I mean, now I had to watch a f***ing video . . . ?'"
- Snowden ended up reaching out to Laura Poitras instead

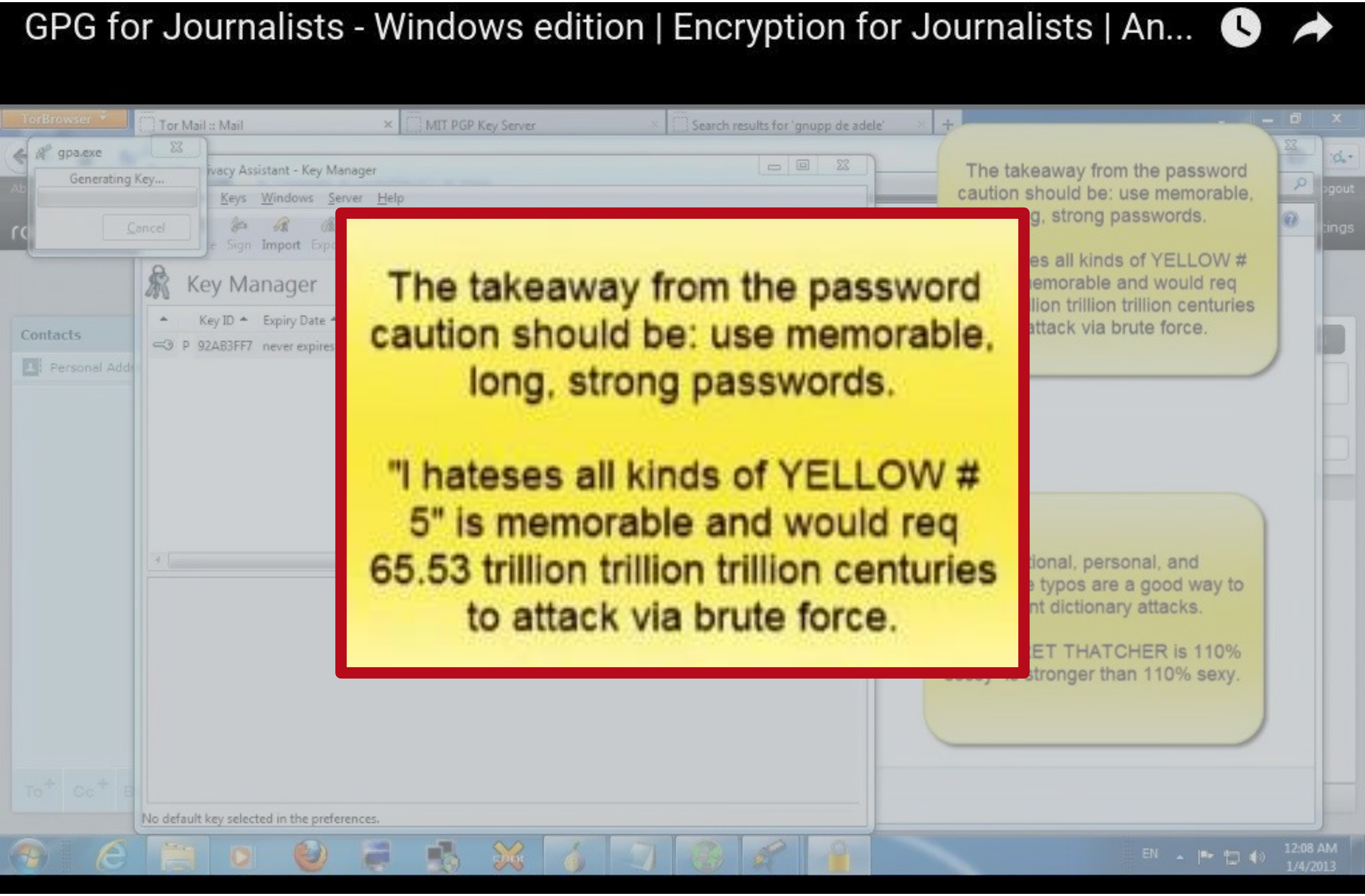
http://www.rollingstone.com/politics/news/snowden-and-greenwald-the-men-who-leaked-the-secrets-20131204
http://www.dailydot.com/politics/edward-snowden-gpg-for-journalists-video-nsa-glenn-greenwald/


GPG for Journalists - Windows edition | Encryption for Journalists | Anonymous 2013
gpg - GNU Privacy Guard
SOURCE
INTERNET
JOURNO
Message that could get source killed
-----BEGIN PGP MESSAGE-----
-----END PGP MESSAGE-----
Public GPG Key
Public GPG Key
0:15 / 12:09


GPG for Journalists - Windows edition | Encryption for Journalists | An...
Tor Mail :: Mail
MIT PGP Key Server
Search results for 'gnupp de adele'
gpa.exe
Generating Key...
Cancel
ivacy Assistant - Key Manager
Keys Windows Server Help
Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Expiry Date Owner Trust Validity User Name
P 92AB3FF7 never expires Unknown Unknown Adele (The friendly OpenPGP email robot) <adele-en@gnup
pinentry
Enter passphrase
Passphrase
Quality:
OK
Cancel
No keys selected
No default key selected in the preferences.
Contacts
Personal Add
Size
1,064 KB
9,779 KB
1 KB
2 KB
38,412 KB
1 KB
47,120 KB
EN
12:08 AM
1/4/2013


GPG for Journalists - Windows edition | Encryption for Journalists | An...
TorBrowser
Tor Mail :: Mail
MIT PGP Key Server
Search results for 'gnupp de adele'
gpa.exe
Generating Key...
Cancel
ivacy Assistant - Key Manager
Keys Windows Server Help
Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Key ID Expiry Date Owner Trust Validity User Name
P 92AB3FF7 never expires Unknown Unknown Adele (The friendly OpenPGP email robot) <adele-en@gnup
pinentry-qt4
Warning: You have entered an insecure passphrase. A passphrase should contain at least 1 digit or special character.
Take this one anyway
Enter new passphrase
No keys selected
No default key selected in the preferences.
Contacts
Personal Addr
The takeaway from the password caution should be: use memorable, long, strong passwords.
"I hateses all kinds of YELLOW # 5" is memorable and would req 65.53 trillion trillion trillion centuries to attack via brute force.
Intentional, personal, and memorable typos are a good way to prevent dictionary attacks.
"MARGARET THATCHER is 110% sessy" is stronger than 110% sexy.
12:08 AM
1/4/2013


Intentional, personal, and memorable typos are a good way to prevent dictionary attacks.
"MARGARET THATCHER is 110% sessy" is stronger than 110% sexy.
EN
12:08 AM
1/4/2013


GPG for Journalists - Windows edition | Encryption for Journalists | An...
The takeaway from the password caution should be: use memorable, long, strong passwords.
"I hateses all kinds of YELLOW # 5" is memorable and would req 65.53 trillion trillion trillion centuries to attack via brute force.
Key Manager
Keys Windows Server Help
Sign Import
Key ID Expiry Date
P 92AB3FF7 never expires
Contacts
gpa.exe
Generating Key...
Cancel
Tor Mail :: Mail
MIT PGP Key Server
No default key selected in the preferences.
12:08 AM
1/4/2013

This World of Ours

Encryption: A crash course

Encryption basics

- Putting information in code so that unauthorized people can't read it
- What might you want to encrypt?
  - Email or text message
  - Individual file
  - Hard drive, USB stick
  - Communication with a website
  - Everything

One-way functions

- Easy to compute in one direction, but hard to compute in the other
- Hash function
  - Small change in input → big change in output
  - md5("blase") = `12b872adb2588c668d706d847fc1da7e`
- Used for storing passwords
- Current research: make hashing <u>slow</u>
  - (Older and less good) bcrypt: iterated hashes
  - scrypt and Argon2: memory-hard

Trapdoor functions

- Easy to compute in one direction, but hard to compute in the other unless you have some extra information
- Encryption: reversible (if you know secret)
  - "this is a test" → `Xe0yUqyOnY8JskyCQ2cYIg==`
  - `Xe0yUqyOnY8JskyCQ2cYIg==` and `chicago` (secret) → "this is a test"

Two main encryption approaches

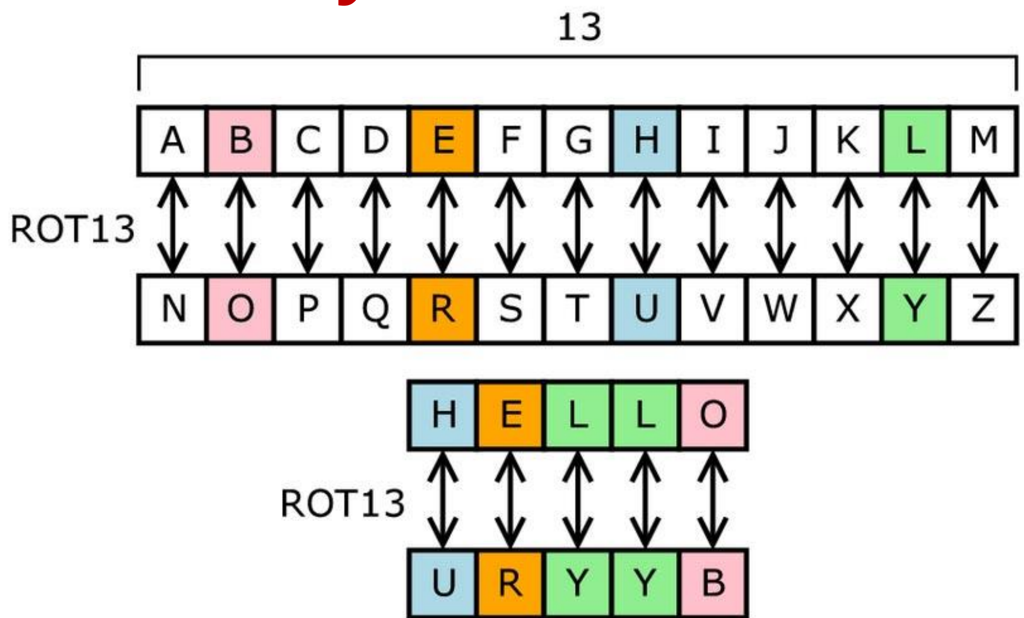
- Symmetric encryption: Same key used for encryption and decryption
  - Requires key exchange (out of band)
  - Prominent examples: AES, DES, etc.
- Asymmetric encryption: Different keys used for encryption and decryption
  - Keypair: public key and private key
  - Prominent examples: RSA, ElGamal, elliptic curve crypto

Properties of encryption

- **Secrecy**: Is Blase the only person who can decrypt my message?
- **Integrity**: Has someone tampered with Blase's message?
- **Authenticity**: Did this message really come from Blase?

Encryption historically

- Caesar shift



- Substitution cipher

CIPHER ALPHABET

A = B	H = A	O = O	V = L
B = V	I = D	P = Y	W = P
C = G	J = Z	Q = F	X = U
D = Q	K = C	R = J	Y = I
E = K	L = W	S = X	Z = R
F = M	M = S	T = H	
G = N	N = E	U = T	

Figure 1

Encryption historically

- Vigenère cipher

- Enigma machine

Block ciphers (symmetric)

- Old (deprecated): DES → 3DES
- AES (Advanced Encryption Standard)
  - Rijndael Cipher (chosen in 2001)
  - 128-bit blocks
  - 128-, 192-, or 256-bit keys
  - https://www.youtube.com/watch?v=evjFwDRTmV0
- No known* feasible* attacks on AES
- Timing side-channel attacks possible

Public key (asymmetric) crypto

- 1970s – Present

Diffie-Hellman key exchange

- 1976: Diffie, Hellman, Merkle
- (Multiplicative group of integers mod p)
- Generator g
- Prime number p
- Secrets (integers) x and y

Diffie-Hellman key exchange

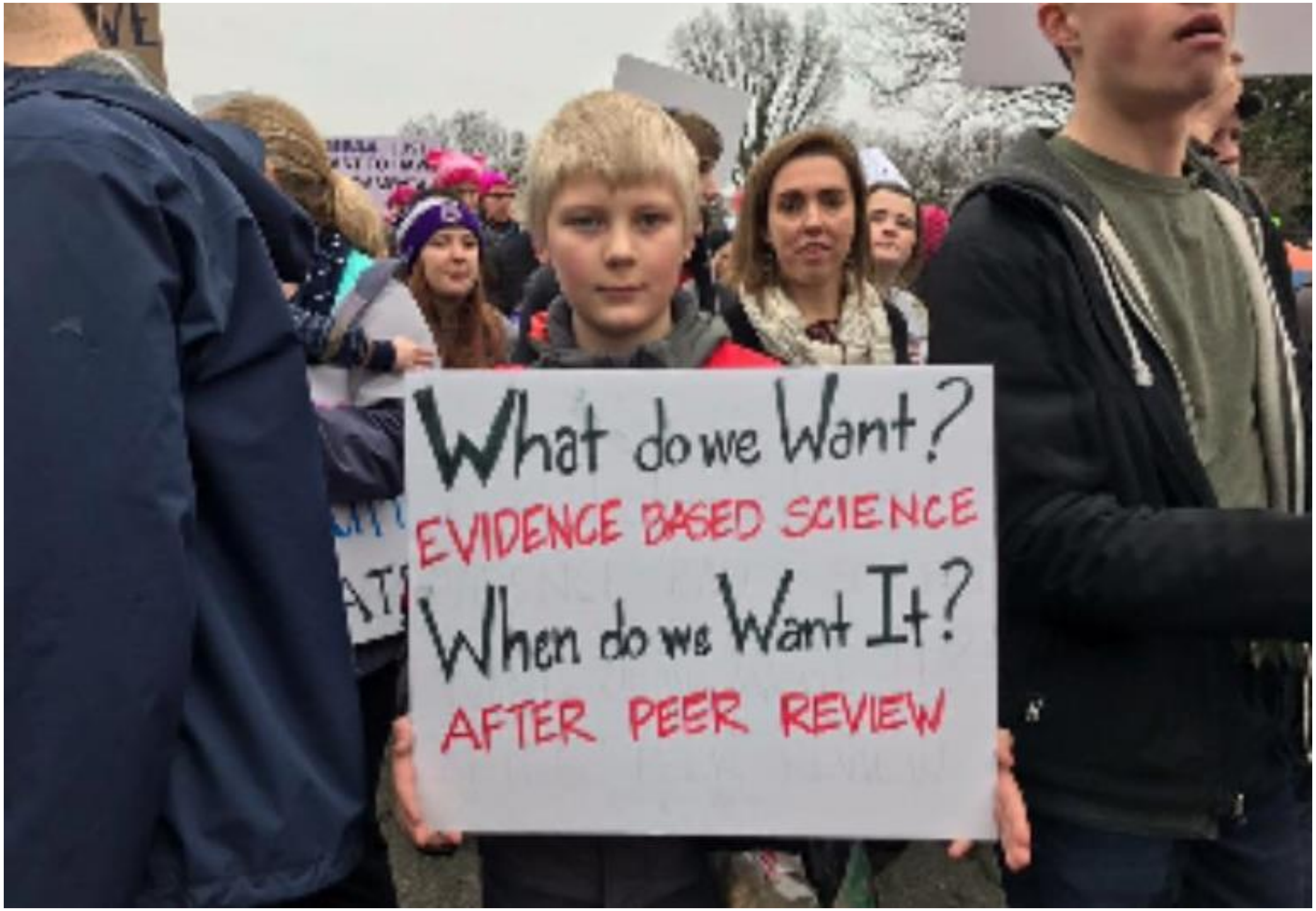
RSA

- Generate a key:
  - Choose primes p, q
  - Calculate $n = p \cdot q$
  - Private key: $\lambda(n) = lcm(p-1, q-1)$
  - Choose integer e so $1 < e < \lambda(n)$ and $e, \lambda(n)$ coprime
  - Solve for d such that $d \cdot e \equiv 1 \pmod{\lambda(n)}$
  - Release e and n as the public key, but keep d private
- To encrypt: $c \equiv m^e \ (mod\ n)$
- To decrypt: c^d
  - Equivalent to $m^{ed} \ (mod\ n)$, which is just m

Usable encryption

Why do user studies?

Purpose	Useful to...
Assess needs	Decide what to build
Evaluate	Determine whether system meets requirements and what needs to be improved
Understand tradeoffs	Decide which features/approaches/systems best fit particular needs
Find root causes	Determine where redesigns or new approaches are needed


What do we Want?
EVIDENCE BASED SCIENCE
When do we Want It?
AFTER PEER REVIEW

User study steps

- Identify research questions, metrics, and use cases
- Decide on type of study and design study protocol
- Develop detailed scripts, surveys, scenarios, incentives, instrumentation, prototypes, recruiting materials, etc.
- Obtain ethics approval
- Pilot and iterate on study design
- Collect data
- Analyze results
- Repeat some or all of these steps as needed

Usable security study challenges

- Keeping it real (ecological validity)
  - Create realistic sense of risk **(but not real risk)**
  - Provide realistic incentives
  - Don't bias participants
- Measuring the right thing
  - Design the right protocol
  - Control the variables
  - Instrument
- Observing infrequent events and small differences
- Legal, ethical, and practical issues

Why Johnny can’t encrypt

- Why can’t Johnny encrypt?
- Why was it so hard for participants to complete the tasks?
- How did the experimenters motivate the tasks and get participants to care about security?
- What role did attackers play in this user study?

Why Johnny can't encrypt

- Classic paper in usable security (1999)
- Interfaces are bad
- Metaphors are wrong (and confusing)
- Opaque process
- Key management is difficult

Why Johnny can't encrypt

- Security principles
  - Unmotivated user
  - Abstraction property
  - Lack of feedback
  - Barn door property
  - Weakest link property
- Cognitive walkthrough vs. user test
- Bad metaphors