CSE 484 / CSE M 584

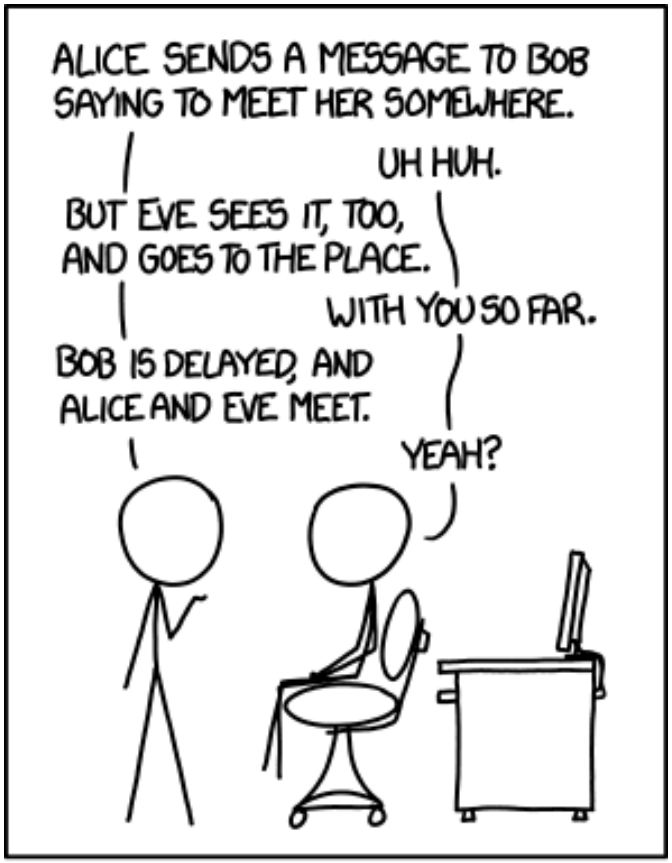
Computer Security: Crypto & Web Security

TA: Thomas Crosley

tcrosley@cs

Many slides by Franziska Roesner and Adrian Sham

HTTP://XKCD.COM/1323/



Lab 1 Deadline Reminders

- Lab 1 Final due tomorrow! (4/29, 8pm).
- Upcoming office hours:
  - Friday 2:00pm – Kevin (CSE 021)

Today

- Crypto Summary
- RSA Summary
- Certificate Authorities
- Security Best Practices

Cryptography Summary

- Goal: Privacy
  - Symmetric keys:
    - One-time pad, Stream ciphers
    - Block ciphers (e.g., DES, AES) → modes: EBC, CBC, CTR
  - Public key crypto (e.g., Diffie-Hellman, RSA)
- Goal: Integrity
  - MACs, often using hash functions (e.g, MD5, SHA-256)
- Goal: Privacy and Integrity
  - Encrypt-then-MAC
- Goal: Authenticity (and Integrity)
  - Digital signatures (e.g., RSA, DSS)

RSA Summary

- Key generation
  - Generate large primes p, q (and keep them private)
    - Say, 1024 bits each (need primality testing, too)
  - Compute $n = pq$ and $\varphi(n) = (p-1)(q-1)$
  - Choose small e, relatively prime to $\varphi(n)$
  - Compute unique d such that $ed \equiv 1 \bmod \varphi(n)$
  - Public key = (e,n); private key = (d,n)
- Encryption of m: $c \equiv m^e \bmod n$
  - m must be, $0 <= m < n$
  - Modular exponentiation by repeated squaring
- Decryption of c: $c^d \bmod n = (m^e)^d \bmod n = m$

Sample RSA Decryption

- 26 2 15 13 7 14 13 13 1 28 14 15 13
  14 20 9 6 31 25 26 14 16 23 15 26 2 6 13 1
- p=3, q=11, n=33, e=7, d=3

- A-1 B-2 C-3 D-4 E-5 F-6 G-7 H-8 I-9 J-10 K-11
  L-12 M-13 N-14 O-15 P-16 Q-17 R-18 S-19 T-20
  U-21 V-22 W-23 X-24 Y-25 Z-26

Sample RSA Decryption

- How to compute d?
  - Recall: $ed \equiv 1 \bmod \varphi(n)$ (where $\varphi(n) = (p-1)(q-1)$)
  - So d is inverse of e mod φ(n).
  - How to compute modular inverse?
    - Use extended Euclidean algorithm
    - … or Wolfram Alpha ☺
    - Note that this is hard if you don't know φ(n) (i.e., can't factor n).

Certificates

CA Ecosystem

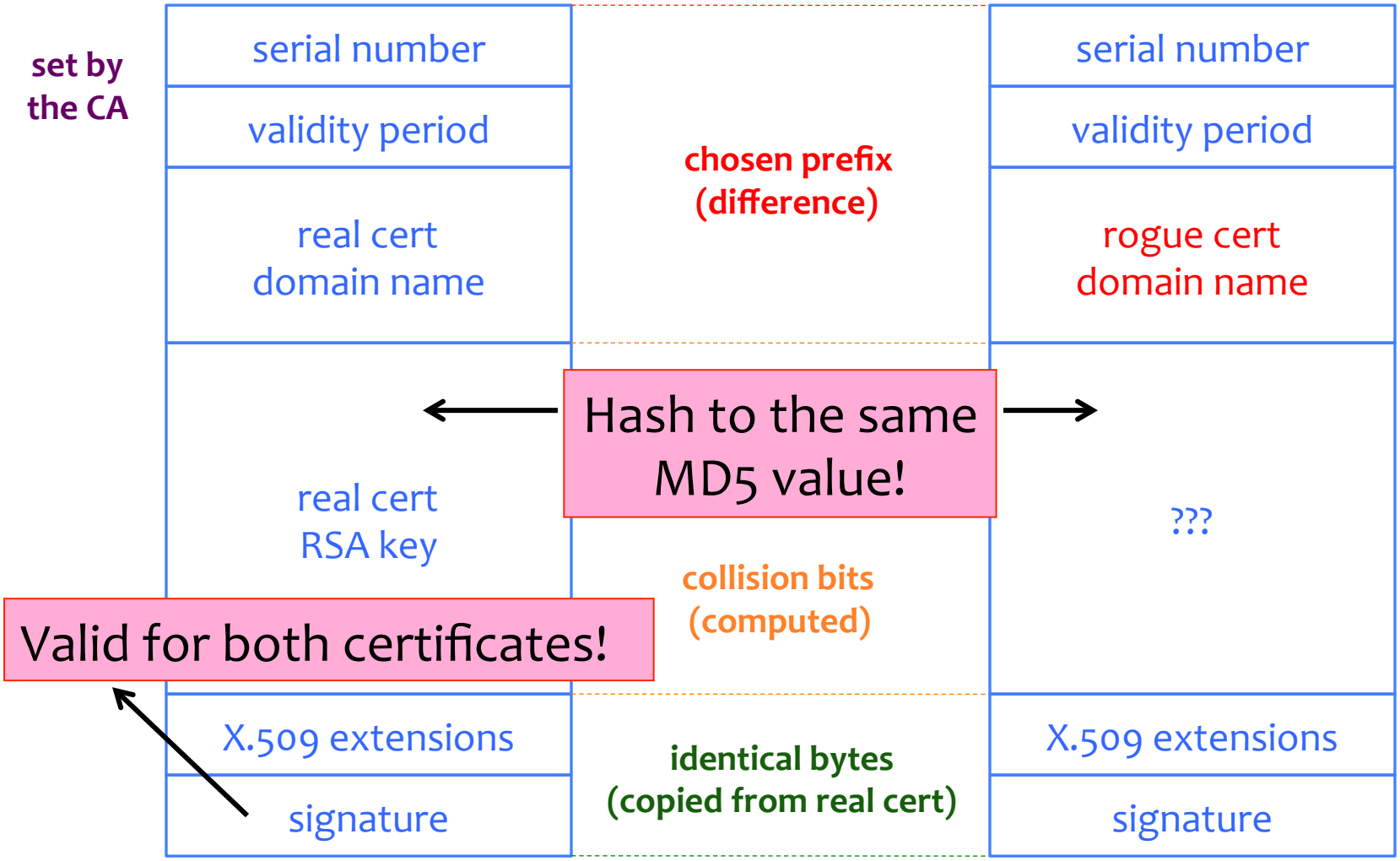
Organization Type	Organizations		Authorities		Leaf Certificates		Hosts	
Academic Institution	273	(39.79%)	292	(15.93%)	85,277	(2.46%)	85,277	(0.92%)
Commercial CA	135	(19.67%)	819	(44.70%)	3,260,454	(94.20%)	3,260,454	(76.33%)
Government Agency	85	(12.39%)	250	(13.64%)	17,865	(0.51%)	17,865	(0.23%)
Corporation	83	(12.09%)	191	(10.42%)	30,115	(0.87%)	30,115	(4.80%)
ISP	30	(4.37%)	58	(3.16%)	8,126	(0.23%)	8,126	(1.55%)
IT/Security Consultant	29	(4.22%)	88	(4.80%)	22,568	(0.65%)	22,568	(0.98%)
Financial Institution	17	(2.47%)	49	(2.67%)	2,412	(0.06%)	2,412	(0.03%)
Unknown	*unknown*		15	(0.81%)	2,535	(0.07%)	2,535	(0.02%)
Hosting Provider	7	(1.02%)	12	(0.65%)	10,598	(0.30%)	10,598	(14.70%)
Nonprofit Org	7	(1.02%)	15	(0.81%)	11,480	(0.33%)	11,480	(0.11%)
Library	5	(0.72%)	6	(0.32%)	281	(0.00%)	281	(0.00%)
Museum	4	(0.58%)	4	(0.21%)	35	(0.00%)	35	(0.00%)
Healthcare Provider	3	(0.43%)	4	(0.21%)	173	(0.00%)	173	(0.00%)
Religious Institution	1	(0.14%)	1	(0.05%)	11	(0.00%)	11	(0.00%)
Military	1	(0.14%)	27	(1.47%)	9,017	(0.26%)	9,017	(0.27%)

Table 3: Types of Organizations with Signing Certificates — We found 1,832 valid browser-trusted signing certificates belonging to 683 organizations. We classified these organizations and find that more than 80% of the organizations that control a signing certificate are not commercial certificate authorities.

Source: http://conferences.sigcomm.org/imc/2013/papers/imc257-durumericAemb.pdf

[Sotirov et al. "Rogue Certificates"]

Colliding Certificates



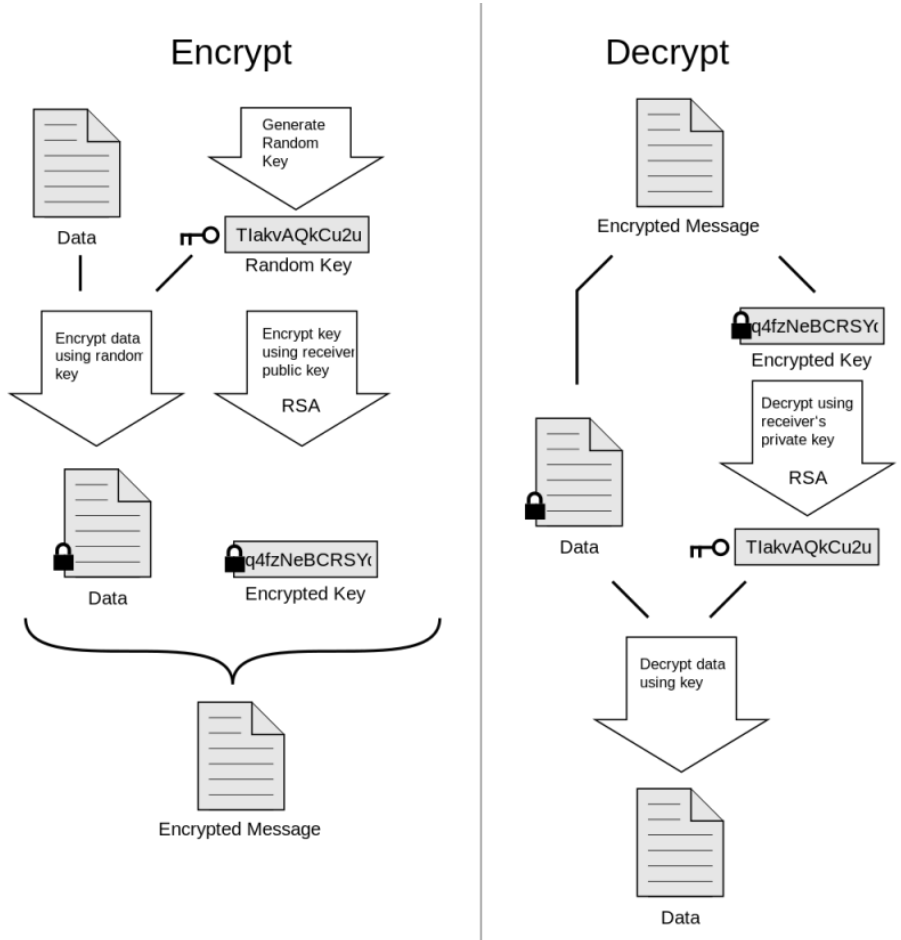
Problem With Collisions

- **Goal:** Snape wants to trick Dumbledore into accept a document B from Harry that is different than document A that Harry actually signed
- Snape creates 2 documents A and B that have identical hash value (collision!)
- Snape sends document A to Harry, who signs the hash and gives a signature to Snape
- Snape attaches that signature to document B and sends it to Dumbledore
- Dumbledore accepts it because the signatures match

More Rogue Certs

- In Jan 2013, a rogue *.google.com certificate was issued by an intermediate CA that gained its authority from the Turkish root CA TurkTrust
  - TurkTrust accidentally issued intermediate CA certs to customers who requested regular certificates
  - Ankara transit authority used its certificate to issue a fake *.google.com certificate in order to filter SSL traffic from its network
- This rogue *.google.com certificate was trusted by every browser in the world

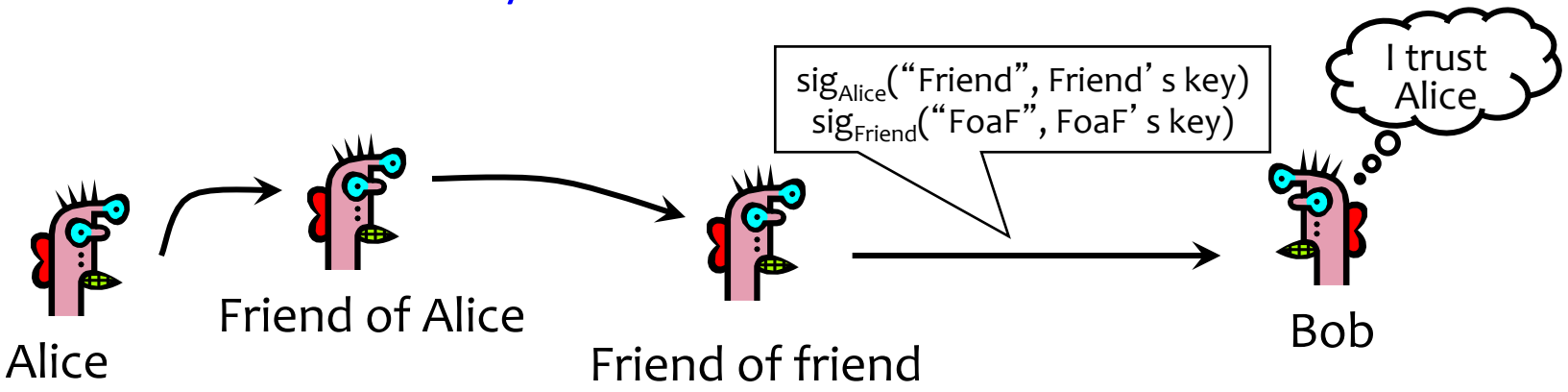
What is Pretty Good Privacy (PGP)



http://lifehacker.com/how-to-encrypt-your-email-and-keep-your-conversations-p-1133495744

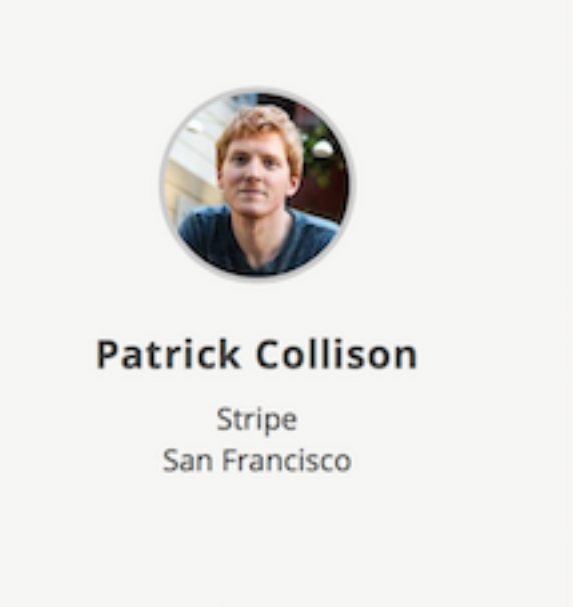
Alternative: "Web of Trust"

- Used in PGP (Pretty Good Privacy)
- Instead of a single root certificate authority, each person has a set of keys they "trust"
  - If public-key certificate is signed by one of the "trusted" keys, the public key contained in it will be deemed valid
- Trust can be transitive
  - Can use certified keys for further certification



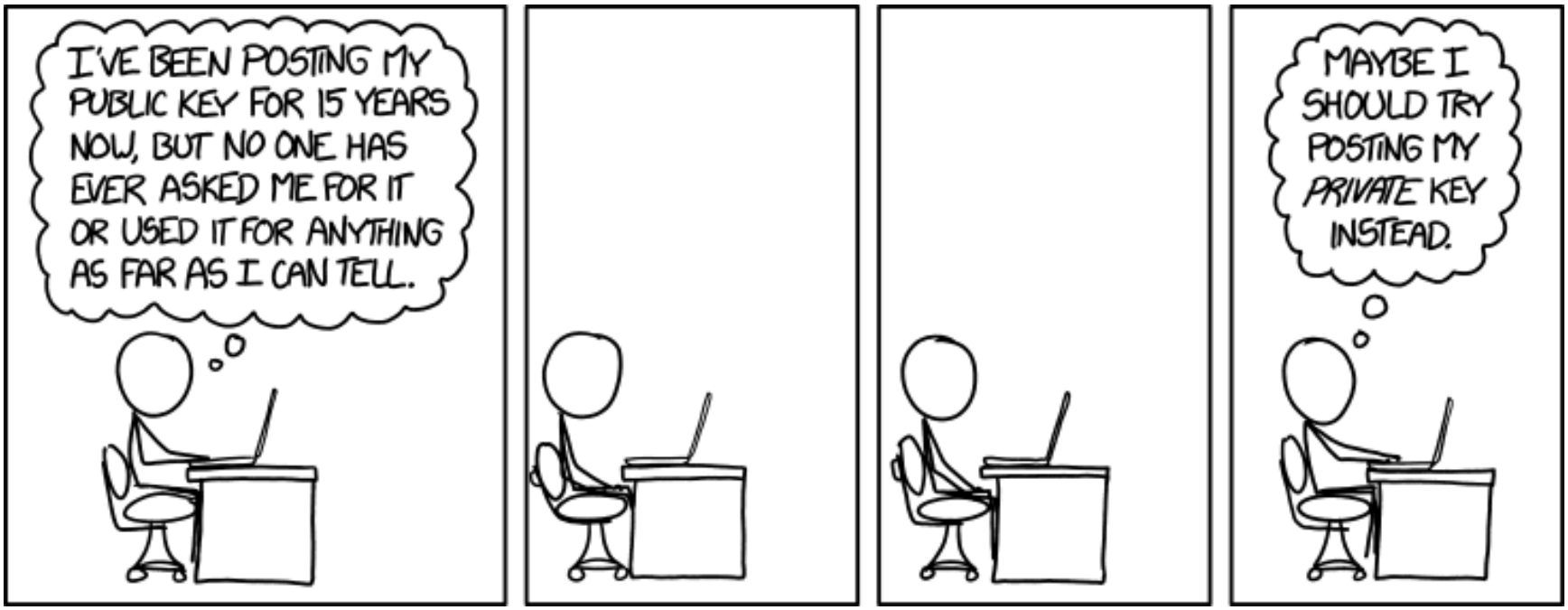
KeyBase

- Connect people's social media identities to their public cryptographic keys.



https://medium.com/@cdixon/keybase-bringing-public-key-cryptography-to-mainstream-users-16a9379dddda#.klwu6rt36

HTTP://XKCD.COM/1553/



Security Best Practices

Ad and Social Media Blocking

- Benefits
  - Can block malicious content from ads
  - Faster loading pages
  - Reduce bandwidth
  - Privacy
- Cons
  - Allows software to directly modify page
  - False positives
  - Economic consequences for online businesses

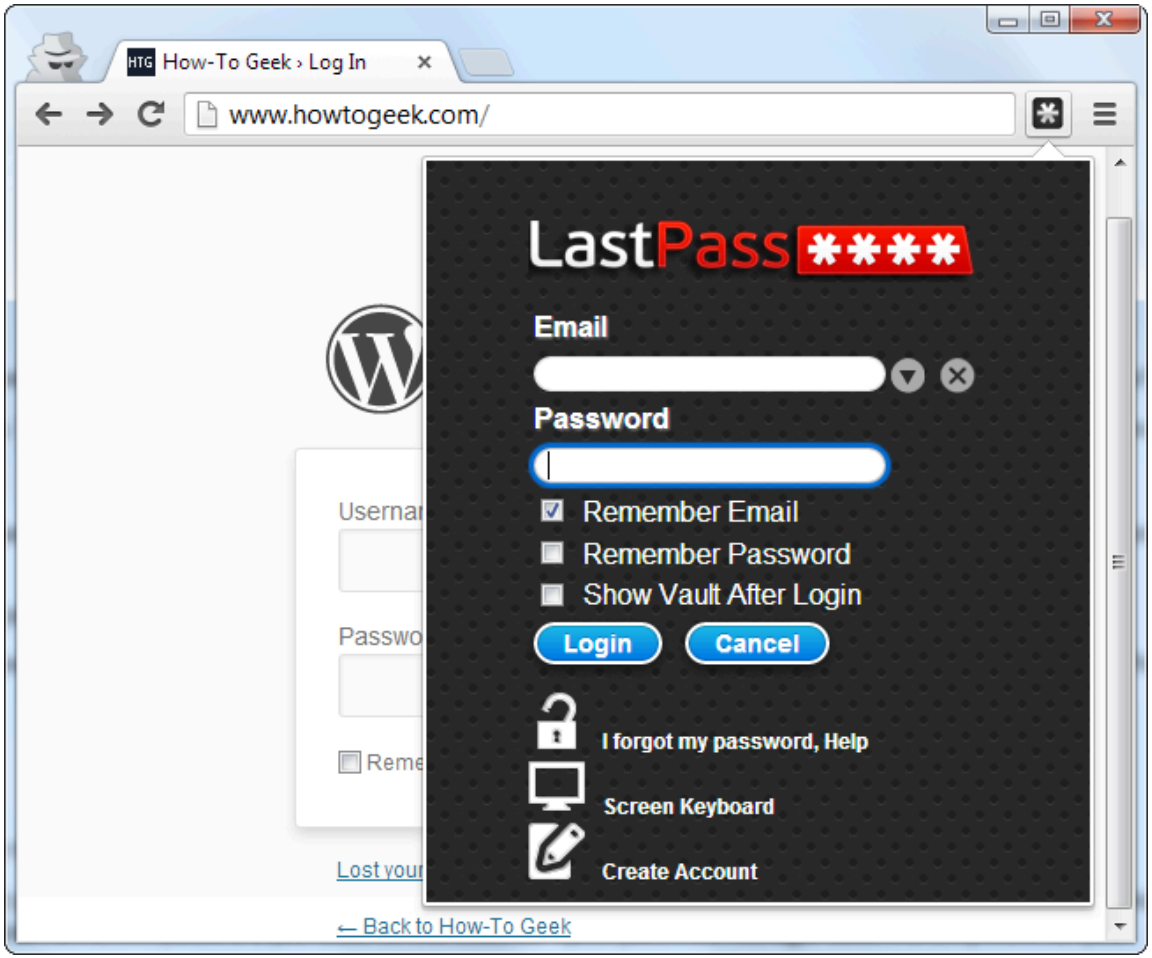
Social Widget Blocket: https://addons.mozilla.org/en-US/firefox/addon/sharemenot/

Password Managers

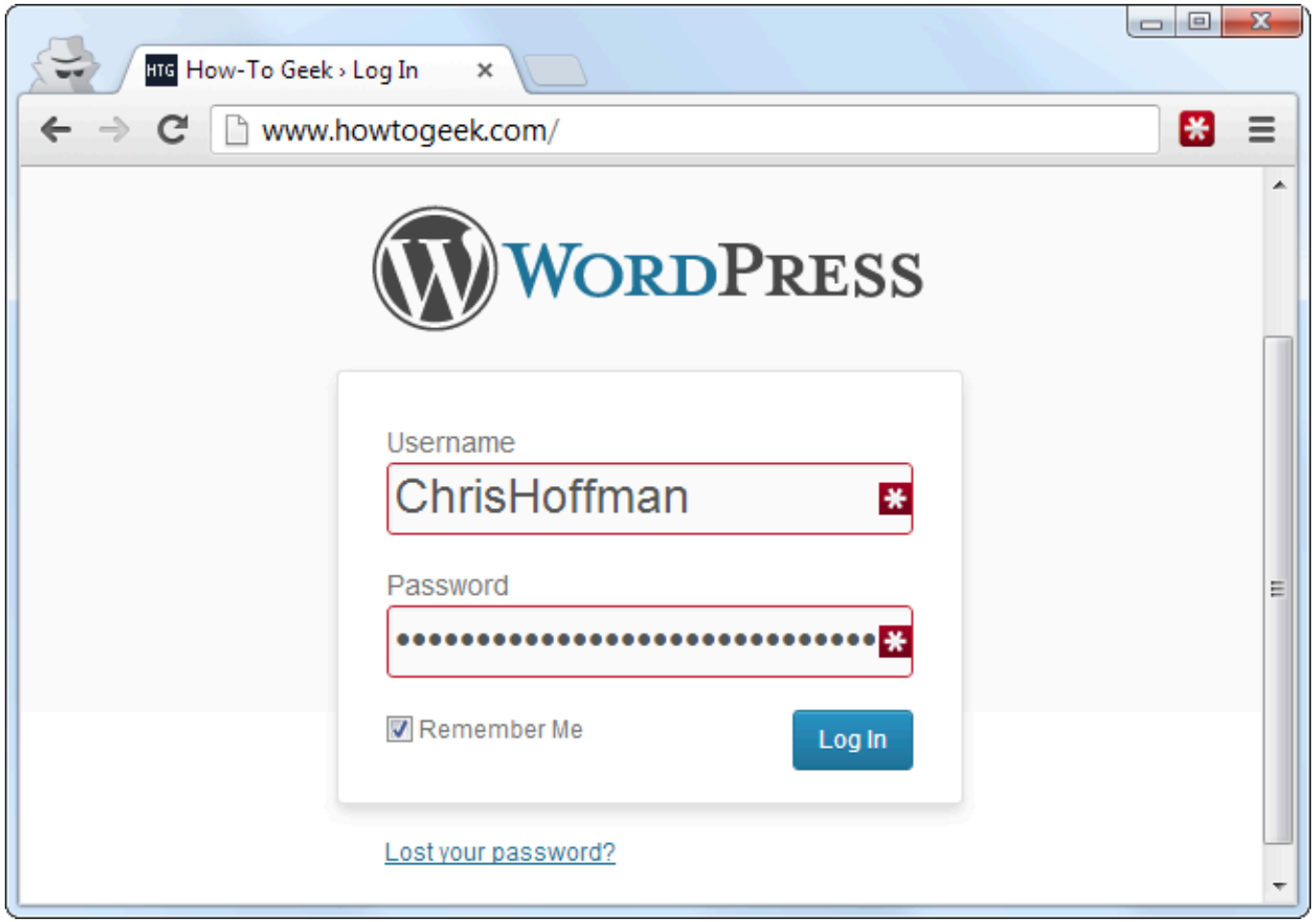
- Helps prevent reuse of passwords
- One ~~ring~~ master password to rule them all!
- Many options available:
  - LastPass: CloudBased password manager
  - KeePass: Desktop application

Images : http://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/

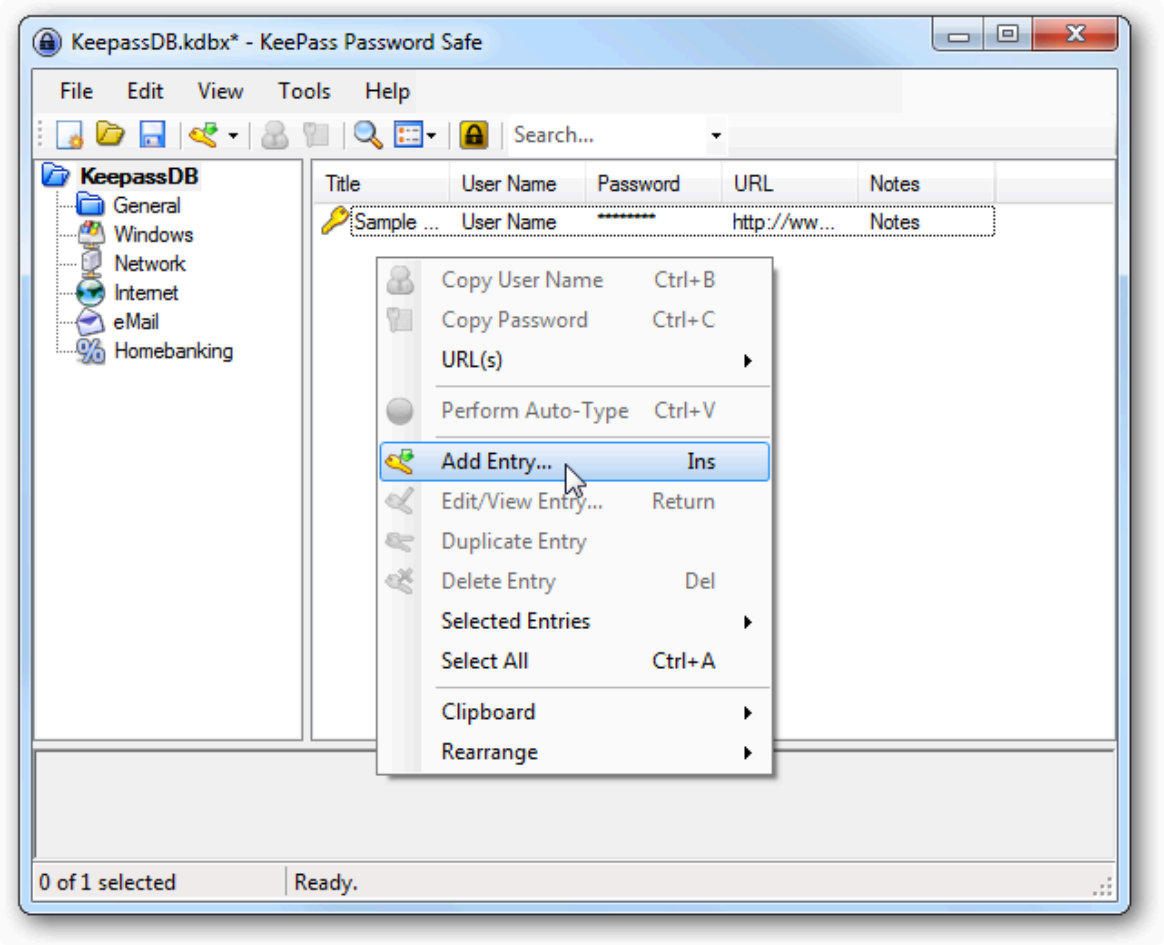
Last Pass


How-To Geek › Log In
www.howtogeek.com/
LastPass ****
Email
Password
Remember Email
Remember Password
Show Vault After Login
Login
Cancel
I forgot my password, Help
Screen Keyboard
Create Account
← Back to How-To Geek

Last Pass


How-To Geek › Log In
www.howtogeek.com/
WordPress
Username
ChrisHoffman
Password
Remember Me
Log In
Lost your password?

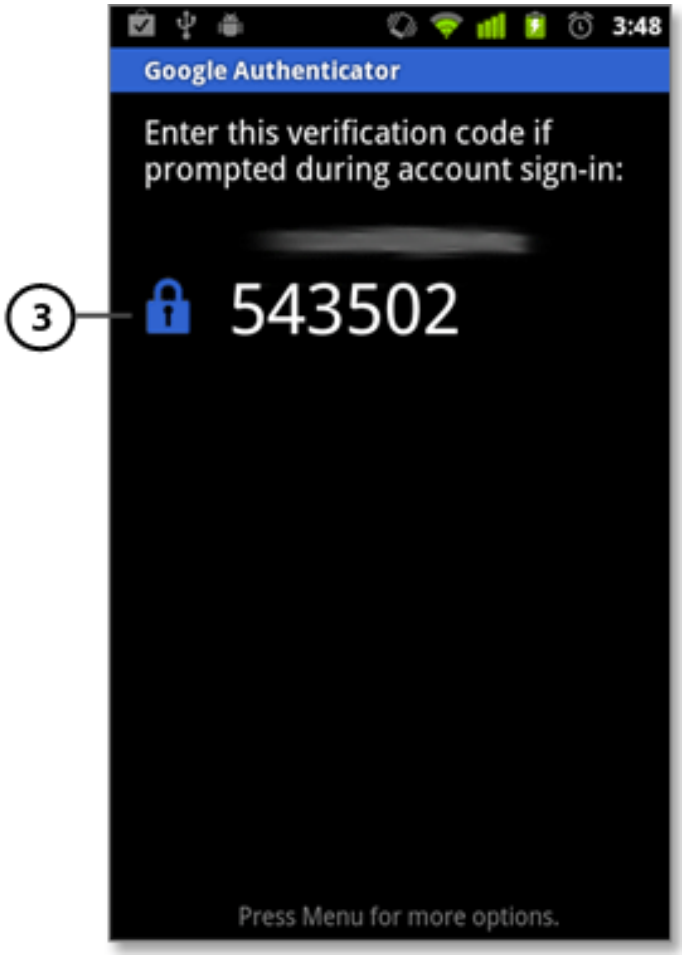
KeePass


KeepassDB.kdbx* - KeePass Password Safe
File
Edit
View
Tools
Help
Search...
KeepassDB
General
Windows
Network
Internet
eMail
Homebanking
Title
User Name
Password
URL
Notes
Sample ...
User Name
****
http://ww...
Notes
Copy User Name Ctrl+B
Copy Password Ctrl+C
URL(s)
Perform Auto-Type Ctrl+V
Add Entry... Ins
Edit/View Entry... Return
Duplicate Entry
Delete Entry Del
Selected Entries
Select All Ctrl+A
Clipboard
Rearrange
0 of 1 selected
Ready.

2 Factor Authentication

- Passwords may not be enough
- 2FA provices identification of users by means of the combination of two different components (such as password and phone)
- List of sites that support 2FA:
  - https://twofactorauth.org/

Using your phone



Hardware tokens

https://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/