

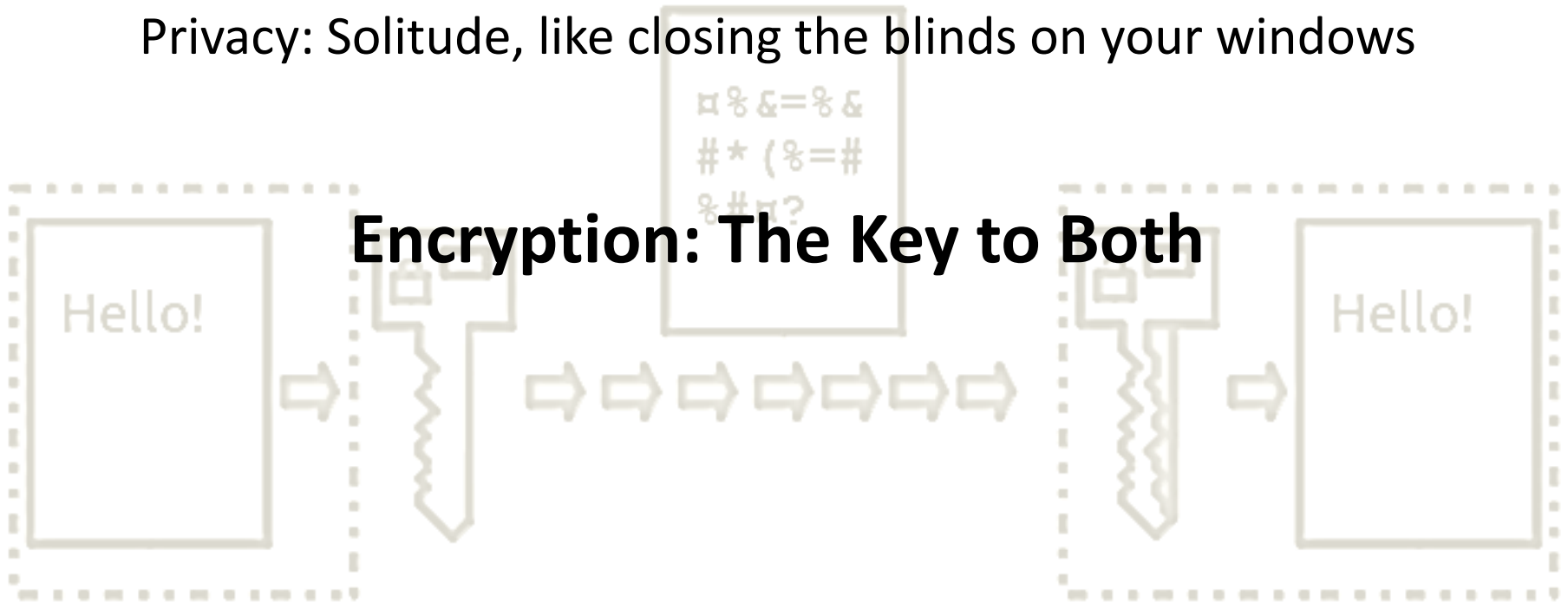
Encrypting Your Digital Life

Learn tips for keeping your private information safer.

Lexicon

Security: Safety, like locking the door of your home

Privacy: Solitude, like closing the blinds on your windows



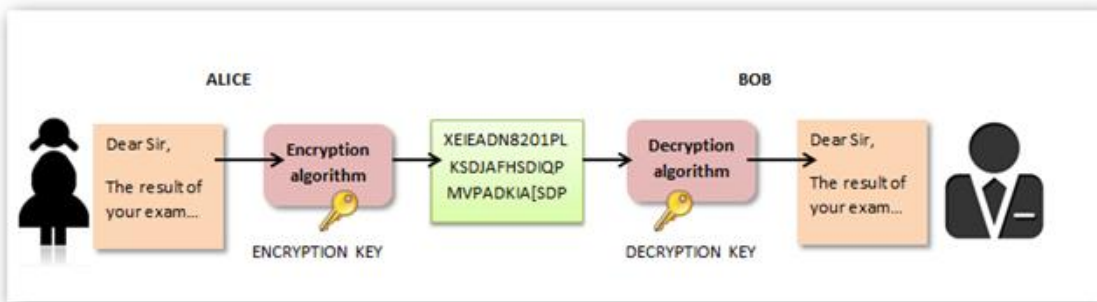
Privacy Matters

“Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say.”

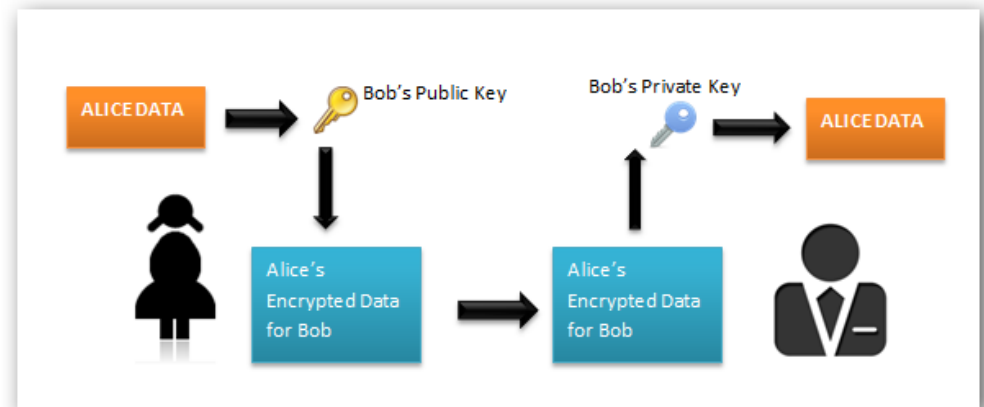
Edward Snowden

Types of Encryption

Symmetric Key



Asymmetric Key



Passwords

**PASSWORDS ARE LIKE
UNDERPANTS**



Change them often, keep them private and never share them with anyone.

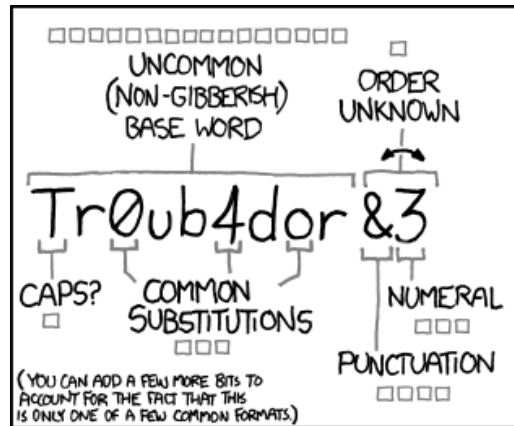
Password Practices

Create secure passwords. Secure passwords are...

- Long
- Random
- Unique

Hackable Password...	Slightly Improved...	Much Better!
jellyfish	jelly22fish	jellY22f1\$hingP0l3
susan	Susan58	.Sus58andMEl@n1e
banklogin	bankLogin90	90b@Nkl0g!n99
lovemydog	loveMYd0g	!0v3myDOGgieBAG

“Unique” Passwords



~28 BITS OF ENTROPY

□□□□□□□□
□□□□□□□□ □
□□□ □□□
□□□□ □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

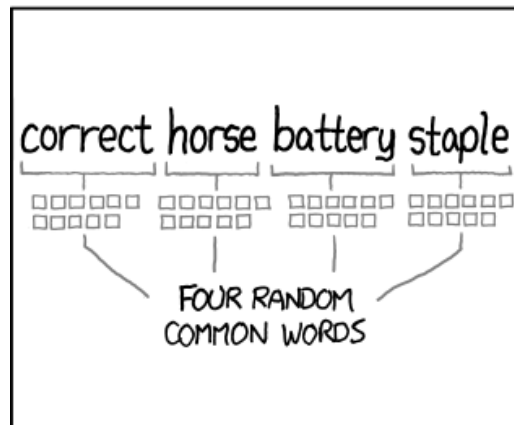
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

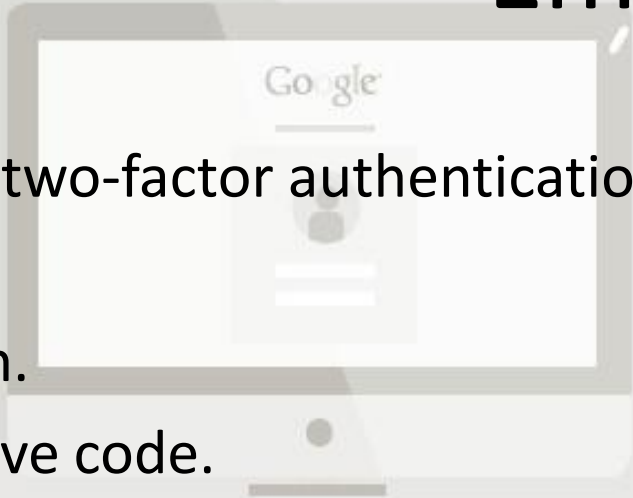
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Email

Turn on two-factor authentication.

- Log in.
- Receive code.
- Enter code.
- Access email.



Computer

Encrypt your hard drive.

Windows: BitLocker

Mac: FileVault



RECOVERY KEY: DO NOT LOSE!

SmartPhone

Turn on password protection.

Text Privately.



Websites

Browse safely.

HTTPS

Browse Privately.



Tor Browser

DuckDuckGo

DuckDuckGo Search Engine

!google I'm a law-abiding citizen who cares about privacy



Recap

- Create secure **passwords**.
- Protect email with **two-factor authentication**.
- Turn on **hard drive encryption** and
...DON'T LOSE THE RECOVERY KEY!!!!
- Use **passcode protection** for your smartphone.
- You may want to text with an **encrypted chat app**.
- Browse more safely using **HTTPS**.
- Browse more privately using either **Tor Browser** or the **Duck Duck Go** search engine.

Questions?

Resources

Handout

Website

Tech Hours

htrrell@milibrary.org