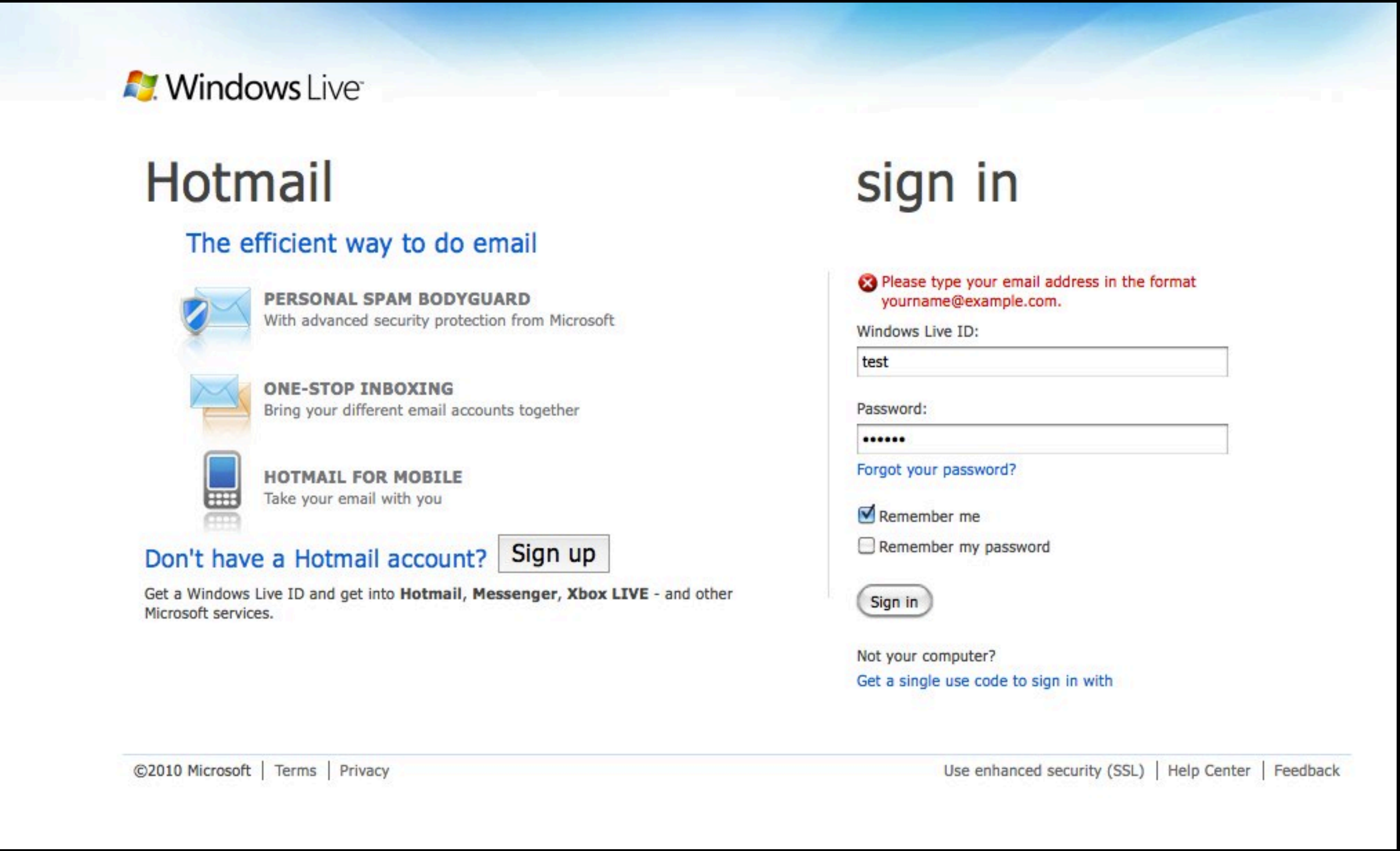
Kamouflage

Elie Bursztein, Hristo Bojinov, Dan Boneh, Xavier Boyen
Stanford University

I am aware that what I am about to say is controversial

54 Millions of smartphone sold during the 1Q 2010

Browsers password managers



Hotmail

The efficient way to do email

PERSONAL SPAM BODYGUARD
With advanced security protection from Microsoft

ONE-STOP INBOXING
Bring your different email accounts together

HOTMAIL FOR MOBILE
Take your email with you

Don't have a Hotmail account?

Get a Windows Live ID and get into **Hotmail, Messenger, Xbox LIVE** - and other Microsoft services.

sign in

Please type your email address in the format yourname@example.com.

Windows Live ID: test

Password: ••••••

Forgot your password?

☑ Remember me

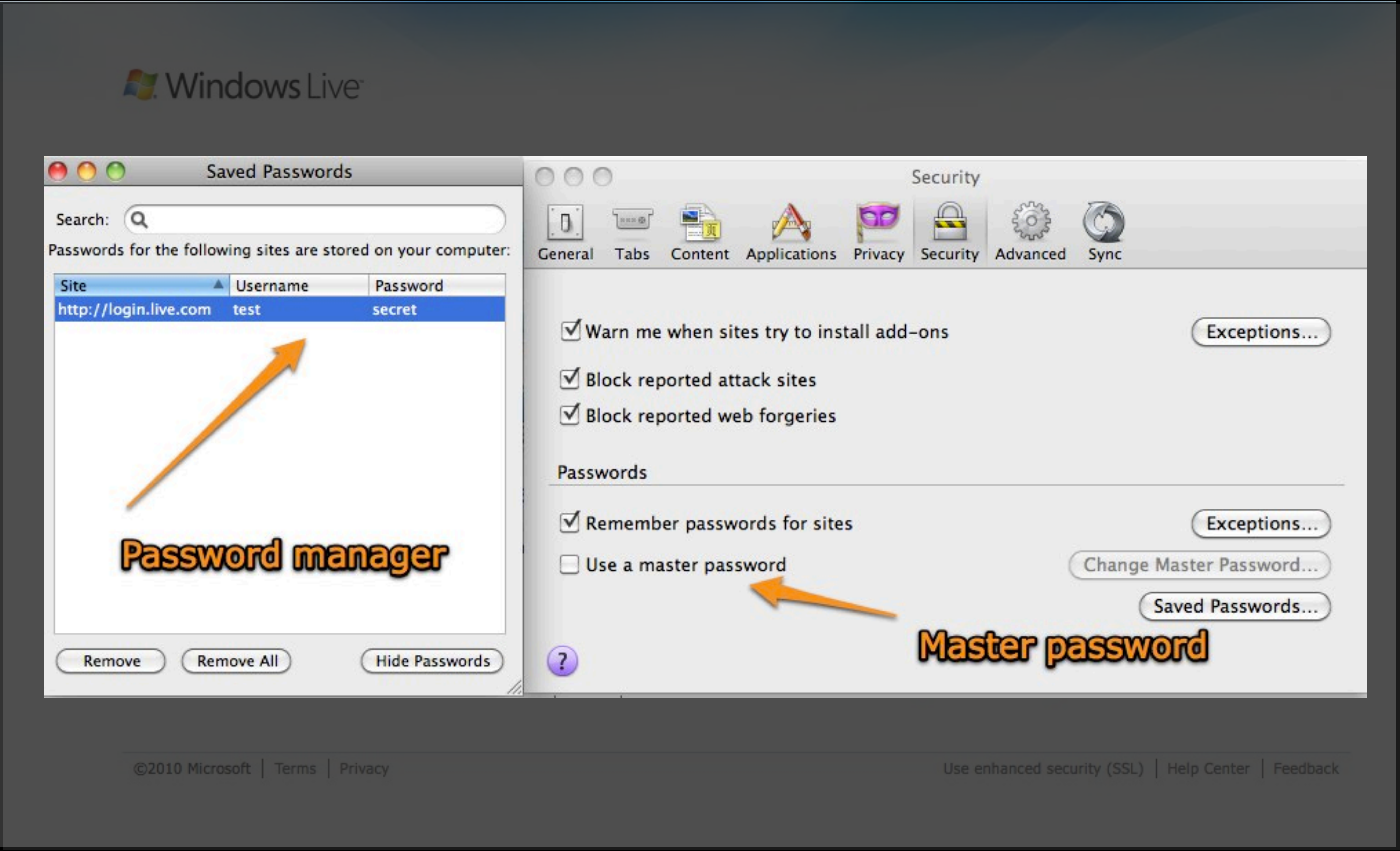
□ Remember my password

Not your computer?
Get a single use code to sign in with

©2010 Microsoft | Terms | Privacy

Use enhanced security (SSL) | Help Center | Feedback

Browsers password managers



Search:

Passwords for the following sites are stored on your computer:

Site	Username	Password
http://login.live.com	test	secret

☑ Warn me when sites try to install add-ons

☑ Block reported attack sites

☑ Block reported web forgeries

Passwords

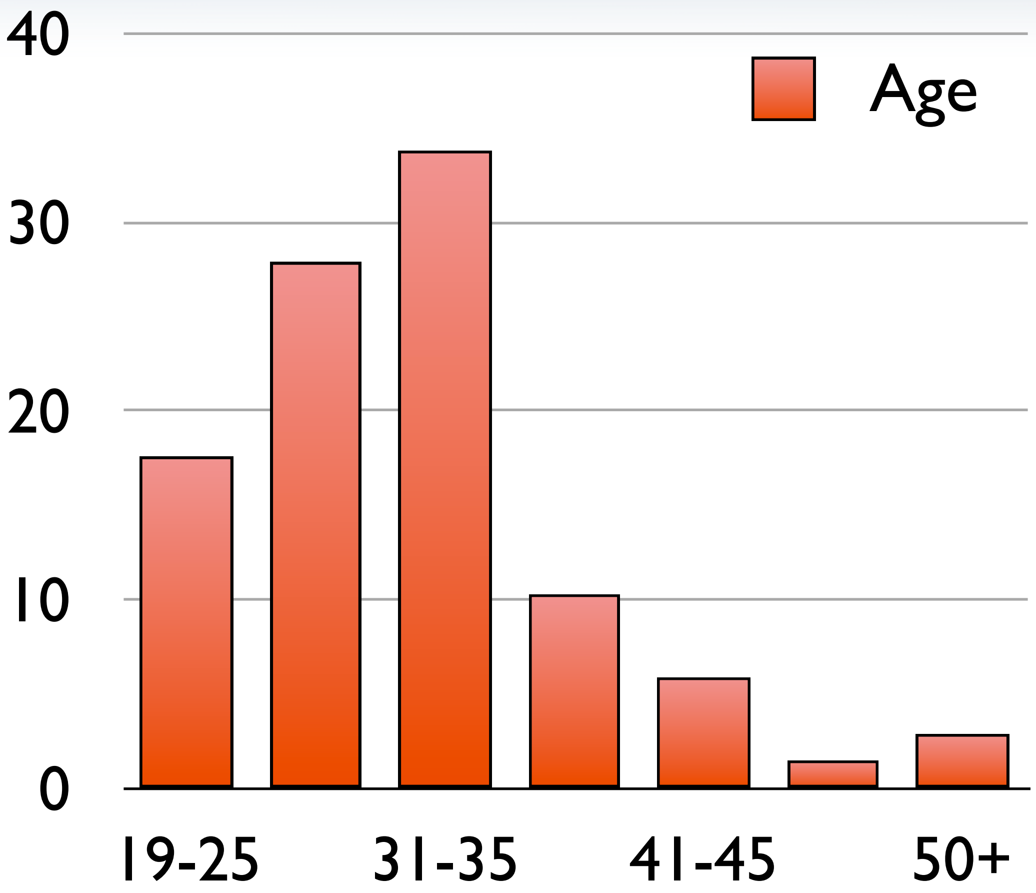
☑ Remember passwords for sites

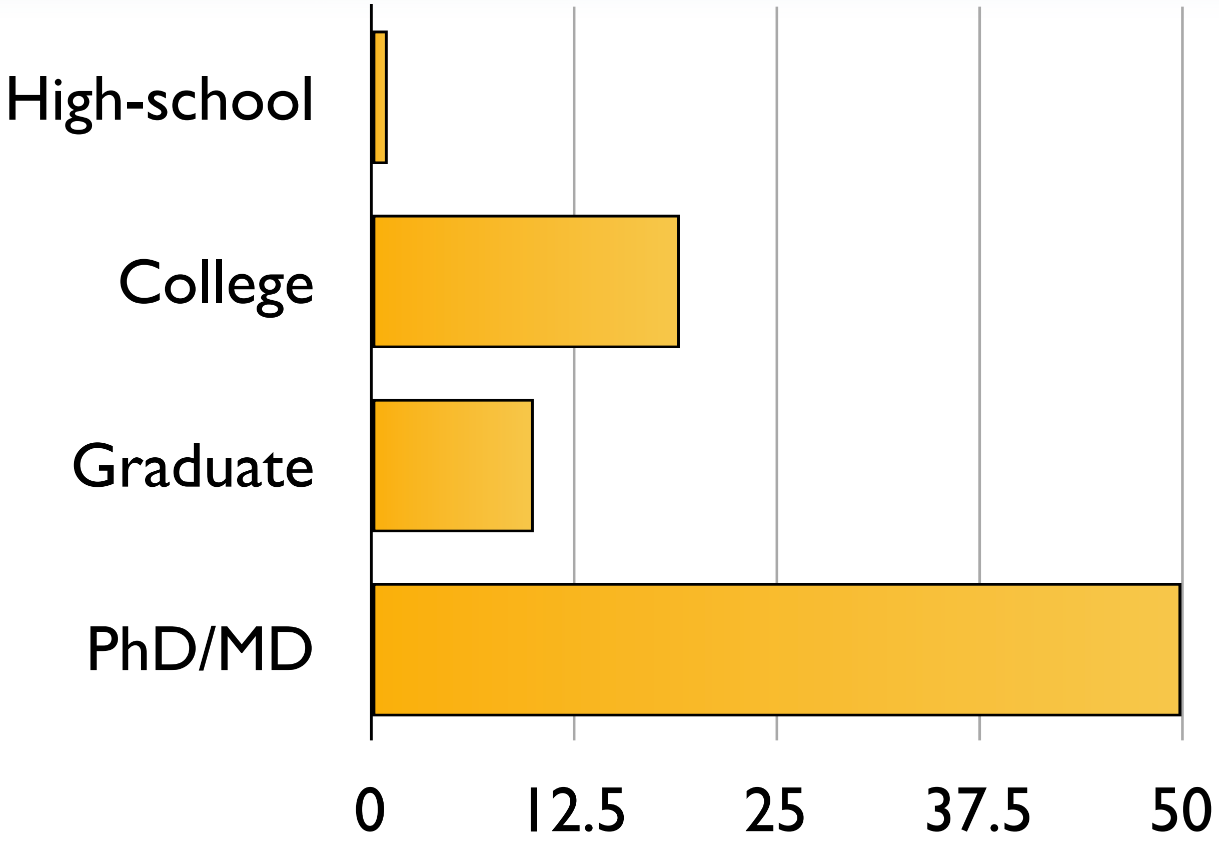
☐ Use a master password

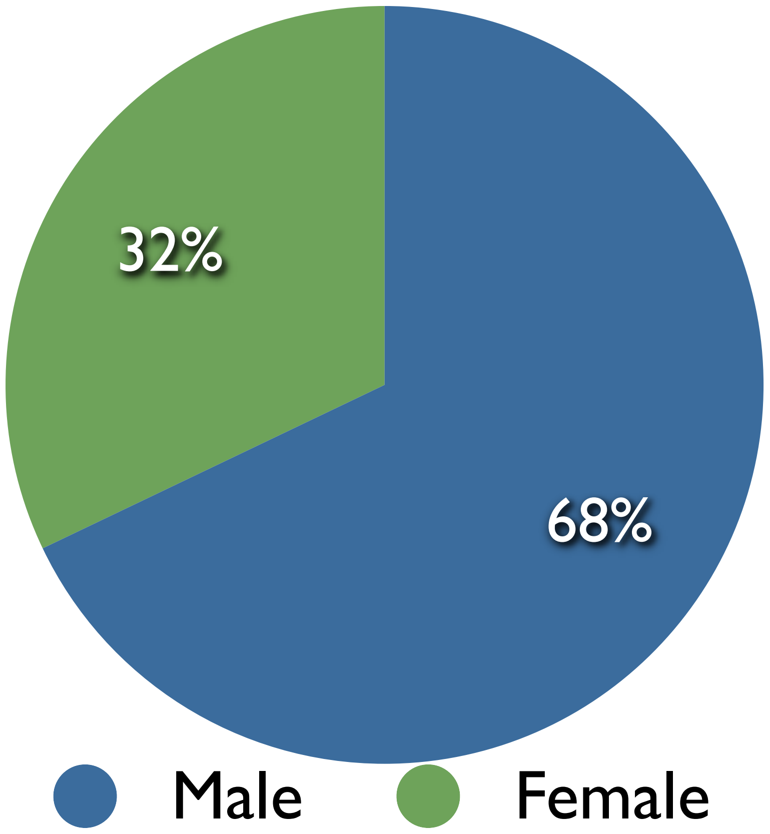
Password manager

Master password

User Study on Password Usages

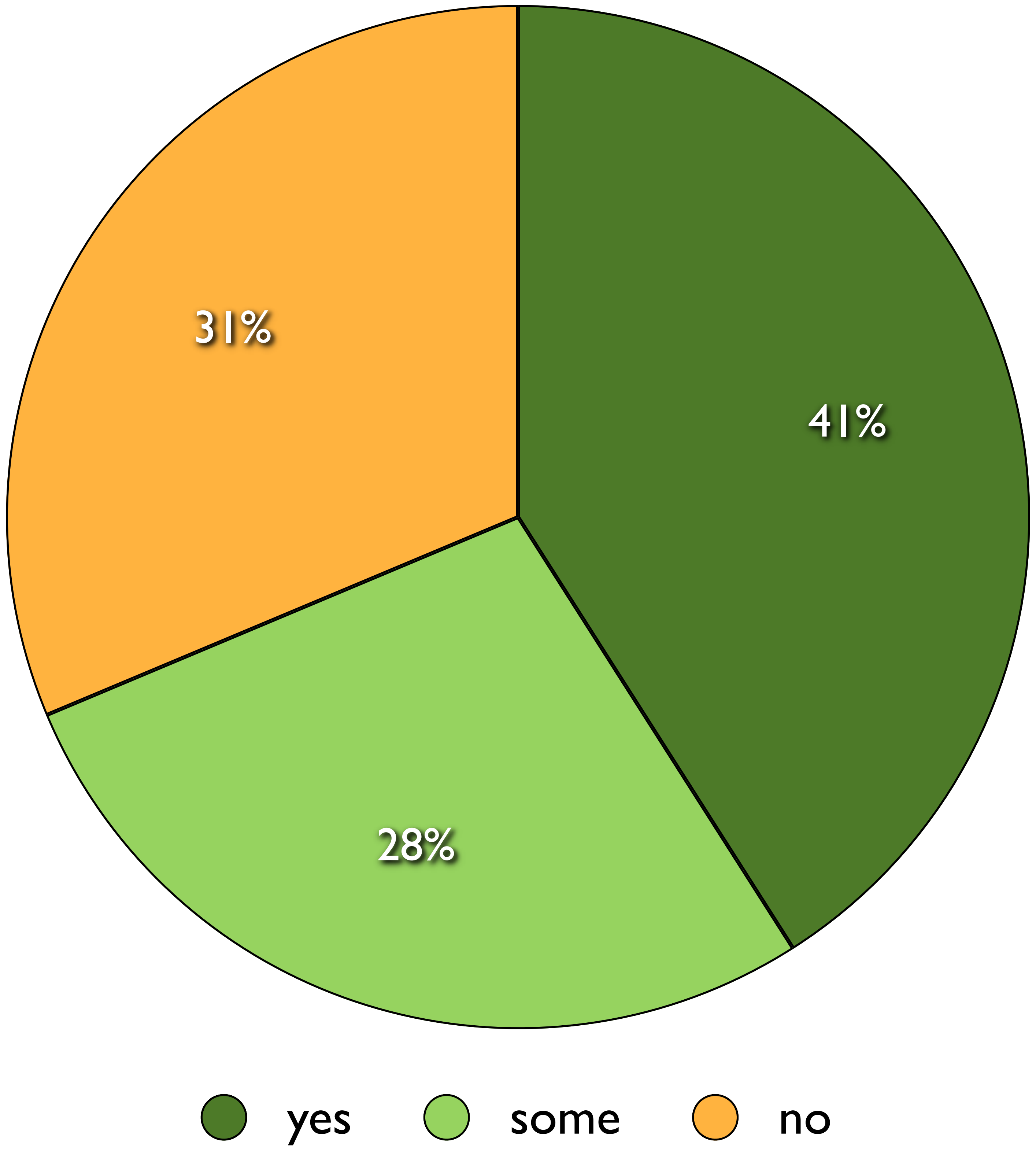






86 people

Do you allows your web browser to remember your password ?



What is our Objective ?

Users want to store their passwords

Threat Model

- Prevents offline attacks
- Forces the attacker to go online

Known approaches

Known approaches

- Make the passwords inaccessible

Known approaches

- Make the passwords inaccessible
- Use a password generator

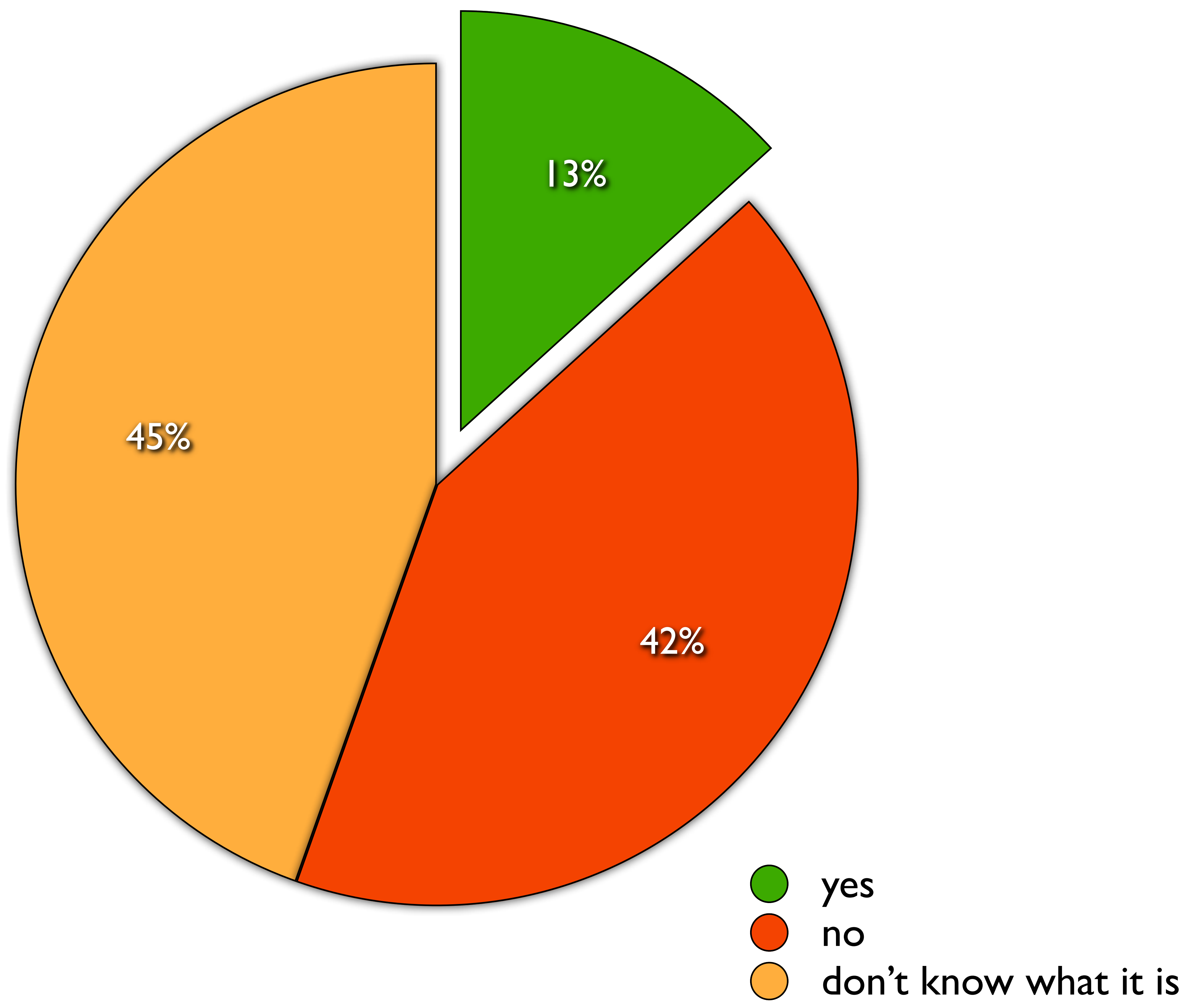
Known approaches

- Make the passwords inaccessible
- Use a password generator
- Have a secure master password

Make passwords inaccessible

- Almost impossible for a large number of passwords
  - Passwords list change and grow overtime
  - Need some form of revocation
- Even system build around this idea have bugs (e.g xbox360)

Do you use a password generator ?

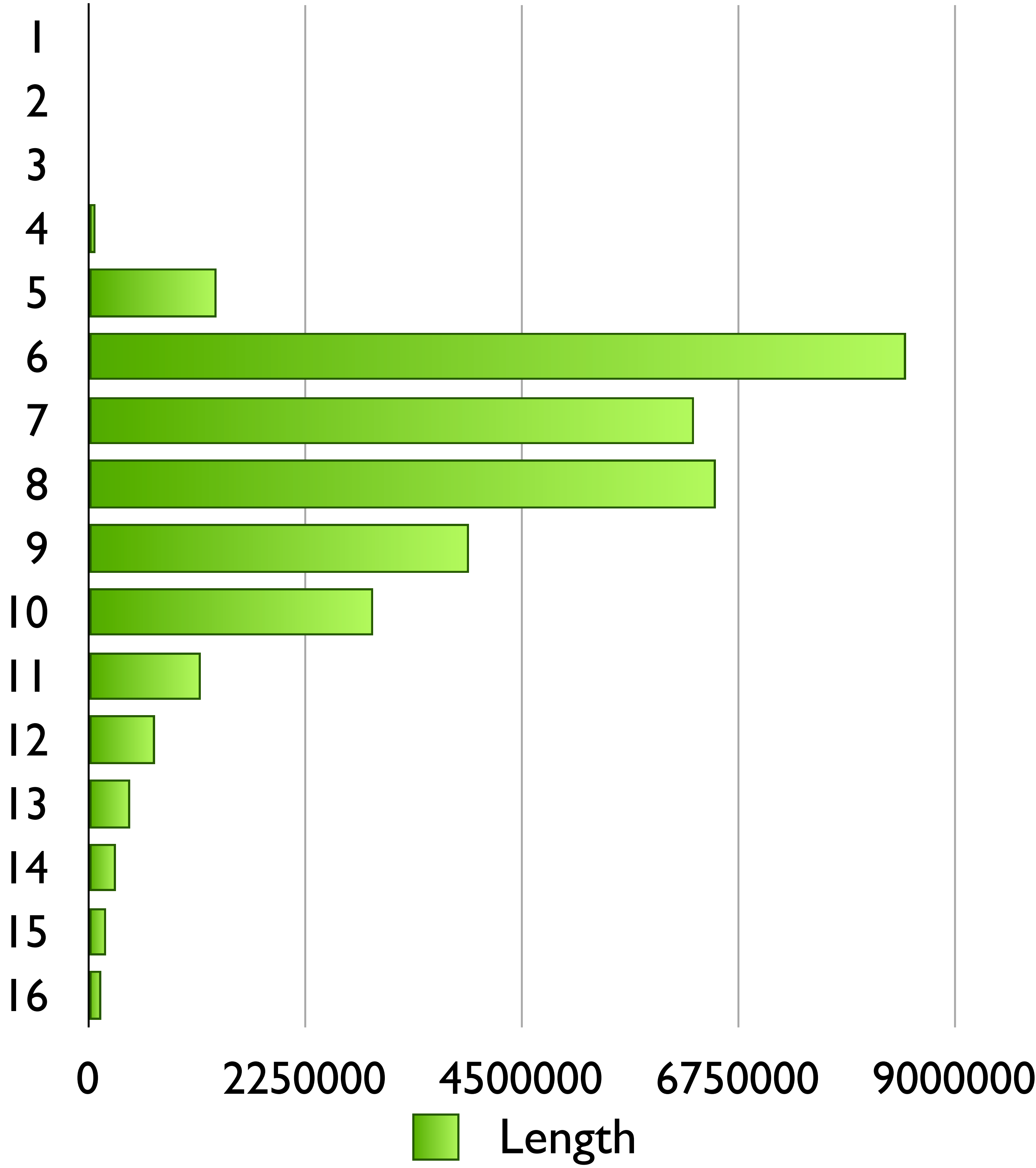


Use strong passwords

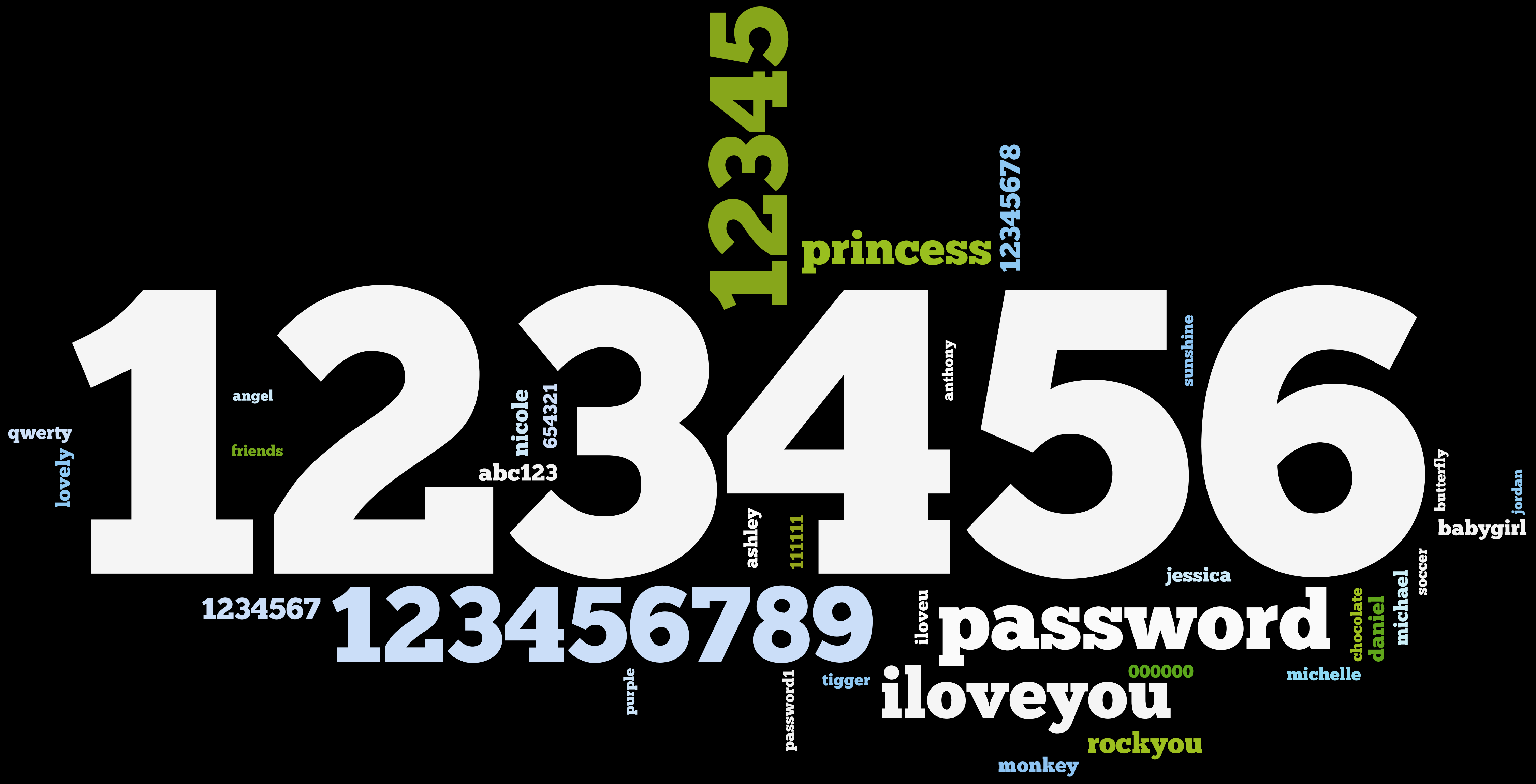
Does anyone still believe users do that ????

The rockyou database

- 32 603 388 passwords
- Disclosed in 2010

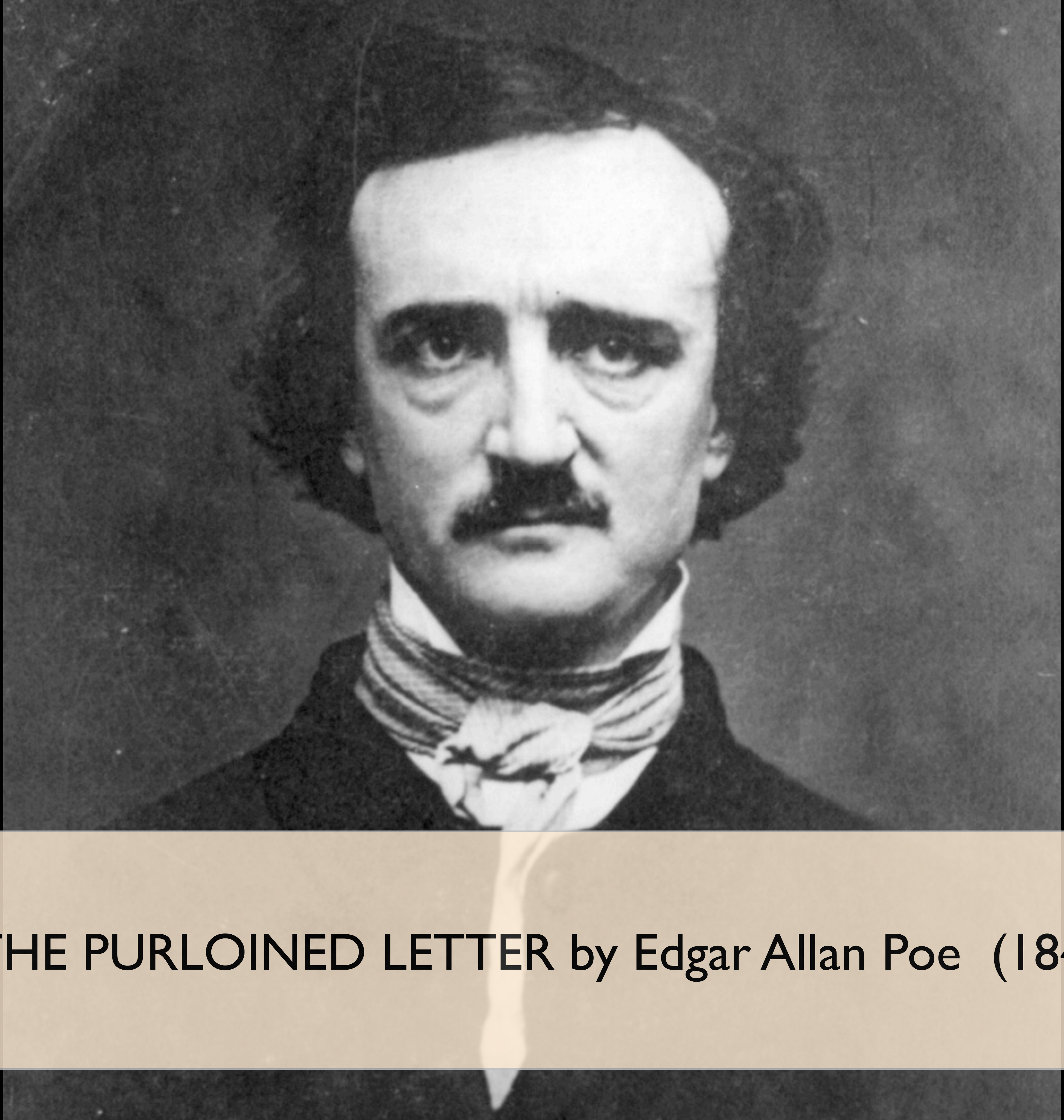


Most used passwords



Embracing the Truth

All known approaches are not working so we can we do ?

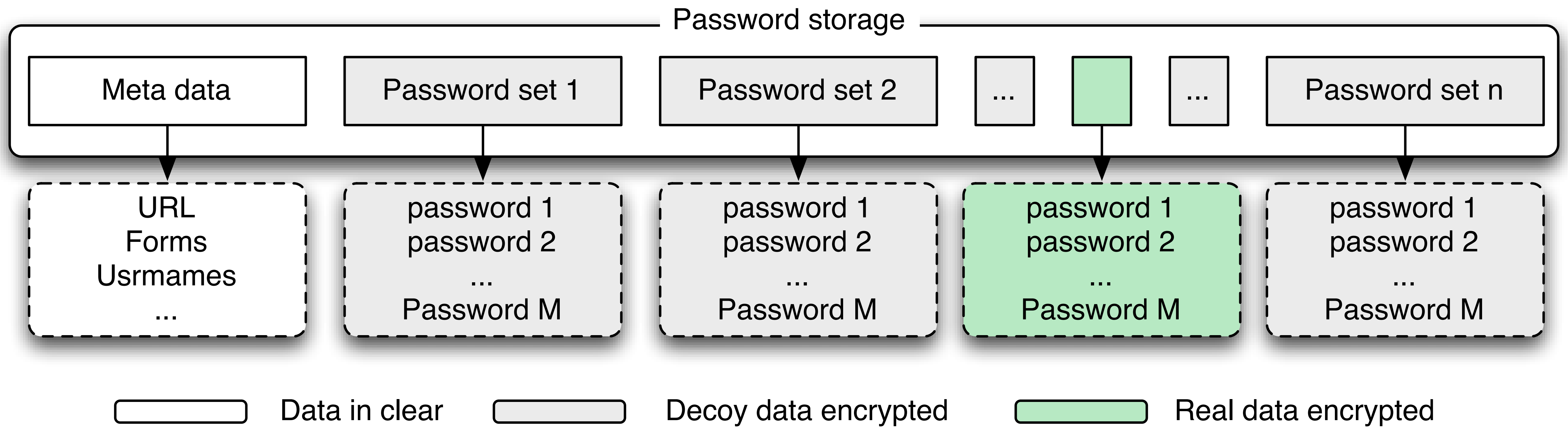


THE PURLOINED LETTER by Edgar Allan Poe (1845)

Here

You can’t perform offline attacks if you don’t know if you are successful

Proposed Architecture



Password storage

Meta data

Password set 1

Password set 2

...

...

Password set n

URL
Forms
Usrmames
...

password 1
password 2
...
Password M

password 1
password 2
...
Password M

password 1
password 2
...
Password M

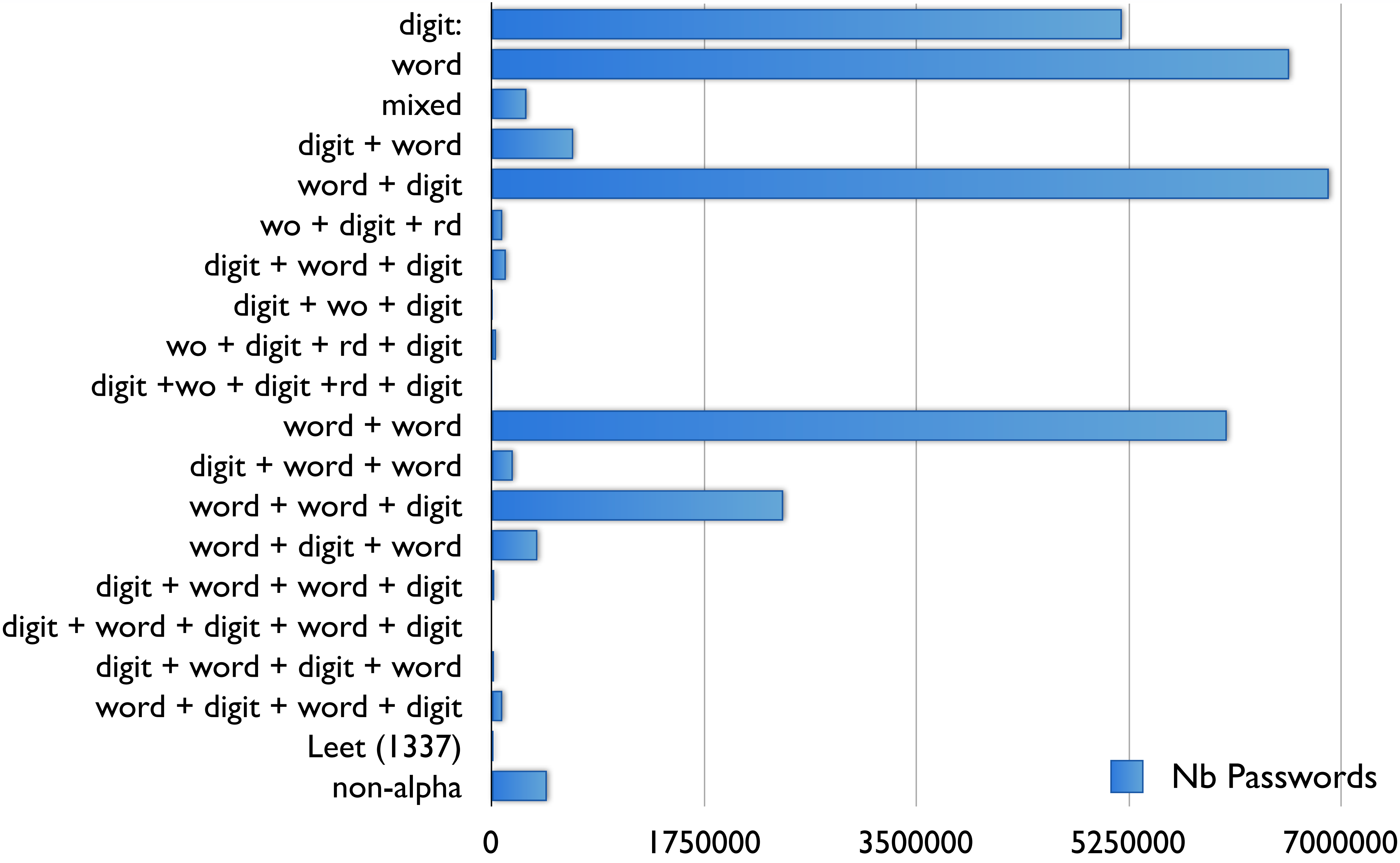
password 1
password 2
...
Password M

▭ Data in clear

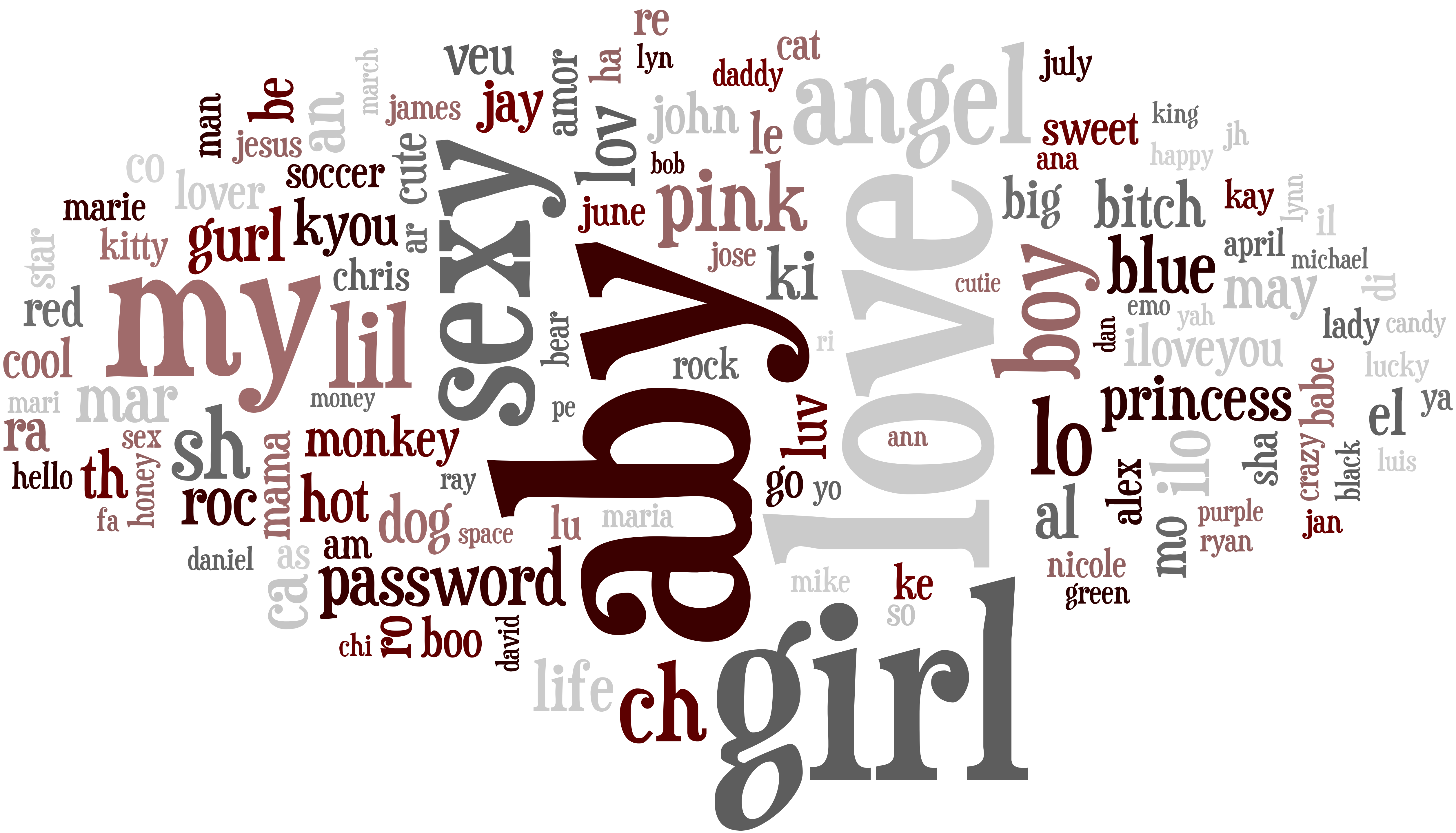
▨ Decoy data encrypted

🟩 Real data encrypted

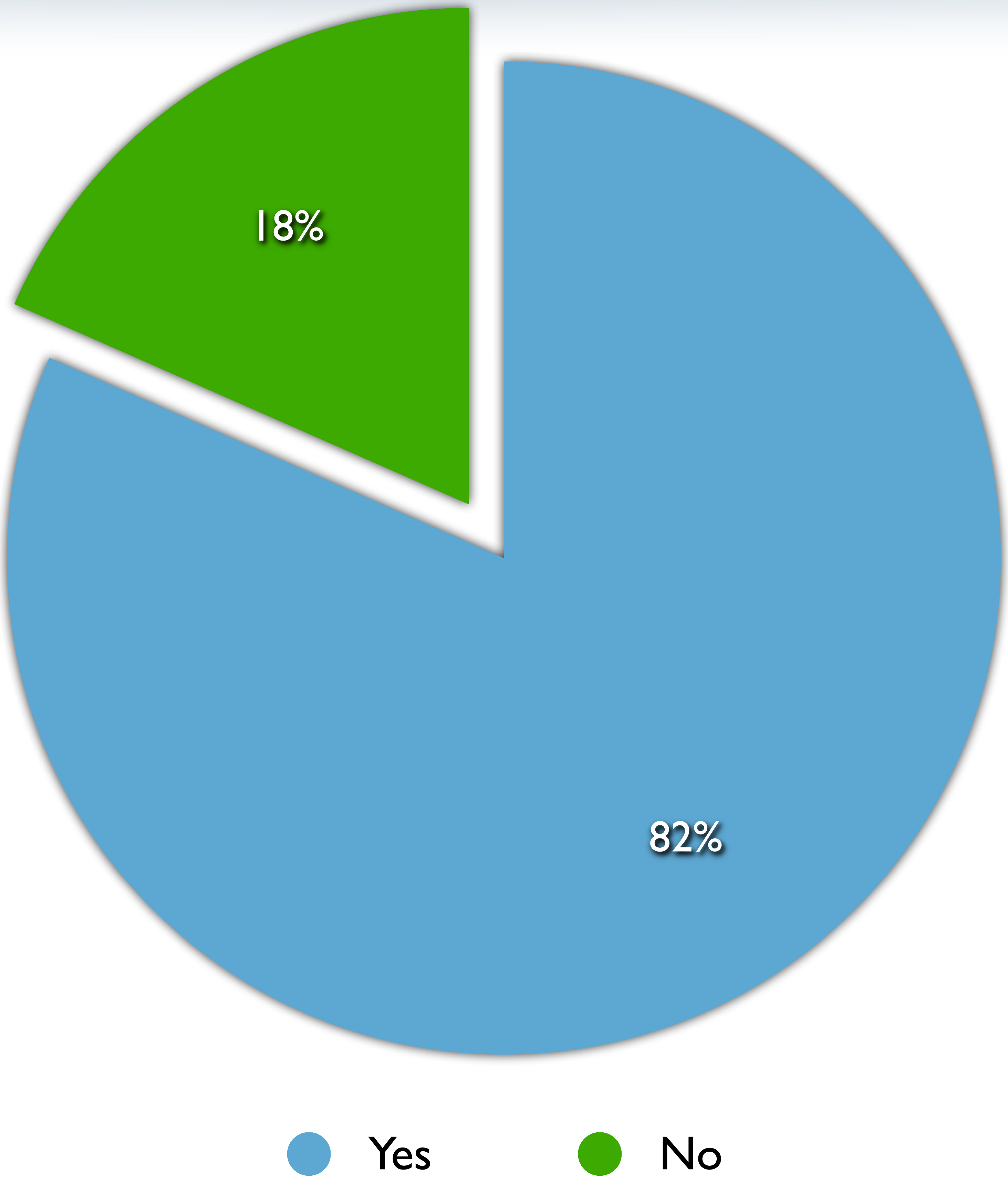
Dealing with Password Structure



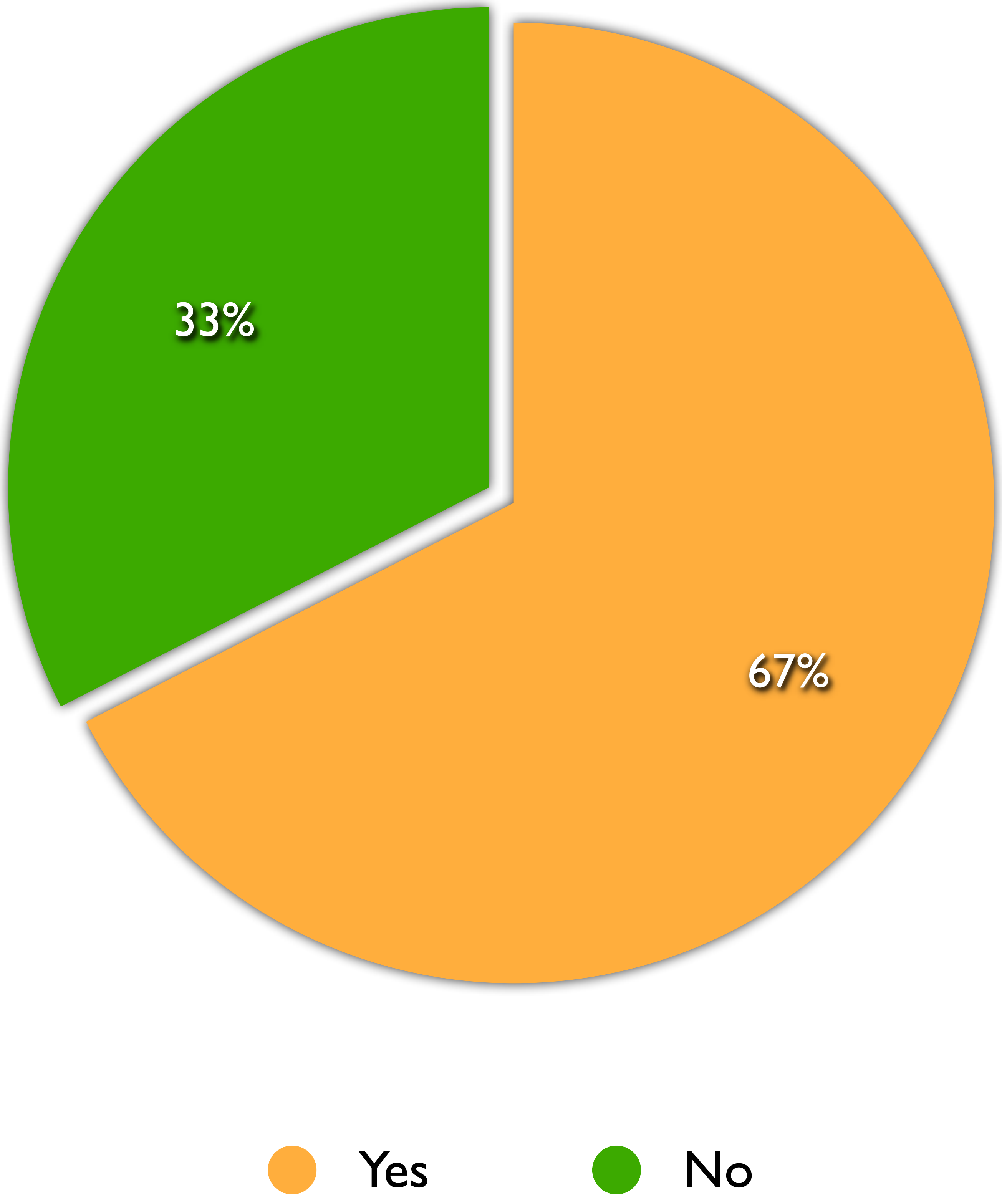
RockYou Top word



Do you reuse password between different web site ?



Do you use related password ?



Web Site Policy

Web Site	**Password Requirement**
Google	at least 8 characters
Yahoo!	at least 6 characters
YouTube	at least 8 characters
Facebook	at least 6 characters
Windows Live	at least 6 characters
MSN	at least 6 characters
MySpace	between 6 and 10 characters, at least 1 digit or punctuation
Fidelity	between 6 and 12 characters, *digits only*
Bank of America	between 8 and 20 characters, $\geq$ 1 digit and $\geq$ 1 letter, no `$ < > & ^ ! [ ]`
Wells Fargo	between 8 and 10 characters, $\geq$ 3 of: uppercase, digit, or special characters

How users will know that they have entered the correct password ?

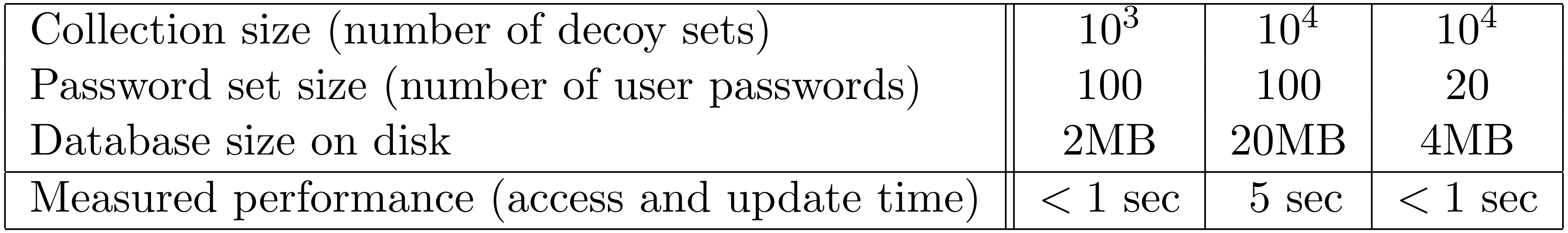
Provide a visual indicator: each set is associated with a visual icon.

Correct

False

False

Evaluation



Collection size (number of decoy sets)	10^3	10^4	10^4
Password set size (number of user passwords)	100	100	20
Database size on disk	2MB	20MB	4MB
Measured performance (access and update time)	$<$ 1 sec	5 sec	$<$ 1 sec

Conclusion

- Hiding in plain sight is promising
- It is also harder than one might expect