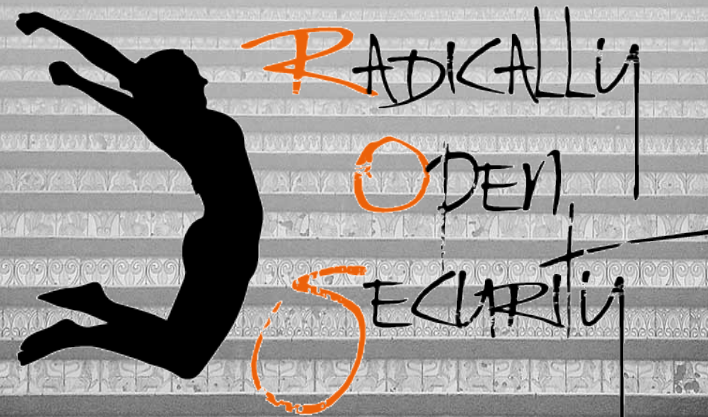


Password Management and Cracking Training

Developed by: Melanie Rieback, Rais Mense,
Nathan Stern, Murtuja Bharmal,
Fernando Quintero



Agenda

- Part I – Password Creation
 - Intro: what are Passwords? Hashes?
 - Weak passwords (guessability, recon, default Pws)
 - Attacks against passwords (brute force, dictionary attacks)
 - DEMO: PW cracking (Online vs. Offline, Rainbow Tables)
 - Solutions (salt, passphrases, PW policies)
- Part II – Password Usage
 - Passwords on the Wire
 - DEMO: ssl-strip
 - Worst Password Management techniques
- Part III – Password Storage
 - Intro to PW Storage (text files, DBs, memory, Linux)
 - Password caching, pros vs. cons
 - DEMO: DumpIt + Volatility
 - Solutions (PW Vaults, encryption in DBs/filesystems)



RAVENLION OPEN SECURITY

Part I - Password Creation



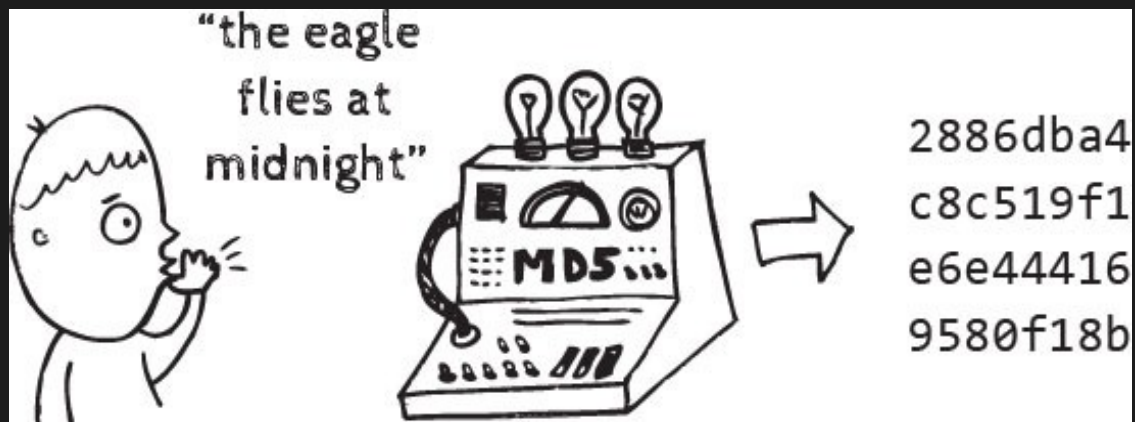
What is a Password?

- A secret word/string of characters used to authenticate a user into a system
- Authentication trilogy
 - What you have
 - Who you are
 - **What you know**



Hash Functions

- Cryptographic one-way functions, that convert a string into fixed number of character.
- Example algorithms: NT Hash, LM Hash, MD4, MD5, SHA1, SHA2, SHA256, SHA512



Hashing Vs Encryption

	Hashing	Encryption
Definition	Hashing involves the conversion of plaintext into a hash or digest. A digest cannot be reversed into the original message.	Encryption is the process of converting plain text into cipher by using an algorithm. The encrypted message can only be read by knowing the encryption key.
Protection of	Integrity	Confidentiality
Unlocking	No key can be used for unlocking	Requires key for unlocking

Courtesy: <http://www.differencebetween.info/difference-between-hashing-and-encryption>



RADICALLY OPEN SECURITY

Worst Passwords of 2015

- Top 15: 123456, password, 12345678, qwerty, 12345, 123456789, football, 1234, 1234567, baseball, welcome, 1234567890, abc123, 111111
- All 11,000,000 passwords of Ashley Madison were hacked



RADICALLY OPEN SECURITY

What makes passwords weak?

- Guessability
 - Predictability and low entropy
- Relevance
 - Studying corporate literature, website sales materials and competitors, build custom word list

USER	PASSWORD	HINT	
4e18acc1ab27a2d6		WEATHER VANE SWORD	<input type="text"/>
4e18acc1ab27a2d6			<input type="text"/>
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1	<input type="text"/>
8bab66299e06eb6d		DUH	<input type="text"/>
8bab66299e06eb6d	a0a2876eb1ea1fca		<input type="text"/>
8bab66299e06eb6d	85e9da81a8a78adc	57	
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES	
1ab29ae86da6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS	
a1f9b2b6299e7a2b	endec1e6ab797397	SEXY EARLOBES	<input type="text"/>
a1f9b2b6299e7a2b	617ab027727ad85	BEST TOS EPISODE	<input type="text"/>
39738b7adb068af7	617ab027727ad85	SUGARLAND	

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD

Extract from XKCD cartoon satirising Adobe's blunder



RADICALLY OPEN SECURITY

Default Passwords

RouterPasswords.com

Select Router Make: LINKSYS

Find Password

Manufacturer	Model	Protocol	Username	Password
LINKSYS	WAP11	MULTI	n/a	(none)
LINKSYS	DSL	TELNET	n/a	admin
LINKSYS	ETHERFAST CABLE/DSL ROUTER	MULTI	Administrator	admin
LINKSYS	LINKSYS ROUTER DSL/CABLE	HTTP	(none)	admin
LINKSYS	BEFW11S4 Rev. 1	HTTP	admin	(none)
LINKSYS	BEFSR41 Rev. 2	HTTP	(none)	admin
LINKSYS	WRT54G	HTTP	admin	admin
LINKSYS	WAG54G	HTTP	admin	admin
LINKSYS	LINKSYS DSL		n/a	admin
LINKSYS	WAP54G Rev. 2.0	HTTP	(none)	admin
LINKSYS	WRT54G Rev. ALL REVISIONS	HTTP	(none)	admin
LINKSYS	MODEL WRT54GC COMPACT WIRELESS-G BROADBAND ROUTER	MULTI	(none)	admin

Courtesy: <http://www.howtogeek.com/131338/how-to-access-your-router-if-you-forget-the-password/>



RADICALLY OPEN SECURITY

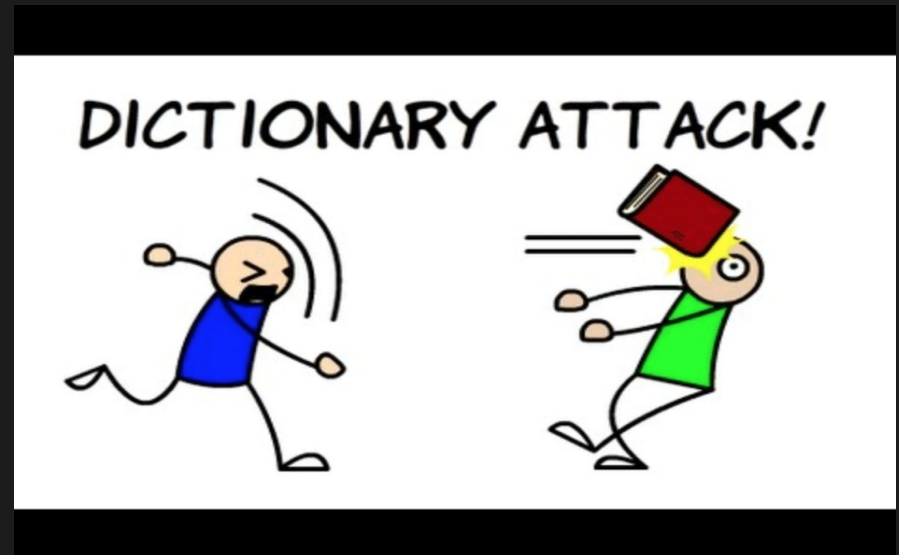
Attacks Against Passwords

- Dictionary Attack

- Systematically entering every word in a dictionary(wordlist) as a password

- Brute force attack

- Decoding encrypted/hashed data through exhaustive effort (using brute force) rather than employing intellectual strategies.



Courtesy: <http://searchsecurity.techtarget.com/>



RADICALLY OPEN SECURITY

Types of Password Cracking

- Online
 - Trying different passwords interactively
 - Usually slow and noisy
 - You might be allowed only a few guesses
- Offline
 - Processing password files/ hashes locally
 - Limited by computing speed



RADICALLY OPEN SECURITY

Rainbow Tables

- Rainbow Tables
 - A rainbow table is a list of pre-computed hashes
 - The hash to test gets compare against the other pre-computed hashes
 - Space/time tradeoff



DEMO TIME!!!

- Estimator
- Generator
- Offline cracking
- Rainbow tables



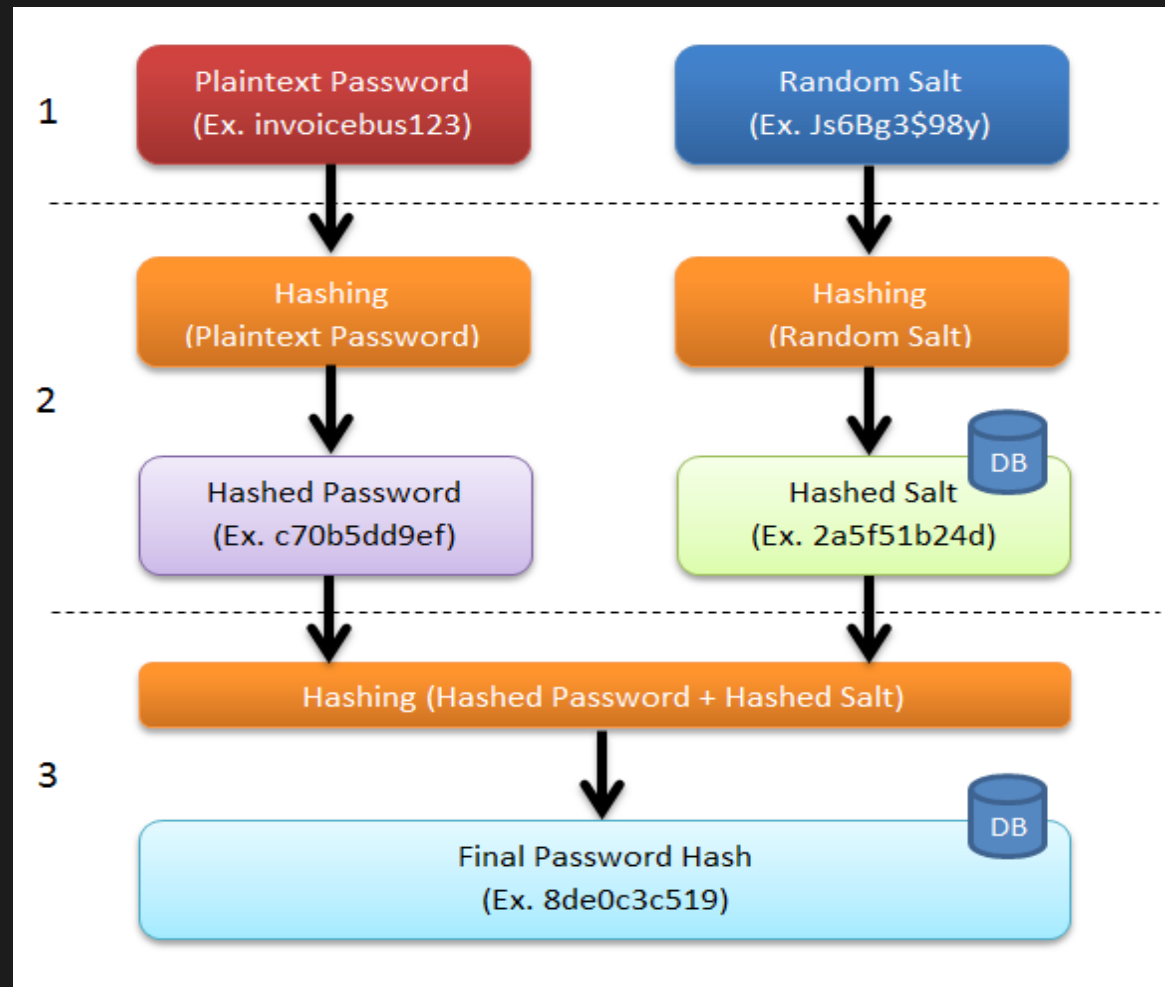
RADICALLY OPEN SECURITY

Solutions: Salt

- Random data used as additional input to a one-way hash function.
- Salt can defend against dictionary attacks or pre-computed rainbow table attacks



Example: Password Salt



Courtesy: <http://sladigitalforensics.blogspot.in/2013/12/salted-hash-future-for-passwords.html>

Passphrases vs Passwords

- Passwords usually 10-12 letters / numbers / symbols
- Passphrase is long sentence which contains spaces. Can also contain symbols.
- Passphrases have more entropy

Test the strength of your password: Type a password into the box.

PASSWORD:

STRENGTH:

Best



xkcd on Passphrases <3

The comic is divided into four panels illustrating password creation and memorability.

Top Left Panel: Shows a password `Tr0ub4dor&3` with annotations: "UNCOMMON (NON-GIBBERISH) BASE WORD" for "Troubador", "ORDER UNKNOWN" for the rearrangement, "CAPS?" for "T", "COMMON SUBSTITUTIONS" for "0" and "4", "NUMERAL" for "3", and "PUNCTUATION" for "&". A note at the bottom says: "(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)"

Top Middle Panel: Titled "~28 BITS OF ENTROPY". It shows a small tree diagram of possible characters. The calculation is $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$. A note says: "(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.)". The "DIFFICULTY TO GUESS:" is **EASY**.

Top Right Panel: A stick figure asks: "WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO? AND THERE WAS SOME SYMBOL...". The "DIFFICULTY TO REMEMBER:" is **HARD**.

Bottom Left Panel: Shows the password "correct horse battery staple" with annotations: "correct", "horse", "battery", and "staple". Below each word is a small tree diagram of possible words. The text "FOUR RANDOM COMMON WORDS" is at the bottom.

Bottom Middle Panel: Titled "~44 BITS OF ENTROPY". It shows a larger tree diagram of possible words. The calculation is $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$. The "DIFFICULTY TO GUESS:" is **HARD**.

Bottom Right Panel: A stick figure says "THAT'S A BATTERY STAPLE." and "CORRECT!". A battery icon is shown. The "DIFFICULTY TO REMEMBER:" is "YOU'VE ALREADY MEMORIZED IT".

Bottom Panel: A summary text: "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."



Password Policy

Enforce password requirements

Change
<90 days

12+
characters

All
character
types

Prohibit
re-use

Pattern
checks?

Support

Crack your own
passwords

Awareness of phishing
and re-use

Courtesy: https://www.rsaconference.com/writable/presentations/file_upload/pdac-w05_the_state_of_modern_password_cracking_final.ppt.pdf



RADICALLY OPEN SECURITY

Part II - Password Usage



Password Pitfalls

- Writing them down on sticky notes
- Maintain a text file with user credentials
- Using same credentials at multiple places*
- *Specially the insecure ones ... (leaks)



RADICALLY OPEN SECURITY

Data on the Wire

- Password sniffing
 - Sniffing with tcpdump, tshark, Wireshark
i.e. HSRP passwords in Cisco routers, VoIP passwords
 - MITM using sslsniff/sslstrip/bettercap



RADICALLY OPEN SECURITY

DEMO TIME!!!

- Password Sniffing with the WiFi Pineapple!
 - Ssl-split



Stuff That Can Help

- Different passwords everywhere
 - Twitter, Facebook, Google
 - Government logins
 - Banks
- Protect your access with additional controls.
i.e. 2FA



RADICALLY OPEN SECURITY

Part III - Password Storage



Where Do Passwords Live?

- In plain-text files
 - .htpasswd,
/etc/ppp/chap-secrets,
browser/application
cache file
- In databases
 - Mysql, MS-SQL, sqlite
- In memory
 - Temporary storage



Where Do Passwords Live?

- Windows
 - SAM database, Active Directory
- Linux
 - /etc/shadow, OpenLDAP
- Application Servers
 - Files and DBs



Saving Passwords on the HD

- Password Hardcoding
 - Software (and filesystems) sometimes contain cleartext passwords, which are used for inbound authentication or outbound communication
 - This is useful for users / sysadmins.. and for attackers!



Saving Passwords in Caches

- Browser/application caches are handy!
 - Login credentials stored locally for later use.
 - Web browsers, applications, etc..
 - Password recovery tools/malware can recover and decrypt stored passwords



Chrome Password Decryptor



The screenshot shows a web browser window with the address bar displaying 'C:\Users\Administrato' and the page title 'Chrome Password Recover...'. The main content area features a green header with the 'Chrome Password Decryptor' logo and the text 'Google Chrome Login Password Recovery Software'. Below the header is a section titled 'Chrome Password Recovery Report' containing a table with three columns: Index, Website URL, Username, and Password. The table lists three entries for Vimeo, LinkedIn, and Pinterest. At the bottom, a footer states: 'Report generated by 'ChromePasswordDecryptor' Application (version 5.0) from www.SecurityXploded.com.'

Index	Website URL	Username	Password
1	https://vimeo.com/log_in	[REDACTED]	[REDACTED]
2	https://www.linkedin.com/uas/login-submit	[REDACTED]	[REDACTED]
3	https://www.pinterest.com/login/	[REDACTED]	[REDACTED]

Report generated by 'ChromePasswordDecryptor' Application (version 5.0) from www.SecurityXploded.com.

Courtesy: <http://securityxploded.com/chromepassworddecryptor.php>



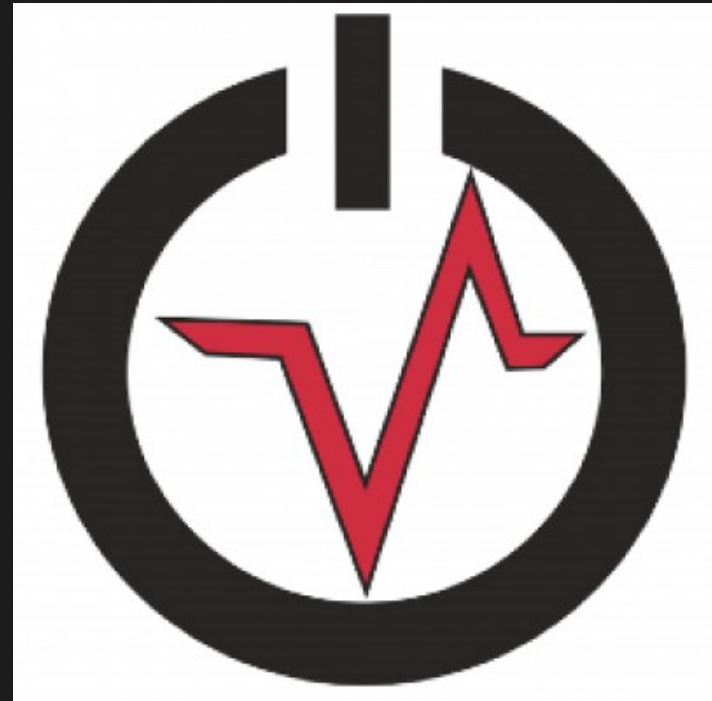
Retrieving Password from Memory

- Passwords are sometimes stored cleartext in memory
 - Attacker compromises a desktop or server + dumps the RAM memory
 - Plain-text or hashed passwords can be extracted from the memory dump
 - i.e. Process Memory Dumper, Volatility, Mimikatz



DEMO TIME!!!


- Retrieving password hashes from memory
 - Dumpit
 - Volatility



Solution: Password Vaults


LastPass...

☒ Toon geavanceerde opties

Wachtwoordlengte: 

☐ Uitspreekbaar

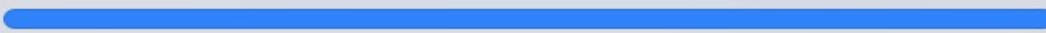
☒ A-Z ☒ a-z ☒ 0-9 ☒ Speciaal

Minimum Numeric Characters 

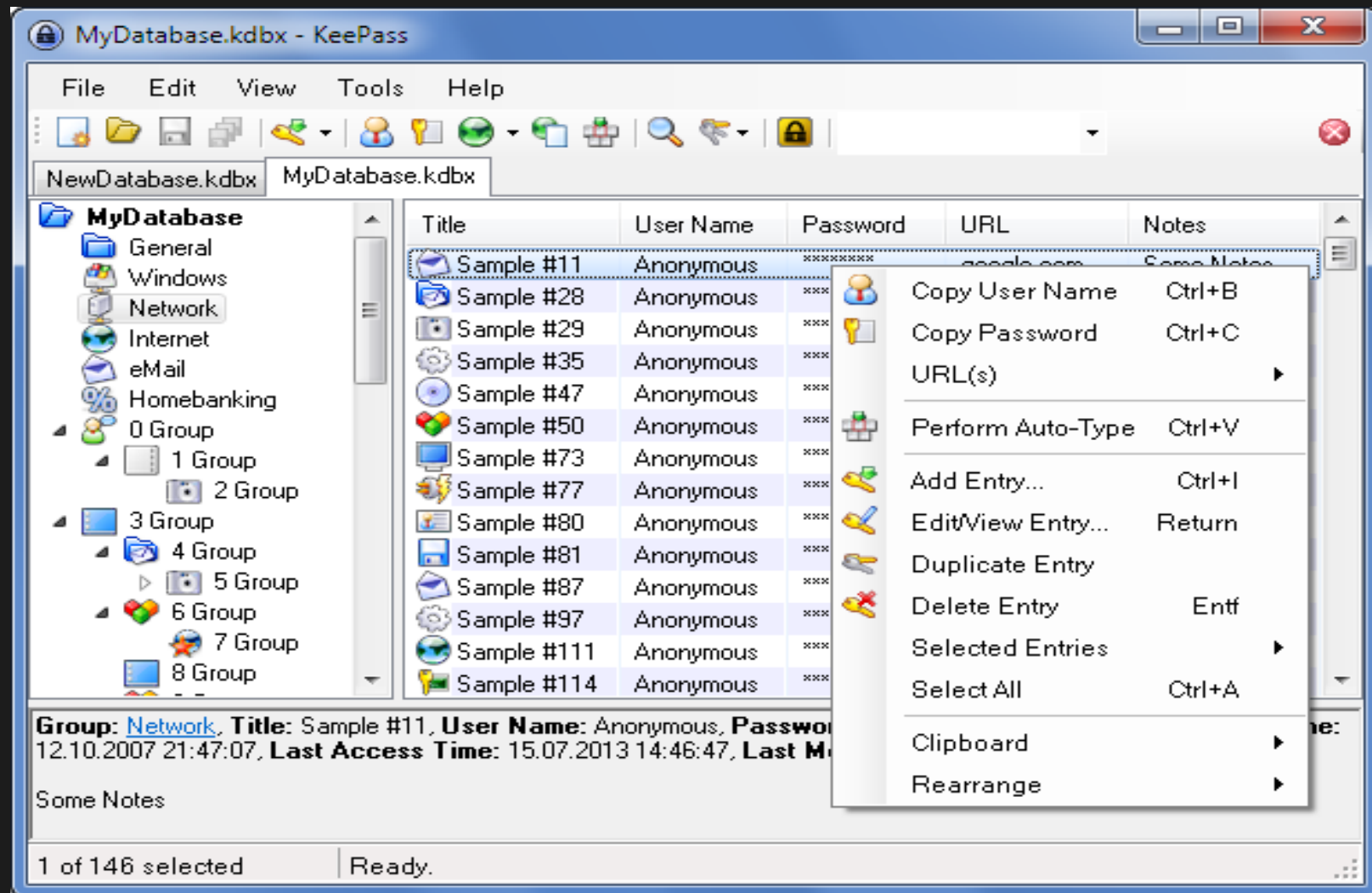
☐ Vermijd dubbelzinnige tekens

☒ Vereist teken van elk type





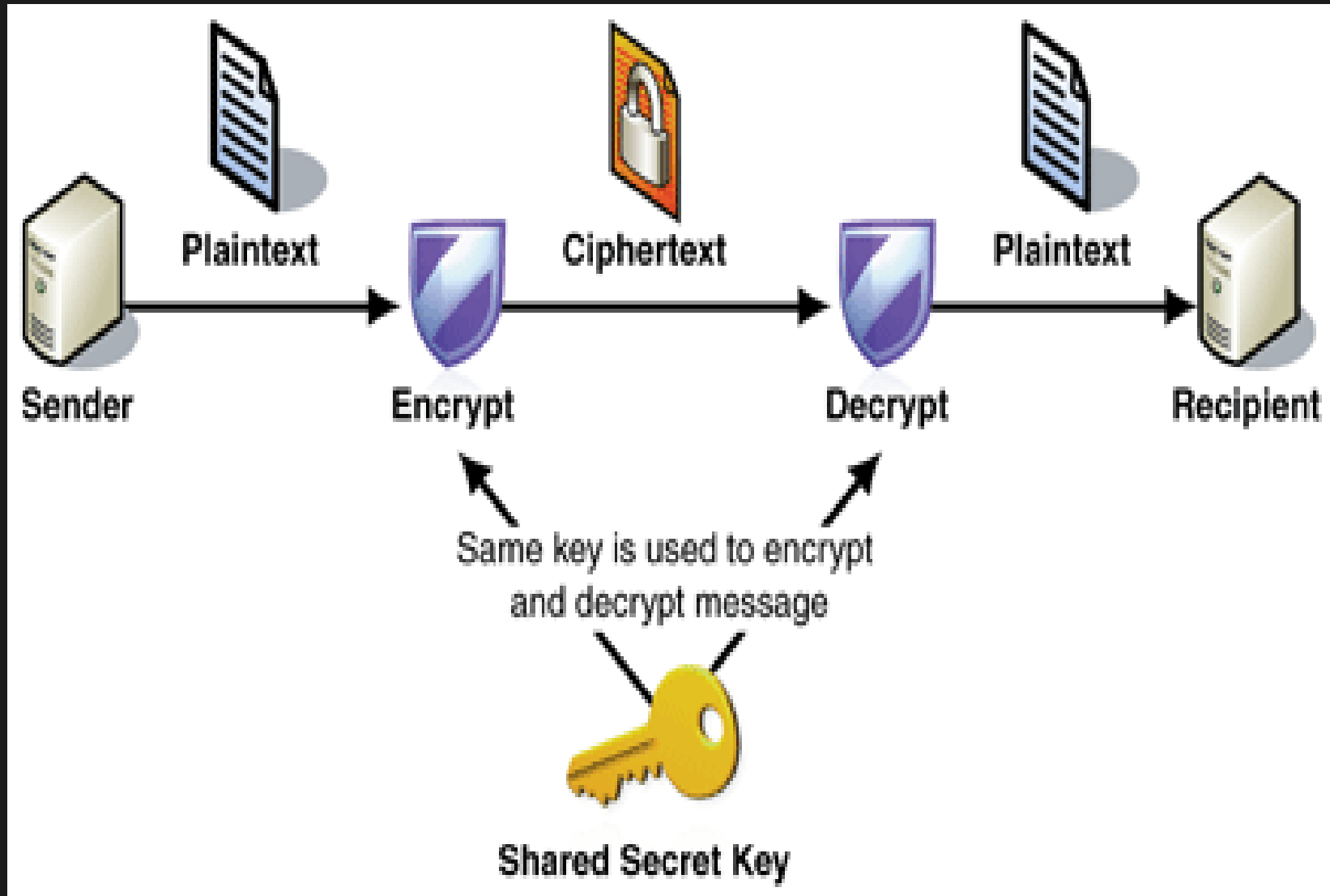
Solution: Password Vaults



Courtesy: <http://keepass.info/>



Solution: Encrypt Data at Rest



Questions?

