SWE 267P Password Hash Assignment
Student: Cheng– Yi Tang

Part 1: Hash generation/cracking online

(1) Generate hashes using MacOS md5 command:

```
❯ cat passwords.txt
qwertyuiop
über_alles!
Lösenord
lakers2023!
❯ while read line; do echo -n "$line" | md5; done < passwords.txt
6eea9b7ef19179a06954edd0f6c05ceb
e44a7cf74cb368dec4e0c0a8af7e6e77
88fc757bb99a74998a3c7de1b8181c20
3b2cd0dc7af78aef77c35e33a9b75b8e

 ~/Doc/M/SWE267/assignment_1 ❯                                    12:04:39
```

(2) Compare hashes: MacOS md5 / md5inline.org / md5decrypt.net

A	B	C	D	E
String	**MacOS md5**	**md5online.org**	**md5decrypt.net**	**md5generator.com**
qwertyuiop	6eea9b7ef19179a06954edd0f6c05ceb	6eea9b7ef19179a06954edd0f6c05ceb	6eea9b7ef19179a06954edd0f6c05ceb	6eea9b7ef19179a06954edd0f6c05ceb
über_alles!	e44a7cf74cb368dec4e0c0a8af7e6e77	e44a7cf74cb368dec4e0c0a8af7e6e77	75db59988623a7fdf3790b41ad3169f3	e44a7cf74cb368dec4e0c0a8af7e6e77
Lösenord	88fc757bb99a74998a3c7de1b8181c20	88fc757bb99a74998a3c7de1b8181c20	da07b18679e77cb2e82df1e6101d60dd	88fc757bb99a74998a3c7de1b8181c20
lakers2023!	3b2cd0dc7af78aef77c35e33a9b75b8e	3b2cd0dc7af78aef77c35e33a9b75b8e	3b2cd0dc7af78aef77c35e33a9b75b8e	3b2cd0dc7af78aef77c35e33a9b75b8e

Finding: md5decrypt.net has different hash output on “über_alles!” And “Lösenord”.
The difference may be due to different encoding of special characters (ü and ö).

Part 2: MD5 hash cracking locally (linkedin_500k_hashes.txt)

2.1 Identify the hash type(s) used in the target file.

Hash type: SHA1

2.2 Rockyou (133 MB) + Noe rule (28.92%)

% hashcat –a 0 –m 100 linkedin_500k_hashes.txt rockyou.txt ––potfile–disable –o cracked_result.txt

Results:
Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: linkedin_500k_hashes.txt
Time.Started.....: Sat Jan 18 15:49:47 2025 (1 min, 15 secs)
Time.Estimated...: Sat Jan 18 15:51:02 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 192.3 kH/s (0.23ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered.....: 144622/500000 (28.92%) Digests (total), 144622/500000 (28.92%) Digests (new)
Remaining.....: 355378 (71.08%) Digests
Recovered/Time...: CUR:113582,N/A,N/A AVG:116322.88,N/A,N/A (Min,Hour,Day)
Progress.....: 14344384/14344384 (100.00%)
Rejected.....: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0–1 Iteration:0–1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b6d3831303838] –> $HEX[042a0337c2a156616d6f732103]

Started: Sat Jan 18 15:49:45 2025
Stopped: Sat Jan 18 15:51:03 2025

2.3.1 Rockyou + Best64 (46.76%)

% hashcat –a 0 –m 100 linkedin_500k_hashes.txt rockyou.txt –r /usr/share/hashcat/rules/best64.rule ––potfile–disable –o best64_cracked_result.txt

Results:
Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: linkedin_500k_hashes.txt
Time.Started.....: Sat Jan 18 15:34:22 2025 (2 mins, 31 secs)
Time.Estimated...: Sat Jan 18 15:36:53 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 7302.9 kH/s (9.24ms) @ Accel:512 Loops:77 Thr:1 Vec:4
Recovered.....: 233812/500000 (46.76%) Digests (total), 233812/500000 (46.76%) Digests (new)
Remaining.....: 266188 (53.24%) Digests
Recovered/Time...: CUR:51795,N/A,N/A AVG:92731.56,N/A,N/A (Min,Hour,Day)
Progress.....: 1104517568/1104517568 (100.00%)
Rejected.....: 0/1104517568 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0–77 Iteration:0–77
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b6d3831303838] –> $HEX[04a156616d6f]

Started: Sat Jan 18 15:34:20 2025
Stopped: Sat Jan 18 15:36:54 2025

2.3.2 Rockyou + InsidePro-PasswordsPro (60.43%)

% hashcat -a 0 -m 100 linkedin_500k_hashes.txt rockyou.txt -r /usr/share/hashcat/rules/InsidePro-PasswordsPro.rule --potfile-disable -o insidePro_cracked_result.txt -w 3

Results:
Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: linkedin_500k_hashes.txt
Time.Started.....: Sat Jan 18 15:57:38 2025 (27 mins, 55 secs)
Time.Estimated...: Sat Jan 18 16:25:33 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/InsidePro-PasswordsPro.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 31518.1 kH/s (28.94ms) @ Accel:512 Loops:256 Thr:1 Vec:4
Recovered.....: 302154/500000 (60.43%) Digests (total), 302154/500000 (60.43%) Digests (new)
Remaining.....: 197846 (39.57%) Digests
Recovered/Time...: CUR:204,N/A,N/A AVG:10825.10,N/A,N/A (Min,Hour,Day)
Progress.....: 46389737856/46389737856 (100.00%)
Rejected.....: 0/46389737856 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:3072-3234 Iteration:0-256
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b6d383931303838] -> $HEX[042a0337c2a176616f6d6f732103]

Started: Sat Jan 18 15:57:37 2025
Stopped: Sat Jan 18 16:25:34 2025

2.4 hk_hlm_founds (389.37 MB) + No Rule (33.68%)

% hashcat –a 0 –m 100 linkedin_500k_hashes.txt hk_hlm_founds.txt ––potfile–disable –o hk_hlm_founds_cracked_result.txt –w 3

Results:
Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: linkedin_500k_hashes.txt
Time.Started.....: Sat Jan 18 17:22:41 2025 (1 min, 35 secs)
Time.Estimated...: Sat Jan 18 17:24:16 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (hk_hlm_founds.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 844.3 kH/s (0.26ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered.....: 168395/500000 (33.68%) Digests (total), 168395/500000 (33.68%) Digests (new)
Remaining.....: 331605 (66.32%) Digests
Recovered/Time...: CUR:99411,N/A,N/A AVG:107201.27,N/A,N/A (Min,Hour,Day)
Progress.....: 38647791/38647791 (100.00%)
Rejected.....: 0/38647791 (0.00%)
Restore.Point....: 38647791/38647791 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0–1 Iteration:0–1
Candidate.Engine.: Device Generator
Candidates.#1....: pirelli67 –> docyzuly

Started: Sat Jan 18 17:22:38 2025
Stopped: Sat Jan 18 17:24:17 2025

2.5 Description

Wordlist + Rule	Cracked Rate	Description
Rockyou + no rule	28.92%	Baseline
Rockyou + best64	46.76%	Adding best64 rules, cracked rate improved
Rockyou + InsidePro–PasswordPro	60.43%	More advanced rules, CR further improved
hk_hlm_founds + no rule	33.68%	Better than baseline, suggesting it contains more relevant password combinations

Part 3: Passphrase cracking

Hash type: SHA256

3.1 Custom wordlist and custom rules (14.29%)

% hashcat –m 1400 hashes/hashes_passphrases.txt wordlists/passphrases.txt –r rules/movie_rules.rule –O –w 3 –o results/custom_results_1.txt

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1400 (SHA2–256)
Hash.Target.....: hashes/hashes_passphrases.txt
Time.Started.....: Wed Jan 22 17:42:54 2025 (14 secs)
Time.Estimated...: Wed Jan 22 17:43:08 2025 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (wordlists/passphrases.txt)
Guess.Mod.....: Rules (rules/movie_rules.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 26169.6 kH/s (1.76ms) @ Accel:512 Loops:17 Thr:1 Vec:4
Recovered.....: 3/21 (14.29%) Digests (total), 0/21 (0.00%) Digests (new)
Progress.....: 395013530/395013530 (100.00%)
Rejected.....: 38543335/395013530 (9.76%)
Restore.Point....: 23236090/23236090 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0–17 Iteration:0–17
Candidate.Engine.: Device Generator
Candidates.#1....: Iran embassy seige –> #private park

Started: Wed Jan 22 17:42:54 2025
Stopped: Wed Jan 22 17:43:09 2025

3.2 Adding more new rules (23.81%)

% hashcat –m 1400 hashes/hashes_passphrases.txt wordlists/passphrases.txt –r rules/movie_rules.rule –r rules/movie_rules2.rule ––force –O –w 3 –o results/custom_results_2.txt

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1400 (SHA2–256)
Hash.Target.....: hashes/hashes_passphrases.txt
Time.Started.....: Wed Jan 22 17:50:26 2025, (2 mins, 56 secs)
Time.Estimated...: Wed Jan 22 17:53:22 2025, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (wordlists/passphrases.txt)
Guess.Mod.....: Rules (rules/movie_rules.rule, rules/movie_rules2.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 34131.0 kH/s (16.84ms) @ Accel:512 Loops:256 Thr:1 Vec:4
Recovered.....: 5/21 (23.81%) Digests (total), 1/21 (4.76%) Digests (new)
Progress.....: 7110243540/7110243540 (100.00%)
Rejected.....: 693780030/7110243540 (9.76%)
Restore.Point....: 23236090/23236090 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:256–306 Iteration:0–256
Candidate.Engine.: Device Generator
Candidates.#1....: IRAN EMBASSY SEIGE –> #private park

Started: Wed Jan 22 17:50:25 2025
Stopped: Wed Jan 22 17:53:23 2025

3.3 Editing existing rules (28.57%)

% hashcat –m 1400 hashes/hashes_passphrases.txt wordlists/passphrases.txt –r rules/movie_rules.rule –r rules/movie_rules2_adv.rule ––force –O –w 3 –o results/custom_results_3.txt

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1400 (SHA2–256)
Hash.Target.....: hashes/hashes_passphrases.txt
Time.Started.....: Wed Jan 22 17:59:49 2025, (3 mins, 40 secs)
Time.Estimated...: Wed Jan 22 18:03:29 2025, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (wordlists/passphrases.txt)
Guess.Mod.....: Rules (rules/movie_rules.rule, rules/movie_rules2_adv.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 34052.4 kH/s (21.91ms) @ Accel:512 Loops:256 Thr:1 Vec:4
Recovered.....: 6/21 (28.57%) Digests (total), 1/21 (4.76%) Digests (new)
Progress.....: 9085311190/9085311190 (100.00%)
Rejected.....: 886496705/9085311190 (9.76%)
Restore.Point....: 23236090/23236090 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:256–391 Iteration:0–256
Candidate.Engine.: Device Generator
Candidates.#1....: IRAN EMBASSY SEIGE* –> #private park23

Started: Wed Jan 22 17:59:48 2025
Stopped: Wed Jan 22 18:03:31 2025

3.4 Description

Hashes File: hashes_passphrases.txt
Hash Type: SHA–256 (mode: 1400)
Dictionary Used: passphrases.txt
Rules Applied:

1. movie_rules.rule (14.29%, 15 s)
2. movie_rules.rule + movie_rules2.rule (23.81%, 2 m 58 s)
   Stacked rules improved recovery rate
3. movie_rules.rule + movie_rules2_adv.rule (28.57%, 3 m 43 s)
   Extended leetspeak rules showed better results

Part 4: Document Password Cracking

4.1 Use Hashcat to crack a password protected Libreoffice document

Extract password hash using John Python script
./libreoffice2john.py hashcat.odt > hashes/odt_hashes.txt

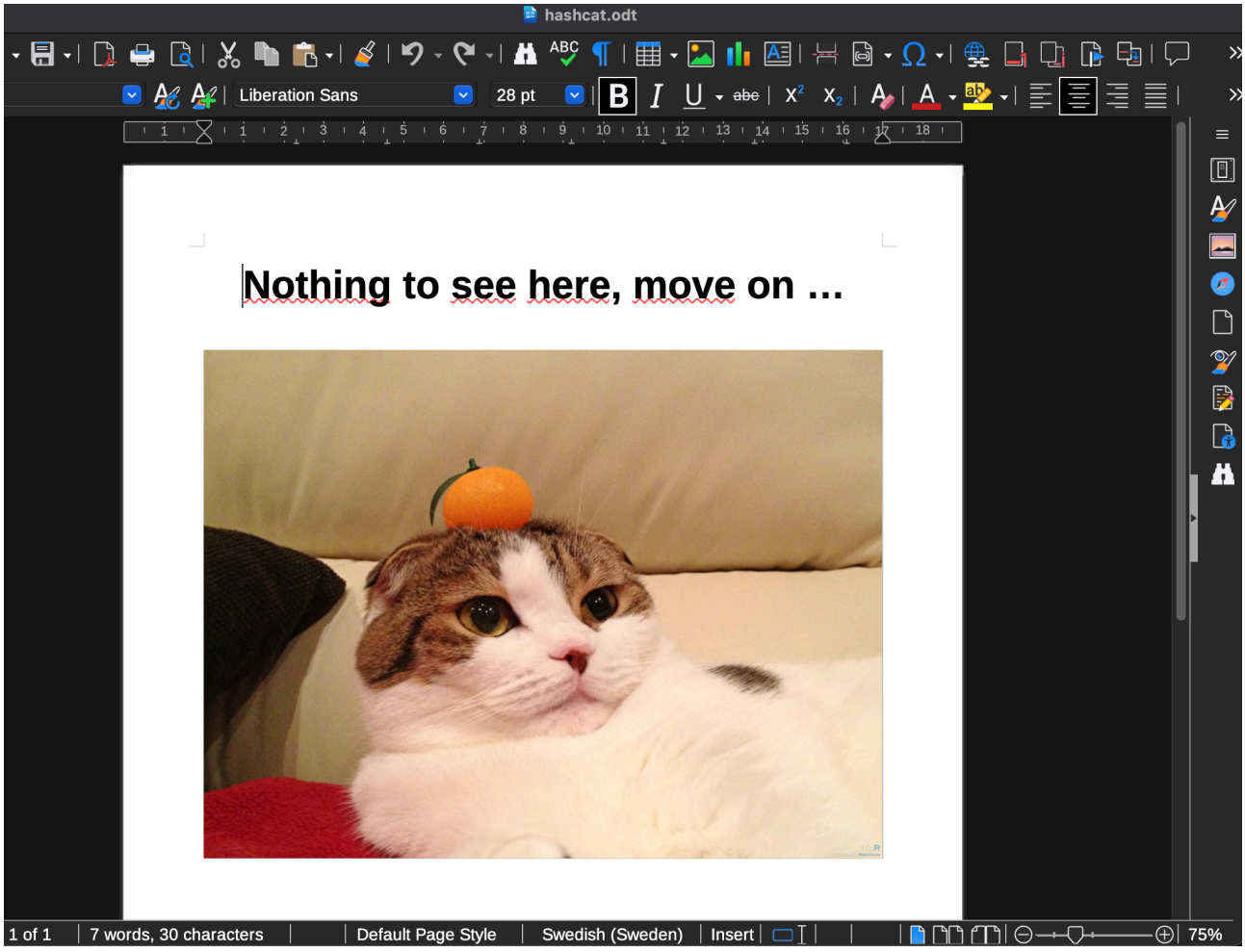
Identify hash type
Open Document Format (ODF) 1.2 (SHA-256, AES) mode: 18400

Crack extracted hash
hashcat -a 0 -m 18400 hashes/clean_hash.txt /usr/share/wordlists/rockyou.txt -w 2

Result:
odf*1*1*1024*32*9fd1c9be34d1bc2dea61644f6f659b330b69eae9fc72d29bd4539c7d7d9cb
434*16*5ab78e4550a9453feb2d60f83d0b6869*16*f1ea2a614223c64274b33866e01a5207*0*
d2076332386588e150207046e8a3510ad6ebb299fec6852852f8dc7494008cbb23692813e259
781bd1c95c0e1a76c92353ccdedd9fed56a2ce4270471414078bb82f88db372765257be963090
ca72a288a16bbd33baf2c0661c18791dc0baf15ed4300d3fc1062479ebbeb31b8cfe93d4b80cc2d
73a9fab83e4bfa427a2cdee2b28a782f1237ae1c55b22fea31adb01cc4a87eecc8b0941d92861df
d1d980d64df1c9858dcaa42b9d6b192554d967da6c82dfe7c2b9ca30efb043e57aa1fa7619ee7d
14b8cf66c657871299572b1c6991707819af6dd6b0e7847f0a57583c5ad43351fca184f1bd20ede
37c376079cee9fe82735ffb021fd7530131195c9c5013060155980e58107709bb48bd29d77cd212
5057658e8e7cd1f399df36f9b3b8a5f88c0cbc8172031f52c37f83d877d55549f0c981d6601b31e
8c76961bb0e0482c568820c109c24580bae82b637a3c2823b799333d1afa4b506cb41acd31605
bc3b1eb6ac8e1cc8b42605237ed251b633c520ece2be909de1deffc881dff7d6be11595b844005a
291b3b4274574ce0dc5c1bc4e0b4b82095c368799328cc0e8c73fe4d26c8c31eb1c6451952c77
4ecfe7b2b0dc22d6df6744ea3f7599a25bd4cd79767cfc9d3899b1fa83ffcddb2f1ec785a5c3183
09495f82e416bd6b5983f10794fb6dc3081e47e82568f4d8ffb32777e99ebc90fb073492676b8d
a1bc5581f79cba3bc6598c8e3c31e79810f2e0503e7f250da2359cd9c74087448a2d8a325275e
2e6f0b32c42efccf2dfc8a0b26aeee4809e638c4718d7ec45d73bd5a483a2e329a81c2e3c2cb3
e4ec179d125470c036ed51da23e3bf06febe3050d0fd6101eaefaf4e19d5a73e44dea9302b2f7e3
608c4c1b8411ccf031ad9d1a9d82be2c2fd8599b69ed7d5777c6ba8b61d0f082ede8878d821c96
52af3b439a545aceeda2d2e0df3588ca4fd1cd857ade2cdd2a295e6b7f74b2577192eb5b4686f
b042d57ed50965fb5ee235c8e262e4a0b6b4037a3b3be427d71fd39e6834ccaa85750d4451a71
a734e20cf0b563a60dff24fda0b5ec54330934e8d6ced72639178c7aa271573ff7e0e1c16f01637
d4db4c75f30f63d22cb57018c7e16b5eb3420ae180fd624fa50d574025c8b3702e9957161ffcbf0
9806ad6e4b58143f84efa4260386a6829e62ef858882e98c696dcbc3eb472402773e2a0e3cffc
391f33f38541cbf3cfd2397b0ca1d35511d1c27b61a8828f3a89500ab94d90883af9e66813f600a5
bfd3c79bd8e1669ac4cf2d09e644fb89792fde191bc478b21b3b36b752e3346f75c566d5a1ca35
41d287aea9f80d3051575945aee0d78bfc6308caadb46dd9cc9d76c9a6226e5dcaab76f944c0b
94a02bafdd2ee72ac118373da55793b1e191ceb4ac1f0900f8e7bc1b489d424c3da3d685d858c18
4a625037a688554934:[cowboys!]

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18400 (Open Document Format (ODF) 1.2 (SHA-256, AES))
Hash.Target.....: odf*1*1*1024*32*9fd1c9be34d1bc2dea61644f6f659b330...554934
Time.Started.....: Thu Jan 23 06:05:33 2025 (12 mins, 14 secs)
Time.Estimated...: Thu Jan 23 06:17:47 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 13380 H/s (9.28ms) @ Accel:16 Loops:1023 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10464128/14344385 (72.95%)
Rejected.....: 0/10464128 (0.00%)
Restore.Point....: 10464000/14344385 (72.95%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1023
Candidate.Engine.: Device Generator
Candidates.#1....: [ensions -> [cokitos]

Started: Thu Jan 23 06:05:30 2025
Stopped: Thu Jan 23 06:17:48 2025



4.2 Description

Hash File: clean_hash.txt (extracted)
Open Document Format (ODF) 1.2 (SHA-256, AES) mode: 18400
Dictionary: rockyou.txt
Recovered: 1/1
Password: [cowboys!]
Time: 12 minutes and 18 seconds