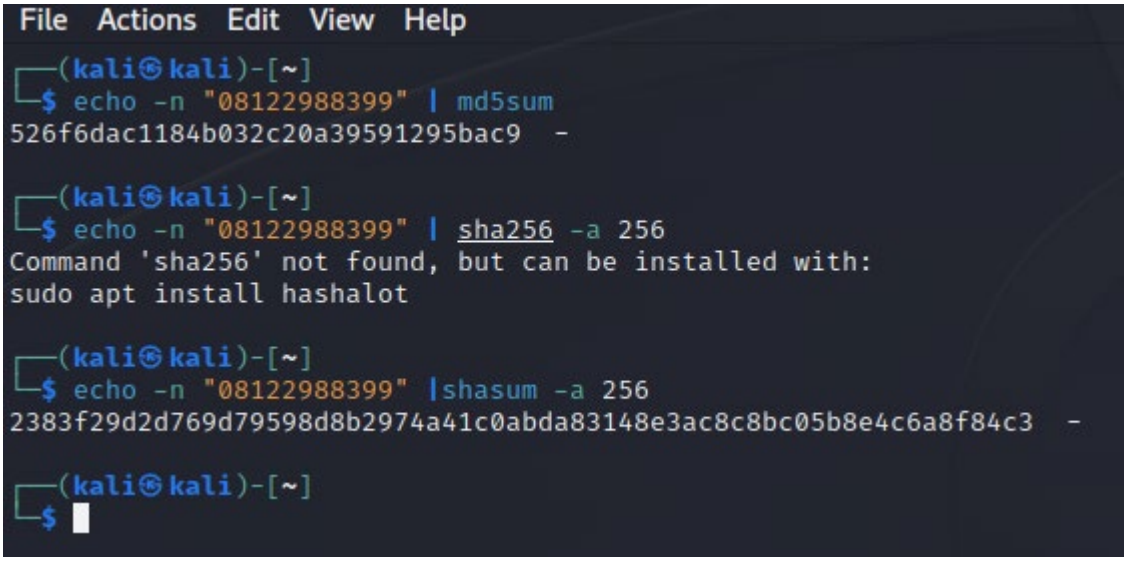
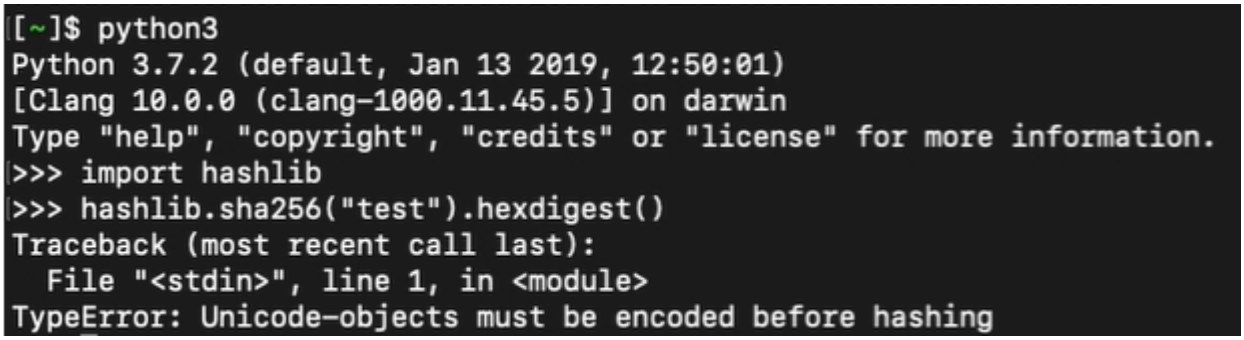
Задание выполнил студент группы 2345 Романенко Кирилл

Задание 1

Необходимо для каждой строки получить хеши с помощью алгоритмов: sha256, bcrypt (с солью '$2b$15$NSVH/I.9u1l/WoYUd/sSI.') и md5. Для выполнения задания используйте библиотеки вашего языка программирования (например, для Python это будут hashlib и bcrypt).





Строка	md5	sha256
08122988399	526f6dac1184b032c20a39591295bac9	2383f29d2d769d79598d8b2974a41c0abda83148e3ac8c8bc05b8e4c6a8f84c3
nampoly2537	32d2958b59c29dfd2c973b89ec1a8d50	77b0171d0810854aac67c3136bd9f71bb71023ac5e84f7392193c4d017ab3d18
lasabre97	e83f103e96dcd748bfe537fabc0aa9f8	eff69674891a0c2302ee2442e42a8da2cacacd439fad77b04d11a05945194962
as534031	e9ef6dc54a12b0a3d6949c52277ec307	a4ca86841ef76acb5670793a0bf6707cc8b7f71a1929d262bcb1453e990b4d22
Victor_	659fcdcd8ff8760a177304343793ec27	8b8a228125ea9ea59171fbfce981831645f113c27a5391a8018385c80ae32dcb
16MSTF68AYSL	5d9f064eb20475ac46386624623fb0b0	1402aa4810a4a079c24da72f1976a2c3591887a3032dfd3b94e8c994626620e4
hhrules	d183c875ab64b60eb8693a8f4cffa39c	f627b35ddf2c53bd37caa6309613161e45c8b59869c0ba683f5f9b902cd614d7
cpt704242	e54b608ea04911e91b9a764f1e344389	df337bec74c109fdd3d647ead37f4623f89f93d3b74141871f054093dae60b1e

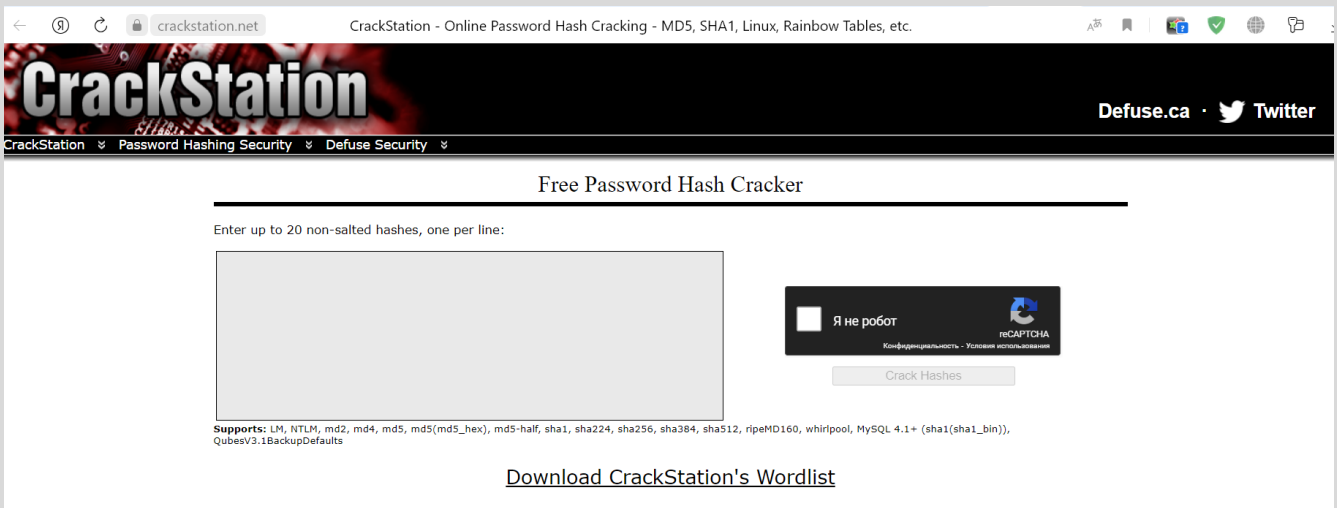
gracemac	6c9f6f998411ca1b358334d13f39a255	a9a3bbf5e6524aa6b3c4643cd0dcd0984874c71fe6b40d6082dbe598a92c9b08
rayas123123	524dfc4987fdcc666635dd8e949e69d5	5ca7cc678969c5732df800a9816d488897707de83ac2da9c4beb304ef2dee0a2

Задание 2

Найдите исходные значения каждого из хешей. Для выполнения задания разрешается использовать любые методы.

```
23f6121371ef7563ec479de345c9e479
7351a8f9d143de67724772ea1a7e7e82d068cb77c3f495d5d234083d686c1226
cf9baae799c1d9164d2b6c37acf8562d
ae6a4840fe4e29991483c8a4115451d105e2e057e6870279c15c211d3375546f
004a602d9e890b00
9407cad0b776fd5f614649eddff47eefc71aa82d
e0728635632956dd3d28e0b9c28bf97735de32c3
3bb0d8c10c4ce5561daa0d82ee65d692a9d70276f7e53006aa5c4ad34aee1c13
9f00e35c7729cdac242e86051a57020d
6650ee0bf5af2a915618beb0361e67c04cedd4ea0c00d68ea72b16866c62dd16
eead40c59c83c69bdd2505ac081e09c0354345e2
7d63b6cbbed434353836dc011701321ac4827b6d
f1df20f71e680534
8a99ad26f053411a73104bfe0f1e19193efd5587eefd84bda435ed92397850d1
78dd2b61c96e895035c87528b5c3e2a9
b3dab40f3d51065754e4f0ef0d20039d
c9203499e3a2ff2b1244913777a3614954c1cd17240695fc160fe96914094912
8e82dfe15d36d6ec75f38de62128cf386964bf80b423ccda4fd239fc942d2cd9
43ca9303ecf07627
3ad12414555b1e01870647cb4dc99df88dbdd7eaf1494900fa9dd89bb2758cb3
```

Вариант 1. Открыл сайт https://crackstation.net/



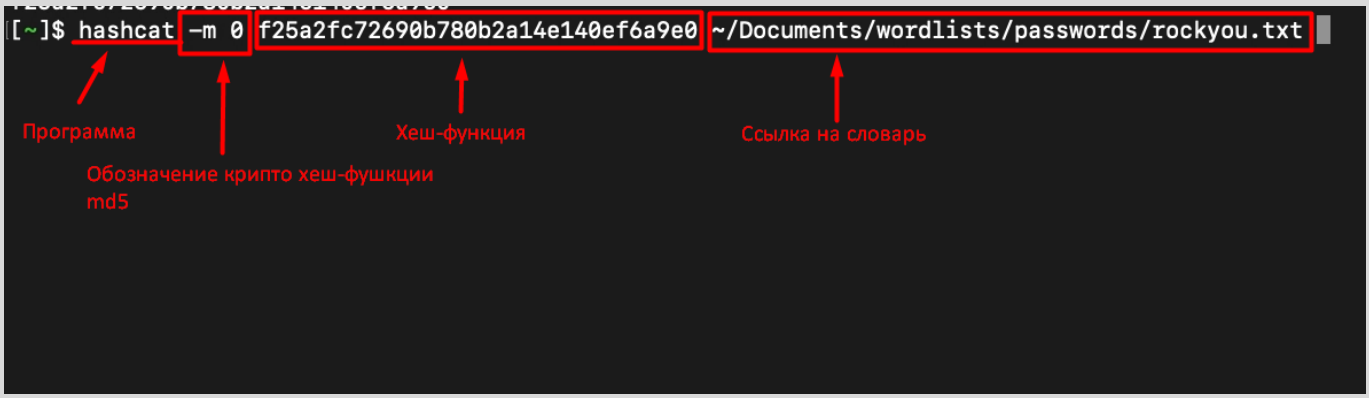
Ввёл задание в окно ввода. Выполнил капчу. Готово

Hash	Type	Result
23f6121371ef7563ec479de345c9e479	md5	4401204
7351a8f9d143de67724772ea1a7e7e82d068cb77c3f495d5d234083d686c1226	sha256	ogledalo15
cf9baae799c1d9164d2b6c37acf8562d	md5	HI2332
ae6a4840fe4e29991483c8a4115451d105e2e057e6870279c15c211d3375546f	sha256	brittls17
004a602d9e890b00	md5	blake1994
9407cad0b776fd5f614649eddff47eefc71aa82d	sha1	h99336724
e0728635632956dd3d28e0b9c28bf97735de32c3	sha1	katana07
3bb0d8c10c4ce5561daa0d82ee65d692a9d70276f7e53006aa5c4ad34aee1c13	sha256	jk01e8211
9f00e35c7729cdac242e86051a57020d	md5	benitesangelina
6650ee0bf5af2a915618beb0361e67c04cedd4ea0c00d68ea72b16866c62dd16	sha256	64tj3y
eead40c59c83c69bdd2505ac081e09c0354345e2	sha1	BIGJOBBY
7d63b6cbbed434353836dc011701321ac4827b6d	sha1	honestthai
f1df20f71e680534	md5	michaelallen2
f1df20f71e680534	md5	michaelallen2
8a99ad26f053411a73104bfe0f1e19193efd5587eefd84bda435ed92397850d1	sha256	RR310501
78dd2b61c96e895035c87528b5c3e2a9	md5	1988what
b3dab40f3d51065754e4f0ef0d20039d	md5	themac
c9203499e3a2ff2b1244913777a3614954c1cd17240695fc160fe96914094912	sha256	37100136
8e82dfe15d36d6ec75f38de62128cf386964bf80b423ccda4fd239fc942d2cd9	sha256	alycia_11
43ca9303ecf07627	md5	samanthya
43ca9303ecf07627	md5	samanthya
3ad12414555b1e01870647cb4dc99df88dbdd7eaf1494900fa9dd89bb2758cb3	sha256	kokofat3

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Вариант 2. С помощью программы hashcat

Ввёл команду



Результат выполнения команды

```
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Temperature abort trigger disabled.

Dictionary cache hit:
* Filename..: /Users/n.stupin/Documents/wordlists/passwords/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

f25a2fc72690b780b2a14e140ef6a9e0:iloveyou

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: f25a2fc72690b780b2a14e140ef6a9e0
Time.Started.....: Sat May  4 17:09:24 2019 (0 secs)
Time.Estimated...: Sat May  4 17:09:24 2019 (0 secs)
Guess.Base.......: File (/Users/n.stupin/Documents/wordlists/passwords/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#2.....:  6464.0 kH/s (11.77ms) @ Accel:16 Loops:1 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 196608/14344384 (1.37%)
Rejected.........: 0/196608 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Candidates.#2....: 123456 -> piggy!

Started: Sat May  4 17:09:20 2019
Stopped: Sat May  4 17:09:25 2019
```

Ответ: iloveyou