Cybersecurity MSc: Applied Cryptography 2024-25

Special Season Project: Reversing password hashes with rainbow tables

July 30, 2025 Due date: September 1, 2025

Changelog

- v1.0 - Initial version.

Introduction

Assume the following scheme is being used to hash passwords: the password is expanded to the right with copies of itself, until its number of bytes is 16 (128 bits) and is used as an AES-128 key to encrypt itself; the result is an hashed password.

$$\text{password} = \text{"abcdef"} \overset{\text{expansion}}{\longrightarrow} \text{key} = \text{"abdcefabcdefabcd"}$$

$$\text{hashed password} = H\left(\text{password}\right) = \text{AES}_{\text{key}}\left(\text{key}\right)$$

Assume that passwords have a given character length l and are formed by caracters from the following 64-character set: [`a-zA-Z0-9?!`].

1 Homework

The work consists on finding a password P given a $H\left(P\right)$. This can always be done by a brute-force attack using about 64^l AES transformations. Alternately, one can pre-compute all 64^l possible hashes and then find P in essentially constant time; this requires $O\left(64^l\right)$ space. The goal of using a rainbow table is to do better, namely less than 64^l time and space.

Write two programs, `table` and `guess`. The first of these corresponds to the pre-processing phase in which you generate a rainbow table, while the second corresponds to the phase in which you are given $H\left(P\right)$ and need to recover P using a pre-computed rainbow table.

`table` should take three command-line arguments, the third being a rainbow file name. The first command-line argument will be l, the password length (in characters from the above referred character set). The second argument s determines the maximum size of the rainbow table; it must be no larger than 16×2^s bytes. The raindow table should include the length of the passwords (l) and the length of the chains (k), that should be computed from s.

`guess` should take two command-line arguments, and write the results to the standard output. The first argument is the rainbow file, from which l and k are extracted. The final argument is $H\left(P\right)$. When you run `guess rainbow H(P)`, the output of `guess` should include two items: the password P or failure, and the number of times AES was evaluated.

2 Homework delivery

Send your code to the course teachers through Elearning (a submission link will be provided). Include a small report, with no more than 10 pages, describing the implementation (not copies of the code!)

and the mathematical relationship between the space used by rainbow (which is proportional to 2^s) and the number of (expected) AES evaluations by `guess`.

Use your programs to recover the passwords from the following hashes and include the answer in your report (values in hexadecimal, low-order bytes on the left):

Note: it may not be possible to find solutions with Python programs during the period given to implement, test and deliver this project, since performance is crucial.

#	4-character passwords
1	f8 34 0c 83 6d 41 f7 7c d9 27 08 bb d5 44 3c be
2	a5 da 39 d0 4c 81 72 87 74 0f 53 e6 bd c1 3b 5c
3	53 21 ab b3 b5 7f 53 5e 0e 31 86 b7 a3 20 4d ff
4	62 6e 33 f1 35 74 40 29 35 a3 0b 2d 20 0e be 53
5	ff 29 3b 3c 17 78 5c 6e af cc 1d 0f 06 15 f4 45
6	21 25 49 07 1c 90 2a e2 8b c2 39 ce 6f 1e ec 49
7	c1 fd be 6d c8 eb 0e d6 ae ea 0e 87 7b a8 36 dd
8	72 75 78 e6 76 8a 67 50 ad a7 16 f8 db b0 e4 7c
9	c7 7e 40 f4 17 dc 4e d0 74 b1 df 3b 91 6f 85 c9
10	11 cd 64 9a 72 07 5e 28 38 4b ce 23 c7 2c 25 3d

#	5-character passwords
1	2a 06 b9 5a 26 4d 30 c1 28 2c 0e ac c8 fd 4e ff
2	f3 67 b5 55 77 26 a7 a7 e3 c4 12 e2 e2 b8 b6 7d
3	0b 91 2f 37 2a e9 01 46 99 20 80 30 51 d9 5b 6c
4	b6 bb 41 44 91 8a 25 7b 25 62 93 b7 df e0 80 ae
5	7f 15 0f 79 90 a2 5b 72 ff 28 81 af e4 b8 8b 62
6	25 8f 7e ba d2 96 c6 b1 4d cd 7d 11 fd 21 fb 57
7	30 ac 5f 6e 34 3f cf a9 67 18 c4 65 e6 9e a0 e0
8	05 93 bd 4d 2a 40 db 0e de 8c 55 bf 62 ee 86 46
9	80 1c 58 0f d6 1a 3a 36 fe ea 0f 02 7b 99 0c 22
10	7f 03 98 78 4a 06 92 bd 30 18 04 ae b9 43 6d 76

#	6-character passwords
1	02 18 86 70 c5 29 1c 33 fe 51 76 f9 e4 7b 55 76
2	98 62 47 da d9 d3 ae 53 fa 97 1e 0d 85 31 61 2c
3	84 53 08 66 21 fa c9 a8 e4 db 75 70 8a 05 3b 48
4	aa 92 6e 31 b4 a1 d3 49 e1 e8 e0 68 7b e1 9b 99
5	48 05 1a 93 06 67 ac 6d 0f f9 23 4c 4a af 8f e3
6	ca f8 60 1b 99 71 61 d9 d8 b4 67 a2 4f d5 02 04
7	21 18 62 bf d5 b5 fd ad 68 47 4e df 8c e5 9d 1c
8	5e b0 cc b1 e0 cd 2a 5a 3a 85 32 23 11 3e 12 4f
9	27 2f 3f e7 cb 9a d5 5d 2b e1 ec db 9c 83 6f 67
10	f9 67 08 5d 62 3b d1 70 58 4d 4e 80 21 1f 38 b0

#	7-character passwords
1	89 c6 a9 63 86 46 d4 d5 30 80 a3 04 f2 3c 7f 4e
2	c3 ae 09 89 3f e5 8f 0f 39 95 61 fa 96 a6 cb 41
3	8b 91 e9 96 7c f6 d5 18 2b 2a 28 61 e6 39 d3 9b
4	ff a7 6f a8 67 d0 d0 75 f2 f7 7d 99 74 1c 28 3b
5	69 12 0c 68 50 03 f0 55 95 20 83 16 ba 45 79 b4
6	92 b1 80 33 98 69 ae 0e 74 ff 71 ee 24 36 40 59
7	8d a0 50 0f f7 59 af 32 68 e9 3f d7 3e ba a7 bc
8	d8 47 d6 06 11 ed 81 4c 33 e8 f7 27 5e 43 d8 bc
9	2a af ba 15 31 3c 0c 80 e0 2d 92 8a 33 c5 07 55
10	90 40 41 32 7e ae 36 75 f3 6e fa ed a1 f1 d3 c1

#	8-character passwords
1	6d 4c c6 10 4e e5 75 20 52 90 5a e3 66 de 17 88
2	25 56 3e 8d d5 02 e7 9f 89 c0 24 33 f0 11 eb 9b
3	76 3e f3 ff 10 f5 95 4e ed 46 26 10 ba e0 34 b5
4	e4 0a 7d 82 d7 d3 60 6a 56 48 49 80 9e a8 e8 82
5	2e 22 96 1e 4b 41 06 7d f8 57 ab a6 e5 0f d7 8a
6	04 dc 6e d7 00 7b e8 f3 2f 2c 27 dd bb d0 0d 2a
7	a5 f9 d6 ba 84 52 47 91 06 3a 50 bb 1e cf d0 b0
8	52 3c 03 4f c8 c5 8b 7a 6a 1e 18 2b b2 3e 01 5c
9	d7 71 d6 57 6c 6a ee 69 a9 77 8f ef 4f b3 45 bc
10	36 8d c4 55 39 ed d4 90 52 64 2e e6 36 0d d7 68

3 Test vectors

The following test vectors were generated with AES-128 using the C Crypto library.

password	key	hashed password
abcd	abcdabcdabcdabcd	80 b3 a6 04 da 5b b7 0e 25 0f ad 29 16 3c e0 c4
abcde	abcdeabcdeabcdea	6a 1d 66 81 cd 5a 19 f3 9b af 63 9c 35 30 19 c4
abcdef	abcdefabcdefabcd	3f 0f 29 b8 9f eb 70 1e a1 68 4c f3 27 4d 34 4a
abcdefg	abcdefgabcdefgab	9b d7 ce 68 57 bb c7 b3 fd a1 98 0c 98 ba 14 ee
abcdefgh	abcdefghabcdefgh	ff 4e b3 ad 54 a5 e1 4a ec b2 10 8b 0e 0a 65 80
abcdefghi	abcdefghiabcdefg	87 70 99 4a d5 ba d0 65 f1 1f e5 90 2e 72 1f 49
abcdefghij	abcdefghijabcdef	65 64 2d 11 20 c8 43 6a ea 03 50 ee 84 fe ad 0a
abcdefghijk	abcdefghijkabcde	bf 51 ed 51 ab 17 d1 39 d6 9b 48 3c a4 44 83 54
abcdefghijkl	abcdefghijklabcd	f1 2b 2b 64 74 6c fd dd a5 b0 bd 3c 0f 4a 55 5a
abcdefghijklm	abcdefghijklmabc	17 fc 34 3a 6b b7 06 50 59 13 a1 8f 08 c8 a2 b3
abcdefghijklmn	abcdefghijklmnab	f6 ef 84 8e 18 77 8b 8b aa 6f 07 a0 ab 8b fd 5a
abcdefghijklmno	abcdefghijklmnoa	34 07 f0 ac a6 18 2a f8 98 3f 63 2d c1 26 91 b1
abcdefghijklmnop	abcdefghijklmnop	a9 13 29 af 99 a7 8d 02 ae c1 7c 50 77 57 aa ef