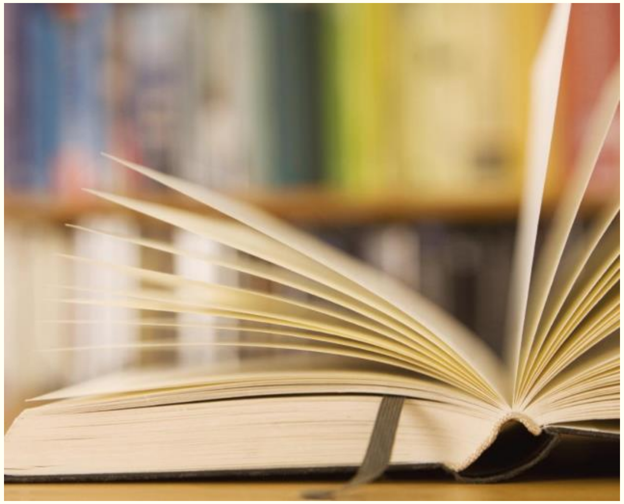
RAINBOW Table

Example



Rainbow table: Example

- The following example demonstrates how rainbow table is constructed and how a pre-image searching is done using rainbow table.
- A small, 15 passwords are randomly selected from a list of common words that may be used as passwords; the password.txt file is shown in the next slide.
- For demonstration purpose, I included the hashed value of each password together with the corresponding reduction value from a typical reduction function. The reduction function I am using is a simple modulus function using the size of the password.txt file as the modulo.

Password.txt

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	15
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	14
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	9
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	1
6	mundane	147e19efcaca65ee9f16ac703514b374	7
7	bake	a6ecfad3e0f9a51c6335848449a91bed	7
8	zoo	d2cbe65f53da8607e64173c1a83394fe	5
9	zombie	0eda241fc65ccf35d9743309ac395215	15
10	freehold	47ebf781047c3340fd5b0363b10c82aa	1
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	5
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	3
13	heel	649be85da19882e6335962b2842385ea	14
14	insect	dce41a93f7edb175dfc59a4d52105847	13
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	7

Reduction function

- I am using a simple reduction function as follow:

$$\boxed{r = MD5(password)\ mod\ sizeOfPasswordFile}$$

Where:

- $r\ - the\ reduction\ value$
- $password\ - the\ current\ password\ to\ be\ hashed\ using\ MD5\ hash\ functions.$
- $sizeOfPasswordFile\ - the\ total\ number\ of\ passwords\ contains\ in\ the\ password.txt\ file.$

- In this example, the sizeOfPasswordFile is 15 (15 different passwords are in the password.txt file that I use.)

Hash-chain

- Create a hash-chain to generate entries for the rainbow table:
  - Read in the list of possible passwords:

10th
Ababa
TWA
Abater
Aaron
mundane
bake
zoo
zombie
freehold
abalone
sun
heel
insect
prosecute

$$\mathit{sizeOfPasswordFile} = 15$$

Hash-chain

- For each previously unused password, mark it as used. For example, the first unused password is 10th.
  - Apply MD5 hash function to the password to get a hashed- value. For example,

$$\begin{aligned} hv &= MD5(10th) \\ &= 515da2caf582ac4801cbb5d876c73c90 \end{aligned}$$

Hash-chain

- Next, convert the digest (hexadecimal value) into long number before we apply the reduction function by taking modulus of the size of the password file. For example,

$$r = (108153653096848345464776048863879838864 \; mod \; 15) + 1 \\ = 15$$

Hash-chain

- The reduction function returns a value 15. The value 15 indicates that the 15th password in the password file will be the next password to be chained into the list. Mark the 15th password as used and repeat the previous described steps 4 more times.
- After the 4th repeat, store the first password in the list and the last hashed value into the rainbow table.

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	15
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	14
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	9
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	1
6	mundane	147e19efcaca65ee9f16ac703514b374	7
7	bake	a6ecfad3e0f9a51c6335848449a91bed	7
8	zoo	d2cbe65f53da8607e64173c1a83394fe	5
9	zombie	0eda241fc65ccf35d9743309ac395215	15
10	freehold	47ebf781047c3340fd5b0363b10c82aa	1
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	5
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	3
13	heel	649be85da19882e6335962b2842385ea	14
14	insect	dce41a93f7edb175dfc59a4d52105847	13
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	7

Hash-list:	
10th	515da2caf582ac4801cbb5d876c73c90
prosecute	dce41a93f7edb175dfc59a4d52105847
bake	a6ecfad3e0f9a51c6335848449a91bed
zombie	0eda241fc65ccf35d9743309ac395215
mundane	147e19efcaca65ee9f16ac703514b374

Rainbow Table:	
10th	147e19efcaca65ee9f16ac703514b374

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

Hash-list:	
Ababa	bbf12b95db10da96472e2e019ffa4659
mundane	147e19efcaca65ee9f16ac703514b374
mundane	147e19efcaca65ee9f16ac703514b374
mundane	147e19efcaca65ee9f16ac703514b374
mundane	147e19efcaca65ee9f16ac703514b374

Rainbow Table:	
10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

Hash-list:	
TWA	47221236d3df2a4cca11b1d7512faf7d
heel	649be85da19882e6335962b2842385ea
abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7
Abater	d48f58d9dc9af4b68b860e71f7336b44
10th	515da2caf582ac4801cbb5d876c73c90

Rainbow Table:	
10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

Hash-list:

sun	ebd556e6dfc99dbed29675ce1c6c68e5
prosecute	c18ac77dbe4b7211c616667e4f8fc526
abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7
Abater	d48f58d9dc9af4b68b860e71f7336b44
10th	515da2caf582ac4801cbb5d876c73c90

Rainbow Table:

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

Hash-list:	
zoo	d2cbe65f53da8607e64173c1a83394fe
Abater	d48f58d9dc9af4b68b860e71f7336b44
10th	515da2caf582ac4801cbb5d876c73c90
insect	dce41a93f7edb175dfc59a4d52105847
bake	a6ecfad3e0f9a51c6335848449a91bed

Rainbow Table:	
10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

Hash-list:

Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e
abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7
Abater	d48f58d9dc9af4b68b860e71f7336b44
10th	515da2caf582ac4801cbb5d876c73c90
insect	dce41a93f7edb175dfc59a4d52105847

Rainbow Table:

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847

Construction of Rainbow table:

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

Hash-list:	
freehold	47ebf781047c3340fd5b0363b10c82aa
zoo	d2cbe65f53da8607e64173c1a83394fe
Abater	d48f58d9dc9af4b68b860e71f7336b44
10th	515da2caf582ac4801cbb5d876c73c90
insect	dce41a93f7edb175dfc59a4d52105847

Rainbow Table:	
10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

The rainbow table:

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

A successful search of a pre-image

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain. User enter 6e1ba55b046f7d62bbd6dc33b63d5ec7.

How does it work?

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain.
User enter 6e1ba55b046f7d62bbd6dc33b63d5ec7.

1. Check if the hash-value is found in the rainbow table.
   No, 6e1ba55b046f7d62bbd6dc33b63d5ec7 is not found in the rainbow table.
2. Apply the reduction function to the hash-value until a match is found in the rainbow table.

6e1ba55b046f7d62bbd6dc33b63d5ec7 → Abater → D48f58d9dc9af4b68b860e71f7336b44 → 10th → 515da2caf582ac4801cbb5d876c73c90.

3. Starting with the password TWA a search is done. After a few reduction is done, the hash-value 6e1ba55b046f7d62bbd6dc33b63d5ec7 is found.
4. The password (preimage of the hash-value 6e1ba55b046f7d62bbd6dc33b63d5ec7) is **abalone**.

A successful search of a password in a chain that involve collision.

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain.
User enter d2cbe65f53da8607e64173c1a83394fe.

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain.
User enter d2cbe65f53da8607e64173c1a83394fe.

1. Check if the hash-value is found in the rainbow table.
   No, d2cbe65f53da8607e64173c1a83394fe is not found in the rainbow table.
2. Apply the reduction function to the hash-value until a match is found in the rainbow table.

d2cbe65f53da8607e64173c1a83394fe → Abater → D48f58d9dc9af4b68b860e71f7336b44 → 10th → 515da2caf582ac4801cbb5d876c73c90.

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain.

User enter d2cbe65f53da8607e64173c1a83394fe.

3. Starting with the password TWA a search is done. After 4 reductions are done, the hash-value d2cbe65f53da8607e64173c1a83394fe is still not found in the rainbow table.
4. Using the next chain starting with the password sun, a search is done. Similarly, after 4 reductions, the hash-value d2cbe65f53da8607e64173c1a83394fe is still cannot be found.

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain.
User enter d2cbe65f53da8607e64173c1a83394fe.

3. Starting with the password TWA a search is done. After 4 reductions are done, the hash-value d2cbe65f53da8607e64173c1a83394fe is still not found in the rainbow table.
4. Using the next chain starting with the password sun, a search is done. Similarly, after 4 reductions, the hash-value d2cbe65f53da8607e64173c1a83394fe is still cannot be found.

A successful search of a password in a chain that involve collision.

Explanation:

- Does this mean we cannot find the pre-image for the hashed value d2cbe65f53da8607e64173c1a83394fe?
- When do we stop searching and conclude that the pre-image of a hashed value cannot be found?

A successful search of a password in a chain that involve collision.

Explanation:

- Notice that when we checked which chain list the pre-image was likely in, we did only two times of reduction function. This means that there are three more hashed values may be appearing at the end of three other chain lists.

A successful search of a password in a chain that involve collision.

Explanation:

- If we continue with the earlier check, we have …

d2cbe65f53da8607e64173c1a83394fe → Abater → D48f58d9dc9af4b68b860e71f7336b44 → 10th → 515da2caf582ac4801cbb5d876c73c90 → insect → dce41a93f7edb175dfc59a4d52105847.

- Another two chain lists that end with the hashed value dce41a93f7edb175dfc59a4d52105847 are found, they are Aaron - dce41a93f7edb175dfc59a4d52105847 and freehold - dce41a93f7edb175dfc59a4d52105847.

A successful search of a password in a chain that involve collision.

Explanation:

- Doing the same search process with the chain lists Aaron - dce41a93f7edb175dfc59a4d52105847, and we still cannot find the pre-image.
- However, the search for the pre-image succeed with the chain list freehold - dce41a93f7edb175dfc59a4d52105847.

Sno	Password	Hashed Value	Reduction Function
1	10th	515da2caf582ac4801cbb5d876c73c90	14
2	Ababa	bbf12b95db10da96472e2e019ffa4659	6
3	TWA	47221236d3df2a4cca11b1d7512faf7d	13
4	Abater	d48f58d9dc9af4b68b860e71f7336b44	1
5	Aaron	1c0a11cc4ddc0dbd3fa4d77232a4e22e	11
6	mundane	147e19efcaca65ee9f16ac703514b374	6
7	bake	a6ecfad3e0f9a51c6335848449a91bed	9
8	zoo	d2cbe65f53da8607e64173c1a83394fe	4
9	zombie	0eda241fc65ccf35d9743309ac395215	6
10	freehold	47ebf781047c3340fd5b0363b10c82aa	8
11	abalone	6e1ba55b046f7d62bbd6dc33b63d5ec7	4
12	sun	ebd556e6dfc99dbed29675ce1c6c68e5	15
13	heel	649be85da19882e6335962b2842385ea	11
14	insect	dce41a93f7edb175dfc59a4d52105847	7
15	prosecute	c18ac77dbe4b7211c616667e4f8fc526	11

10th	147e19efcaca65ee9f16ac703514b374
Ababa	147e19efcaca65ee9f16ac703514b374
TWA	515da2caf582ac4801cbb5d876c73c90
sun	515da2caf582ac4801cbb5d876c73c90
zoo	a6ecfad3e0f9a51c6335848449a91bed
Aaron	dce41a93f7edb175dfc59a4d52105847
freehold	dce41a93f7edb175dfc59a4d52105847

Example: Successful search of a password in a chain.
User enter d2cbe65f53da8607e64173c1a83394fe.

1. Starting with the password freehold a search is done. After one reduction is done, the hash-value d2cbe65f53da8607e64173c1a83394fe is found.
2. The password (preimage of the hash-value d2cbe65f53da8607e64173c1a83394fe) is **zoo**.