CSCI 331:
Introduction to Computer Security

Lecture 9: Password Cracking, part 3

Instructor: Dan Barowy

Williams

Announcements

- TA applications open tomorrow; due by Oct 29.
- TA feedback survey Oct 17.
- Pfizer booster now available in MA.

Topics

Paper reviews

Discussion

Generating PCHC chains

Generating Rainbow chains

Your to-dos

1. Lab 3 part 1, **due Sunday 10/10**.
2. Reading response (Aleph One), **due Wed 10/13**.
3. Lab 3 part 2, **due Sunday 10/17**.
4. Midterm exam: **in class, Thursday, Oct 21**

Final project: you can have a partner

Reminder, who you spoke with

Partner 1	Partner 2	Partner 3
Wael Baalbaki	Whit Jackson	
Maddie Burbage	Atlas Yilmaz	
Diego Esparza	Meghan Halloran	
Jihong Lee	Noah Andrew	
Chrispine Lwekaza	Paul Lapey	Alex Joshua
Ashton Voehl	Hugo Hua	
Karol Regula	Garret Tok Ern Liang	
Nick Hollon	Lucas Tolley	
Jackson Ehrenworth	Petros Markopoulos	
Brian Ha	Lauren Fossel	Nick Gonzalez
Carter Melnick	Henry McGrew	Kirun Cheung
Christopher Liu	Clara Lee	

Get in touch if you want to partner with that person

Contact me if you want help finding a partner

Project Activity

Think about how your conversation affected your thoughts on your project ideas.

Write down 2-3 concrete “next steps.”
Take 2 minutes.

Suggestions:

- How you can improve writing.
- Additional background research.
- How to do a proof-of-concept.
- Resources you might need…

Why do we do paper reviews?

Question

Can a precomputed hash chain **decrypt all hashes**?

Hugo’s question:
“If we **enumerate** all keys, don’t we have **duplication** in our table?”

Lab 3

`hdestroy(3)`; annoying inconsistency in behavior

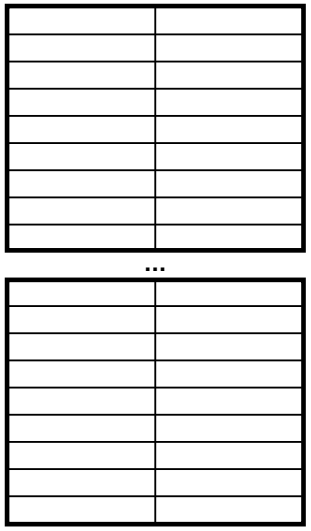
Generating chains.

Searching chains.

Generating Hash Chains with a Fixed Reducer

Example of length 4.

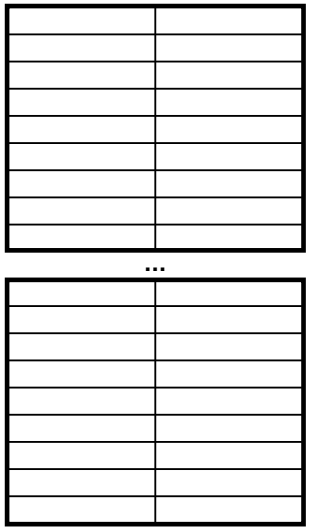
dict



genPlaintext(i) hash(p) reduce(c)

start: null
end: null

dict



genPlaintext(i) hash(p) reduce(c)

start: null
end: null

0000 ← genPlaintext(0)

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: null

0000 ← genPlaintext(0)

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: 0000

0000 ← genPlaintext(0)

0000

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: 0000

0000 ← genPlaintext(0)

0000

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: 0000

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

0000

dict

end	start	genPlaintext(i)	hash(p)	reduce(c)

start: 0000
end: 0000

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)

...

0000

dict

end	start	genPlaintext(i)	hash(p)	reduce(c)

start: 0000
end: 4A7D

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)

...

r(h(p))
0000 → 4A7D

dict

end	start	genPlaintext(i)	hash(p)	reduce(c)

start: 0000
end: 4A7D

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)

...

r(h(p))
0000 → 4A7D

dict

end	start	genPlaintext(i)	hash(p)	reduce(c)

start: 0000
end: 4A7D

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)

DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)

...

0000 —r(h(p))→ 4A7D

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: 4A7D

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)

0000 —r(h(p))→ 4A7D

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: DD75

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)

0000 —r(h(p))→ 4A7D —r(h(p))→ DD75

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c)

start: 0000
end: DD75

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)

0000 —r(h(p))→ 4A7D —r(h(p))→ DD75

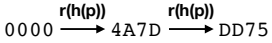
HashMap<String,String> dict

end	start
...	

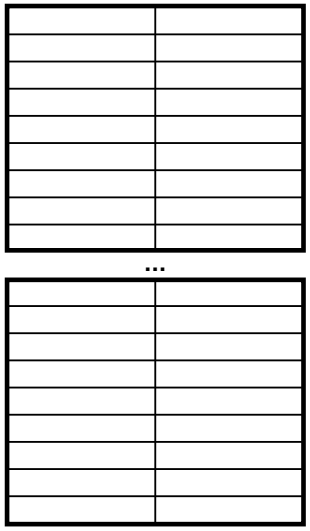
genPlaintext(i) hash(p) reduce(c)

start: 0000
end: DD75

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)



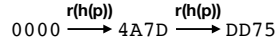
HashMap<String,String> dict



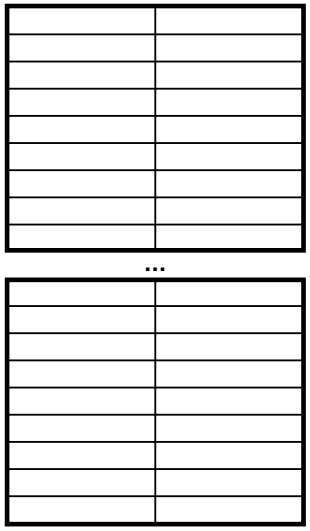
genPlaintext(i) hash(p) reduce(c)

start: 0000
end: DD75

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)



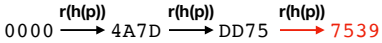
dict



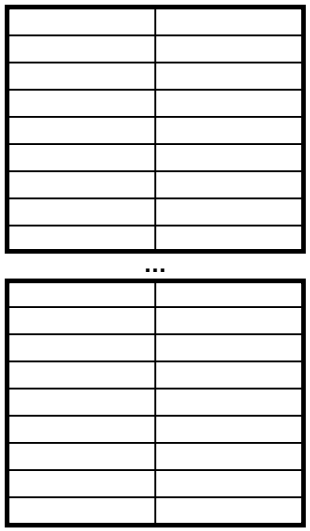
genPlaintext(i) hash(p) reduce(c)

start: 0000
end: 7539

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)



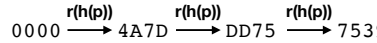
dict



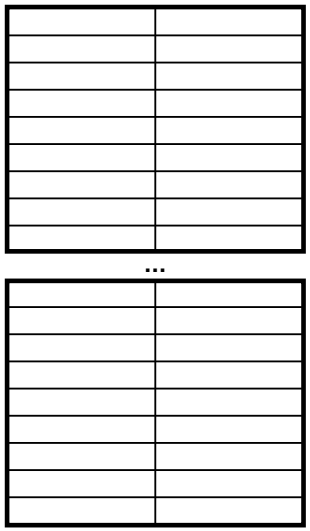
genPlaintext(i) hash(p) reduce(c)

start: 0000
end: 7539

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)



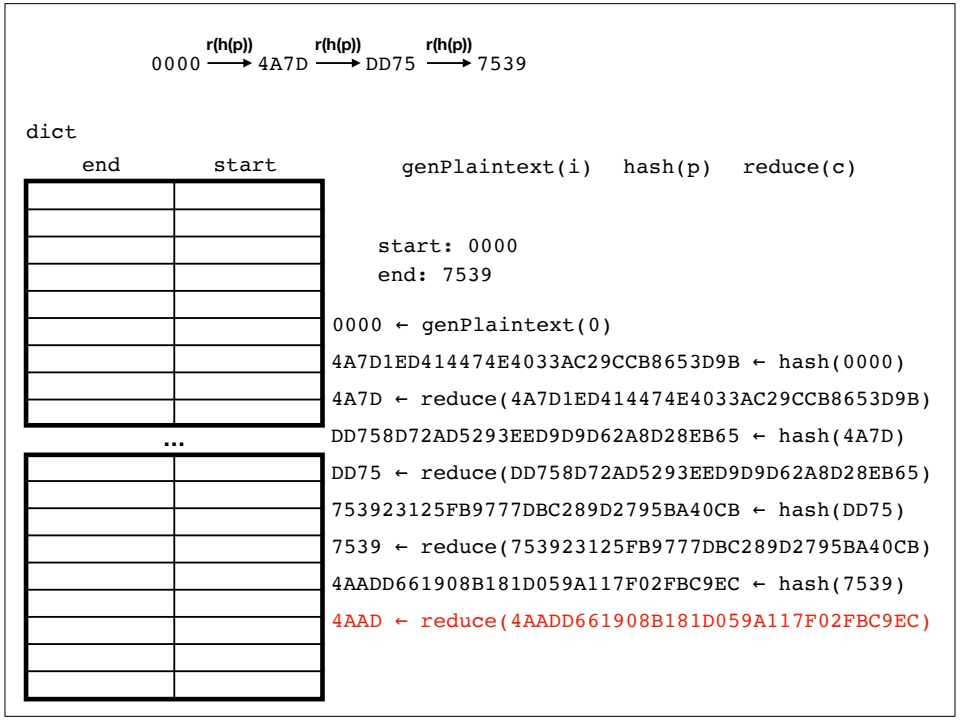
dict

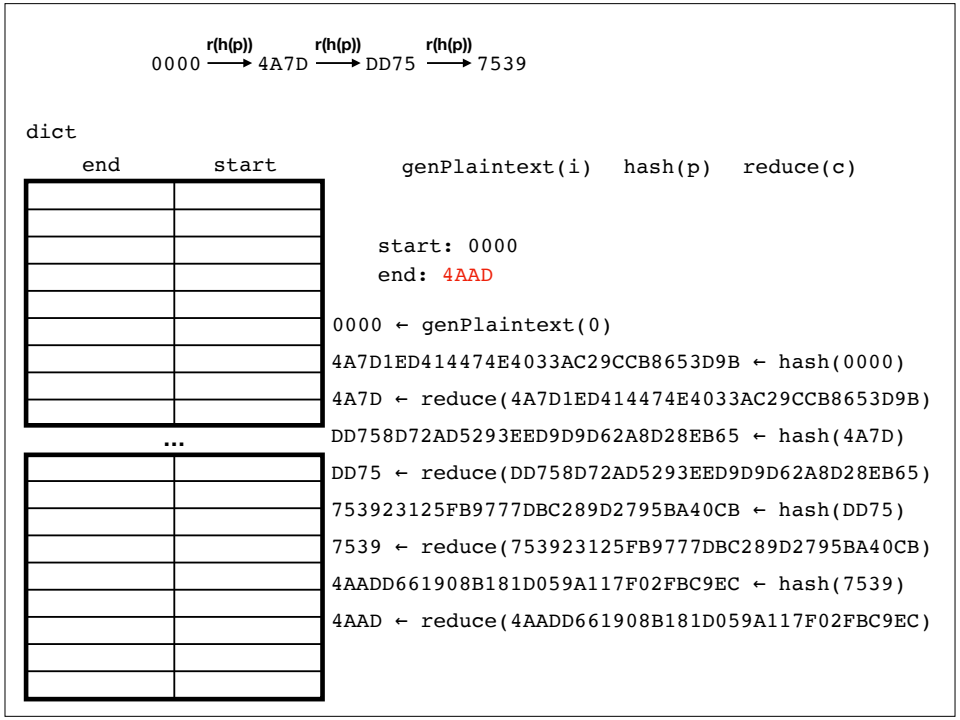


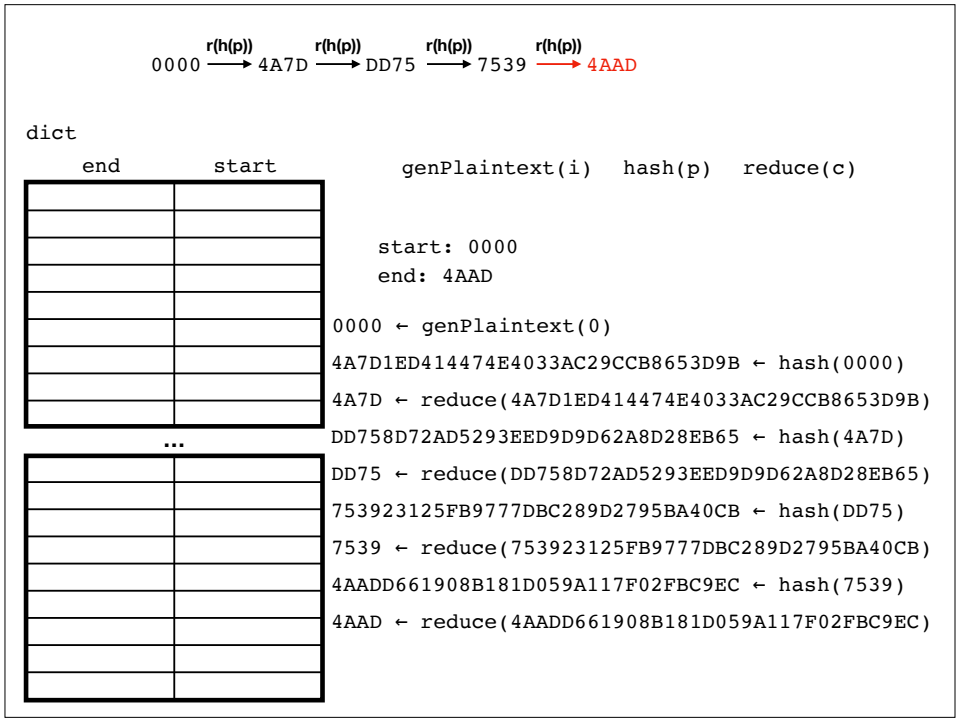
genPlaintext(i) hash(p) reduce(c)

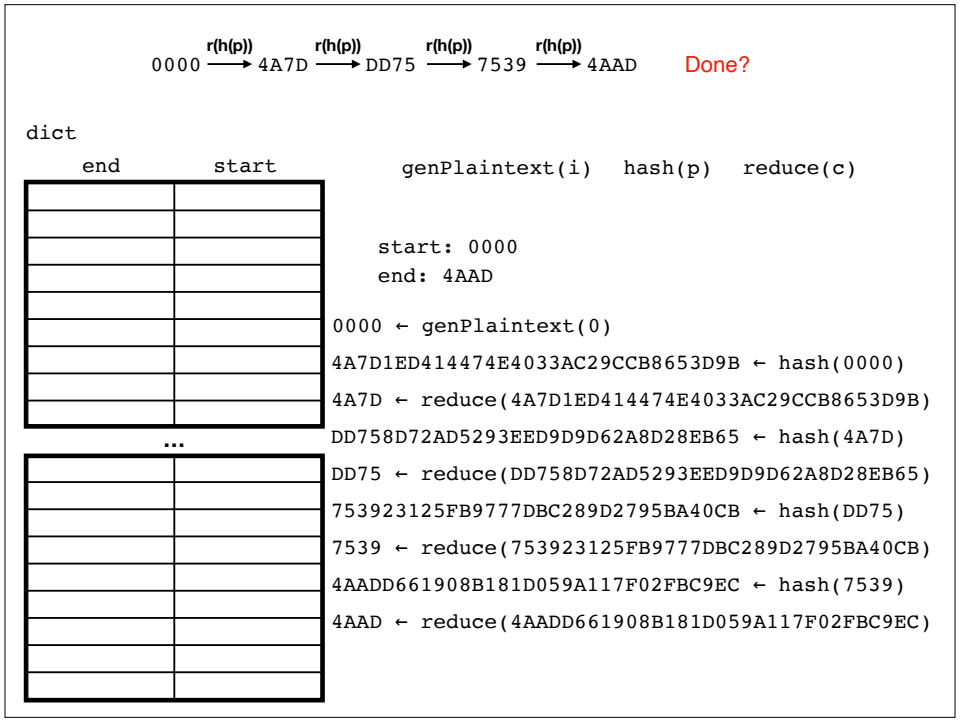
start: 0000
end: 7539

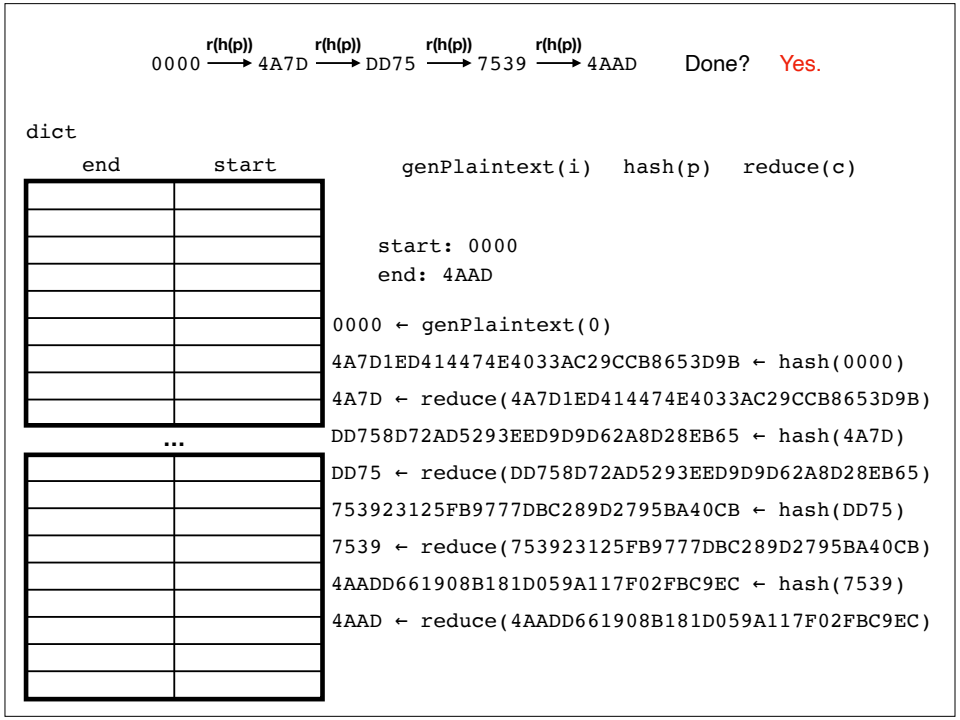
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)

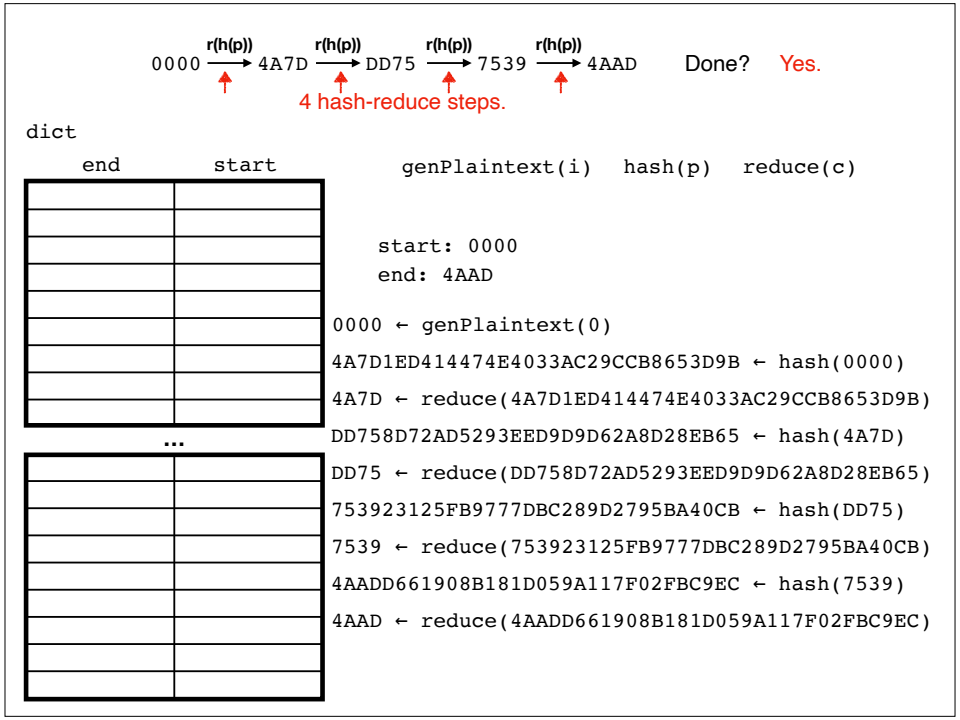

0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
start: 0000
end: 7539
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)
...

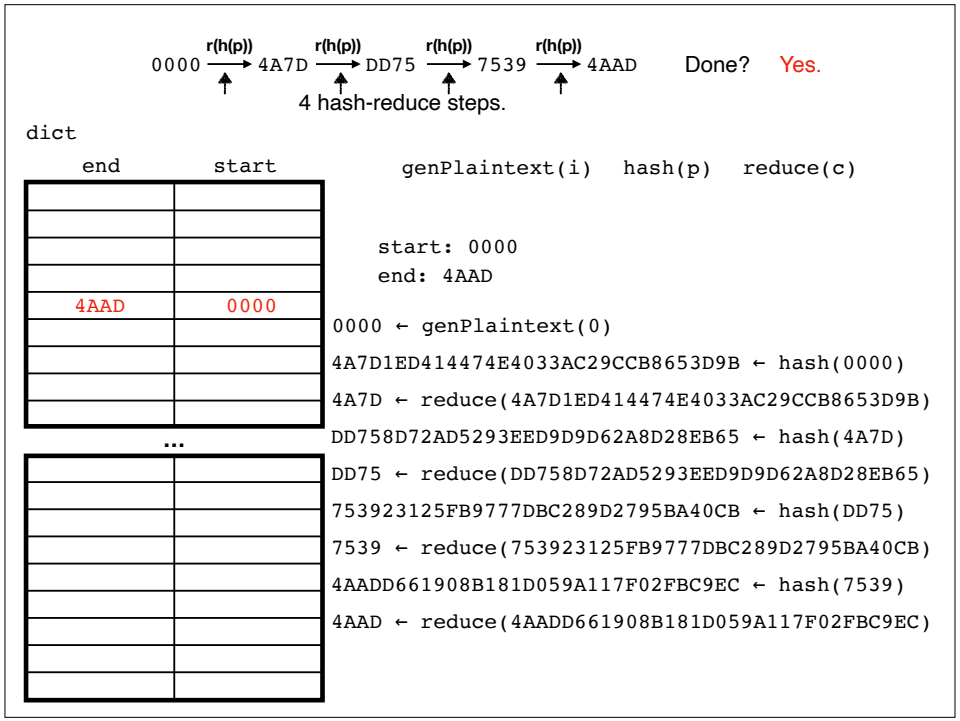

0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
start: 0000
end: 4AAD
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)
...

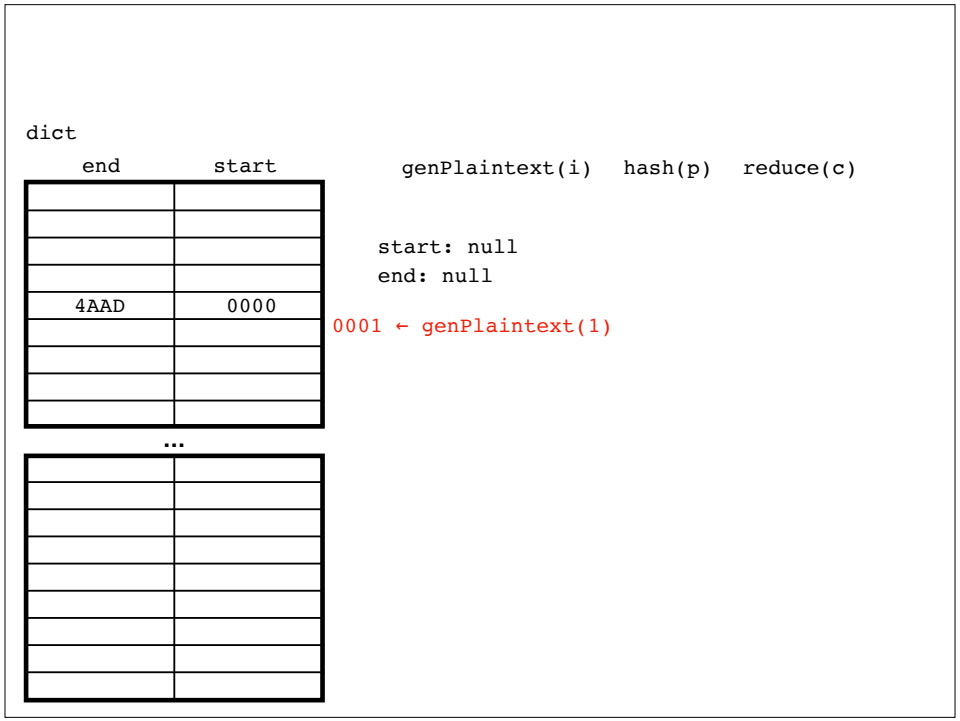

0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539 r(h(p)) 4AAD
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
start: 0000
end: 4AAD
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)
...


0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539 r(h(p)) 4AAD
Done?
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
start: 0000
end: 4AAD
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)
...


0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539 r(h(p)) 4AAD
Done? Yes.
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
...
start: 0000
end: 4AAD
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)


0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539 r(h(p)) 4AAD
Done? Yes.
4 hash-reduce steps.
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
...
start: 0000
end: 4AAD
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)


0000 r(h(p)) 4A7D r(h(p)) DD75 r(h(p)) 7539 r(h(p)) 4AAD
Done? Yes.
4 hash-reduce steps.
dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
4AAD
0000
...
start: 0000
end: 4AAD
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
DD75 ← reduce(DD758D72AD5293EED9D9D62A8D28EB65)
753923125FB9777DBC289D2795BA40CB ← hash(DD75)
7539 ← reduce(753923125FB9777DBC289D2795BA40CB)
4AADD661908B181D059A117F02FBC9EC ← hash(7539)
4AAD ← reduce(4AADD661908B181D059A117F02FBC9EC)


dict
end
start
genPlaintext(i)
hash(p)
reduce(c)
4AAD
0000
...
start: null
end: null
0001 ← genPlaintext(1)

dict

end	start
4AAD	0000
...	

genPlaintext(i) hash(p) reduce(c)

start: 0001
end: null

0001 ← genPlaintext(1)

dict

end	start
4AAD	0000
...	

genPlaintext(i) hash(p) reduce(c)

start: 0001
end: 0001

0001 ← genPlaintext(1)

0001

dict

end	start
4AAD	0000
...	

genPlaintext(i) hash(p) reduce(c)

start: 0001
end: 0001

0001 ← genPlaintext(1)

0001

dict

end	start
4AAD	0000
...	

genPlaintext(i) hash(p) reduce(c)

start: 0001
end: 0001

0001 ← genPlaintext(1)

And so on…

Rainbow Tables

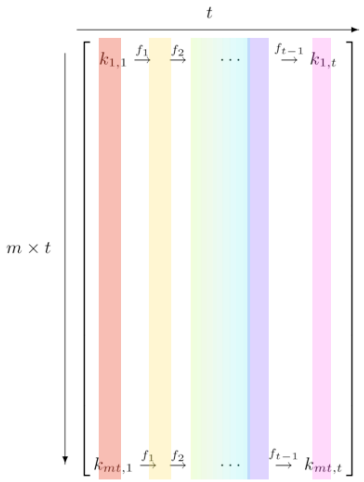
Why “rainbow table”?

Rainbow tables are a tiny modification to PCHC tables:
The reducer function **changes at each link i in the chain**.

Let $f(p, i) = \text{reduce}_i(\text{hash}(p))$

It’s like a “rainbow” of reducer functions.

Why “rainbow table”?



How would we modify our PCHC generation code for rainbow tables?

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: null
end: null

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: null
end: null

0000 ← genPlaintext(0)

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: 0000
end: null

0000 ← genPlaintext(0)

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: 0000
end: 0000

0000 ← genPlaintext(0)

0000

dict

end	start
...	

genPlaintext(i)

length: 4
start: 0000
end: 0000

0000 ← genPlaintext(0)

hash(p)

reduce(c,k)

0000

dict

end	start
...	

genPlaintext(i)

length: 4
start: 0000
end: 0000

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

hash(p)

reduce(c,k)

0000

dict

end	start
...	

genPlaintext(i)

length: 4
start: 0000
end: 0000

0000 ← genPlaintext(0)

4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

4A7D ← reduce(4A7D1ED414…, 0)

hash(p)

reduce(c,k)

0000

dict

end	start
...	

genPlaintext(i)

length: 4
start: 0000
end: 4A7D

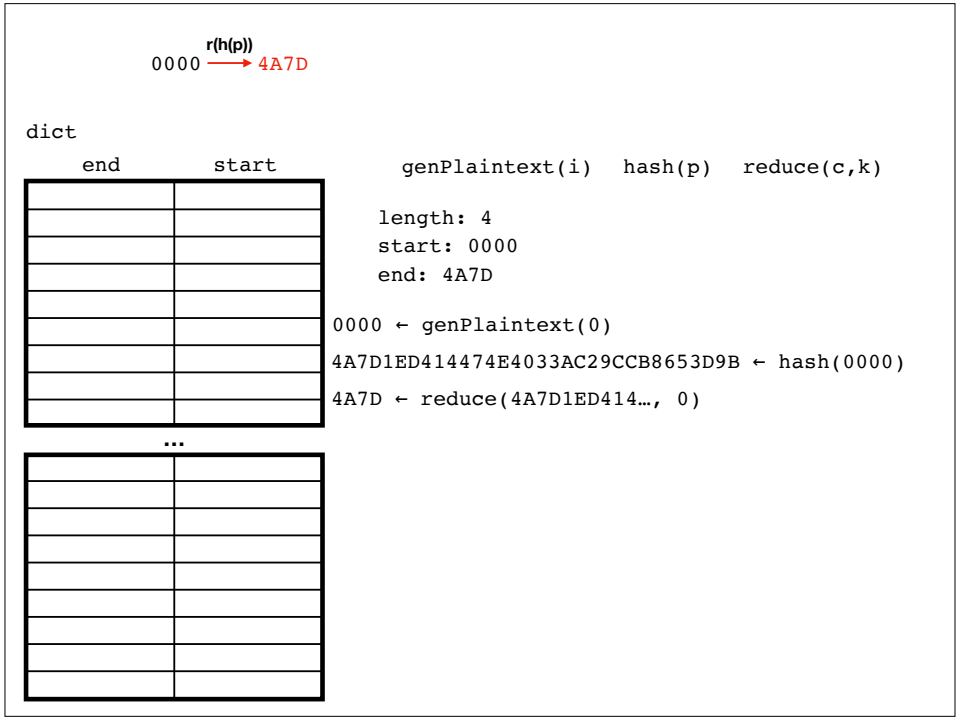
0000 ← genPlaintext(0)

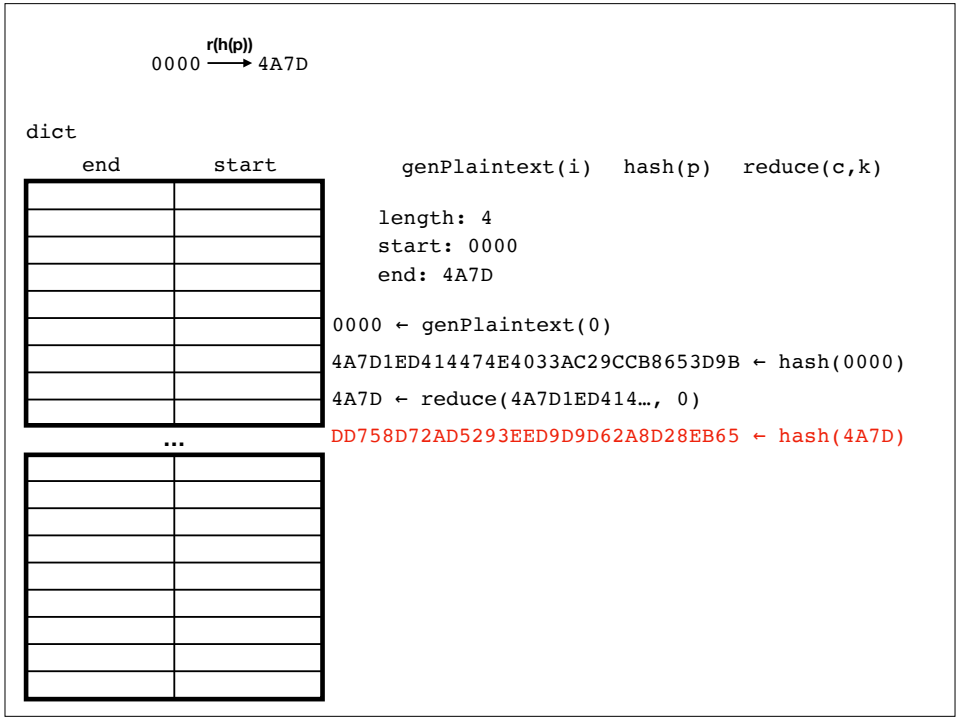
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)

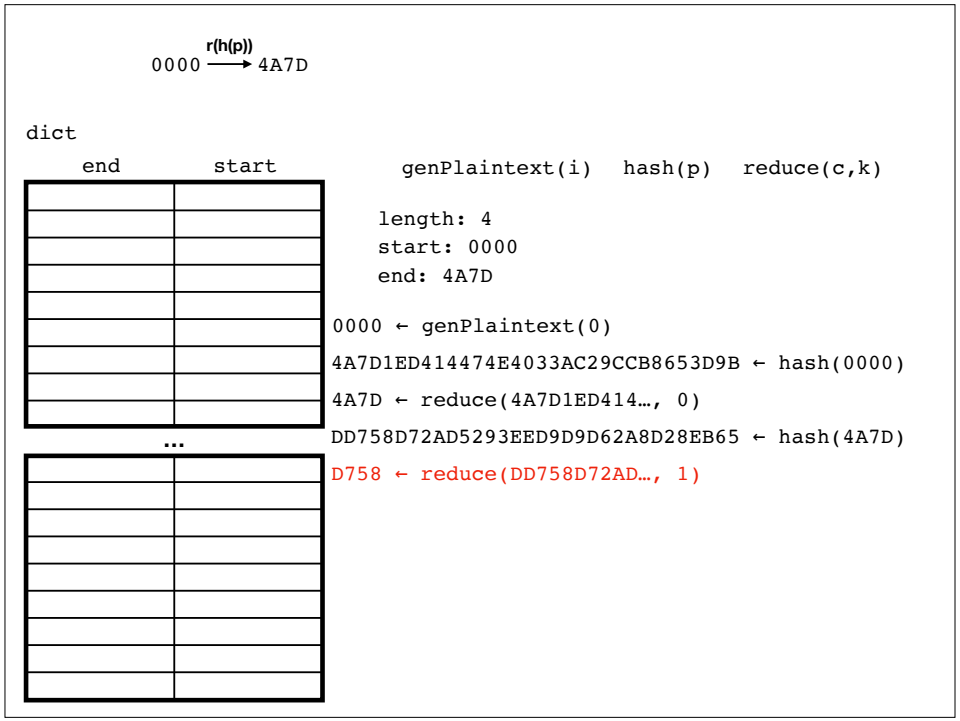
4A7D ← reduce(4A7D1ED414…, 0)

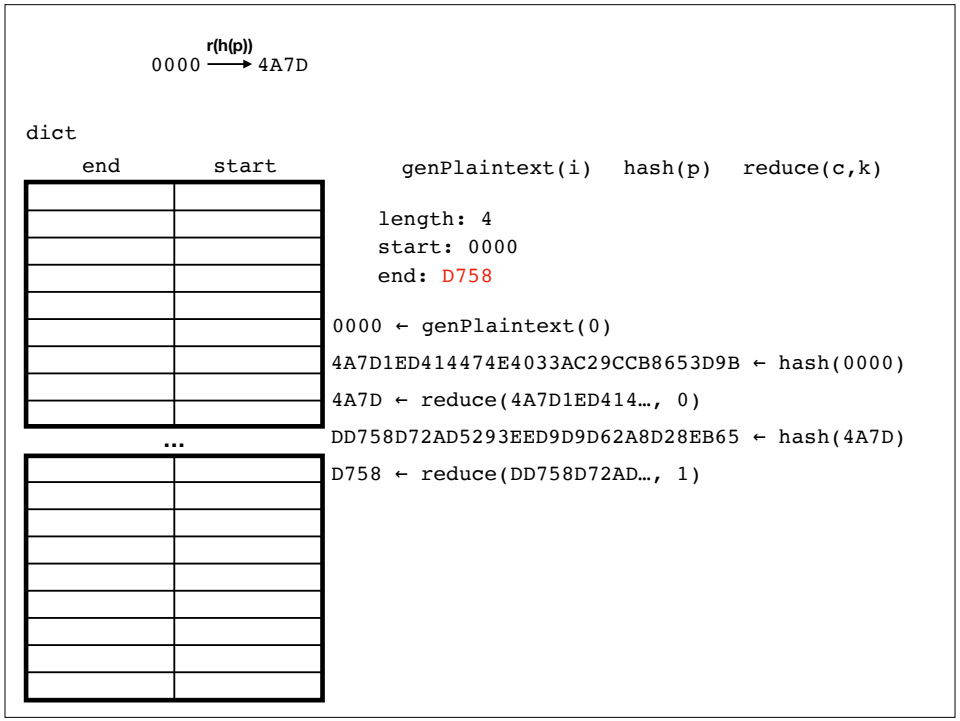
hash(p)

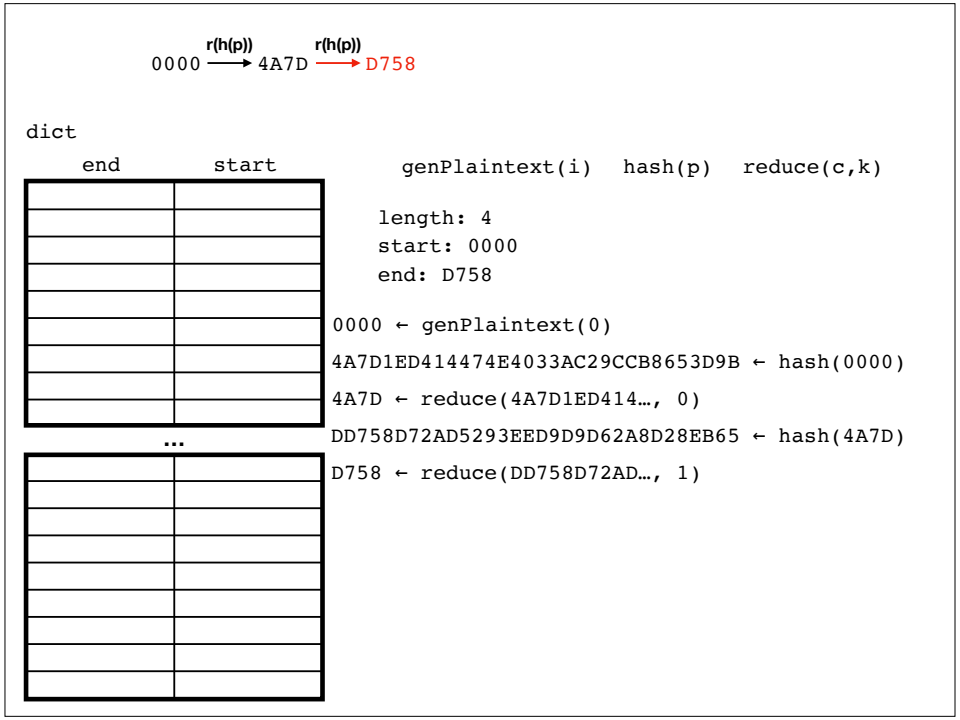
reduce(c,k)

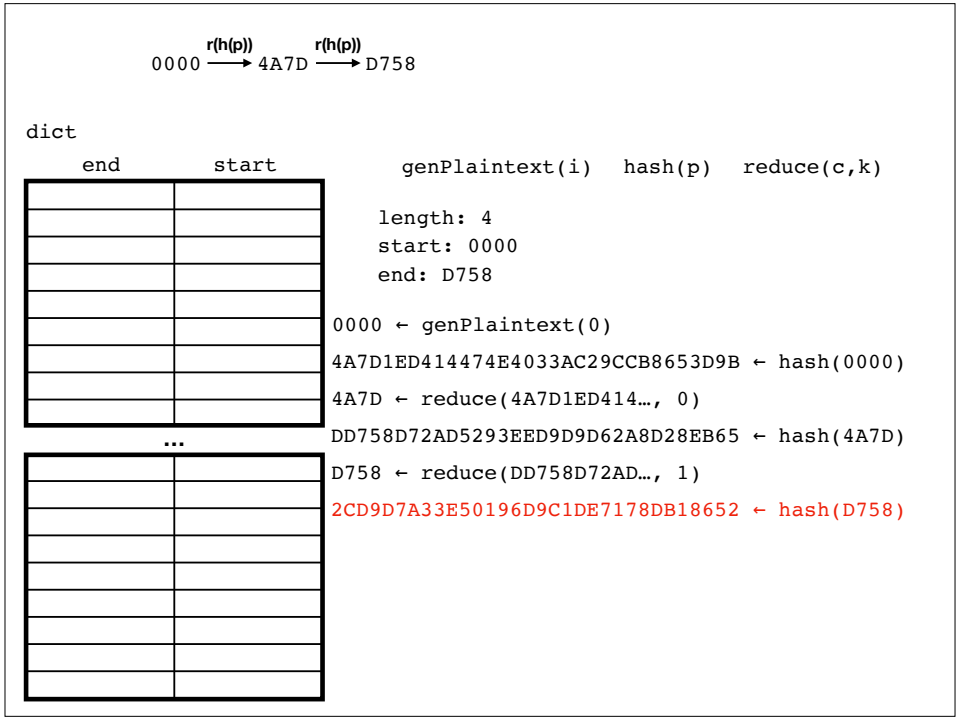

r(h(p))
0000
4A7D
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: 4A7D
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
…

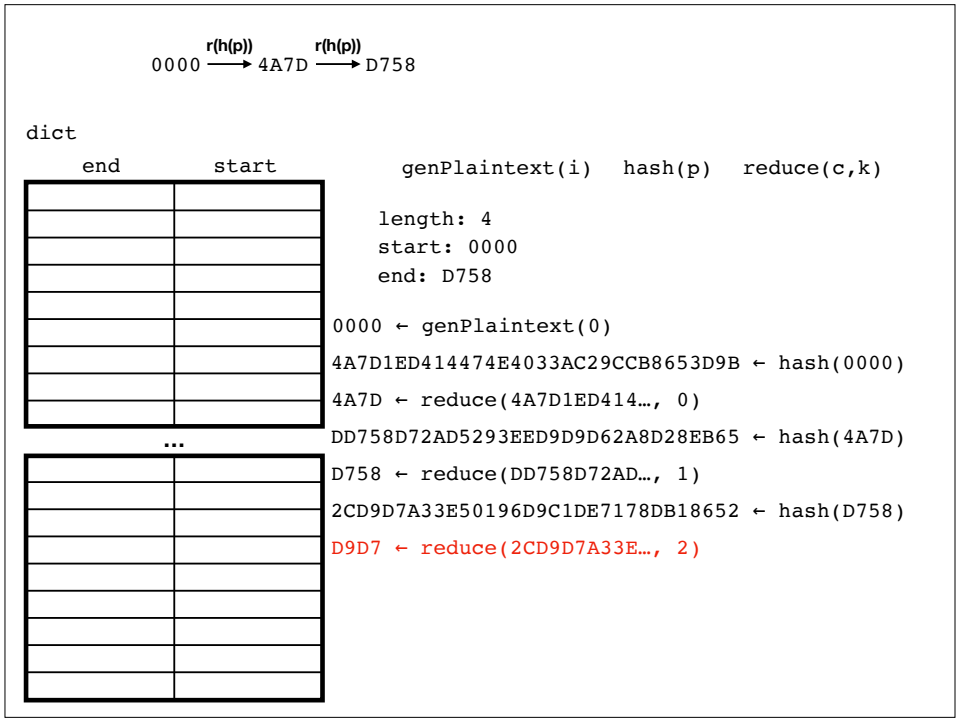

r(h(p))
0000
4A7D
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: 4A7D
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
…

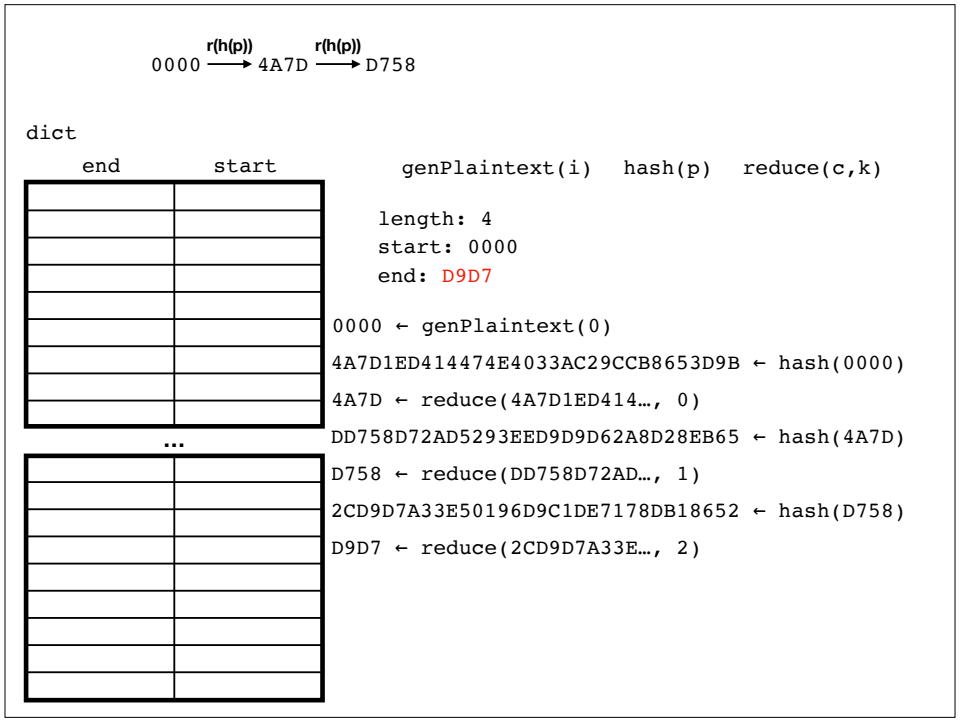

r(h(p))
0000
4A7D
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: 4A7D
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
…

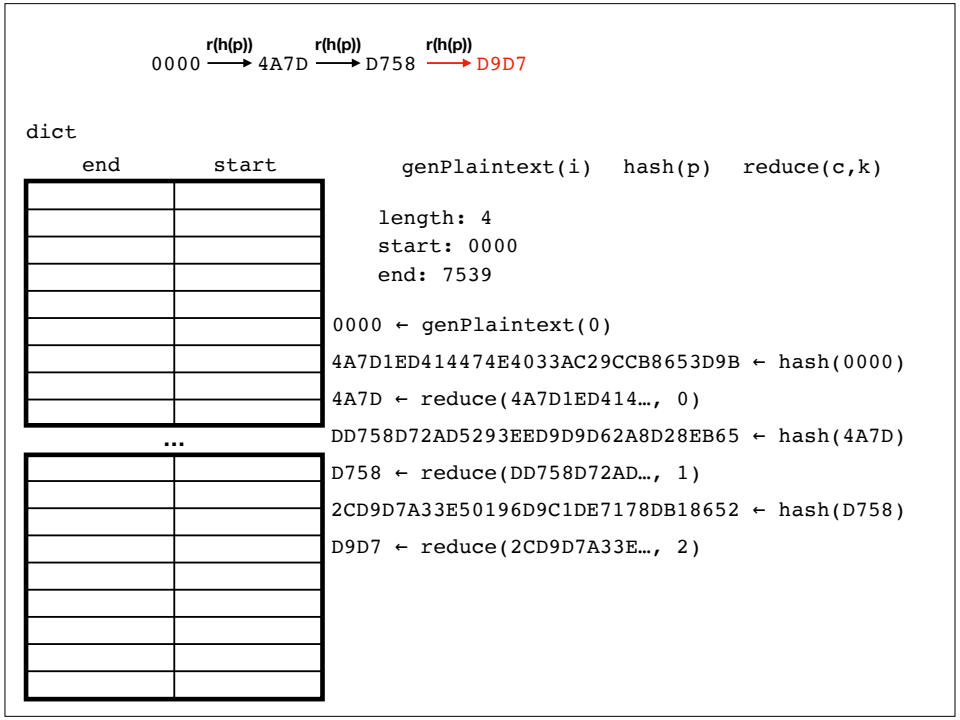

r(h(p))
0000
4A7D
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: D758
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
…

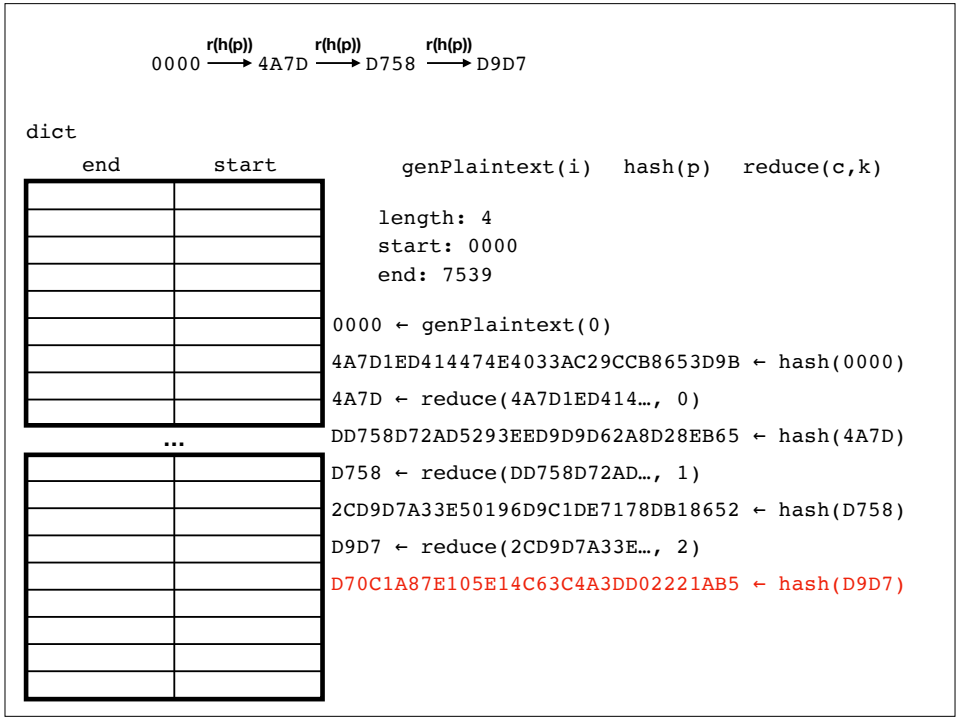

r(h(p))
r(h(p))
0000
4A7D
D758
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: D758
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
…

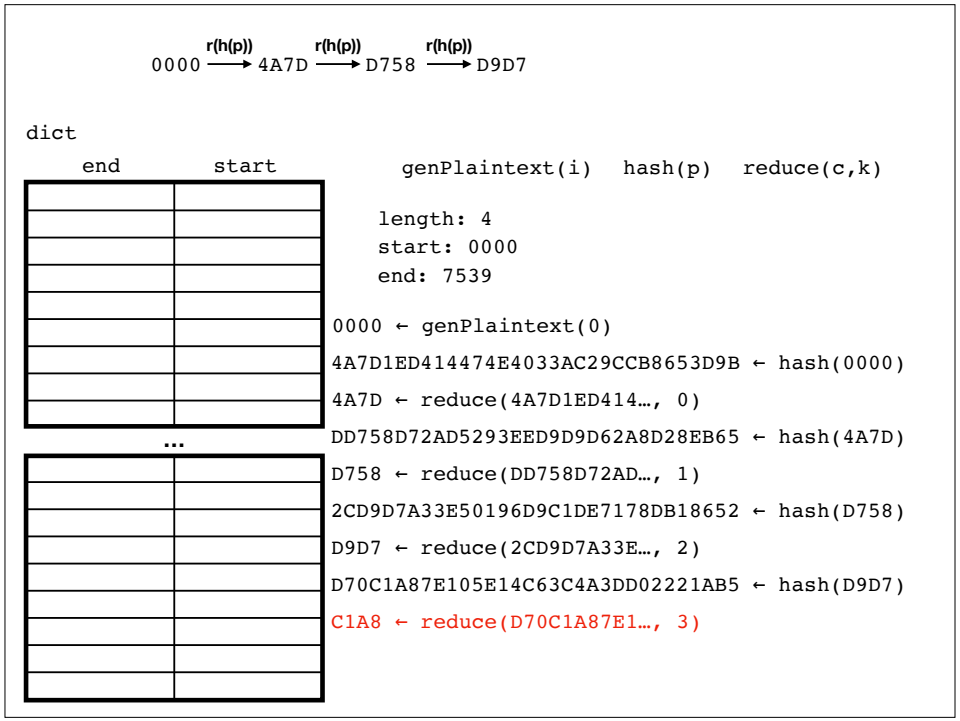

r(h(p))
r(h(p))
0000
4A7D
D758
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: D758
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
…

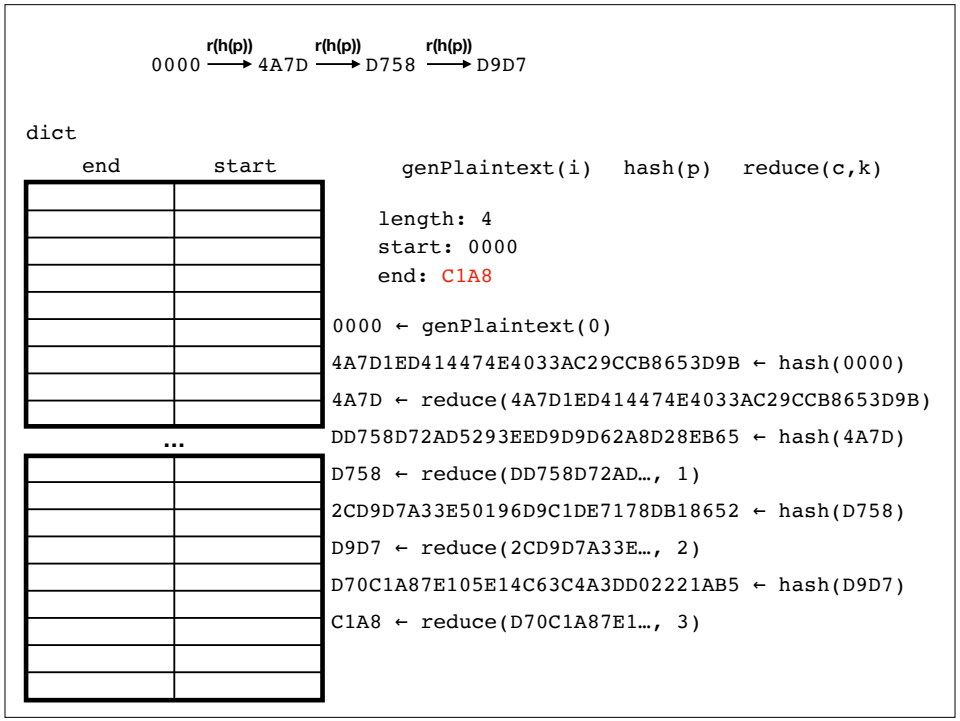

r(h(p))
r(h(p))
0000
4A7D
D758
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: D758
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
…


r(h(p))
r(h(p))
0000
4A7D
D758
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: D9D7
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
…


0000 r(h(p)) 4A7D r(h(p)) D758 r(h(p)) D9D7
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: 7539
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)


0000 r(h(p)) 4A7D r(h(p)) D758 r(h(p)) D9D7
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: 7539
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)


0000 r(h(p)) 4A7D r(h(p)) D758 r(h(p)) D9D7
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: 7539
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)


0000 r(h(p)) 4A7D r(h(p)) D758 r(h(p)) D9D7
dict
end
start
genPlaintext(i)
hash(p)
reduce(c,k)
length: 4
start: 0000
end: C1A8
0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414474E4033AC29CCB8653D9B)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)

0000 —r(h(p))→ 4A7D —r(h(p))→ D758 —r(h(p))→ D9D7 —r(h(p))→ C1A8

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: 0000
end: C1A8

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)

0000 —r(h(p))→ 4A7D —r(h(p))→ D758 —r(h(p))→ D9D7 —r(h(p))→ C1A8 Done?

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: 0000
end: C1A8

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)

0000 —r(h(p))→ 4A7D —r(h(p))→ D758 —r(h(p))→ D9D7 —r(h(p))→ C1A8 Done? Yes.

dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: 0000
end: C1A8

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)

0000 —r(h(p))→ 4A7D —r(h(p))→ D758 —r(h(p))→ D9D7 —r(h(p))→ C1A8 Done? Yes.

4 hash-reduce steps.

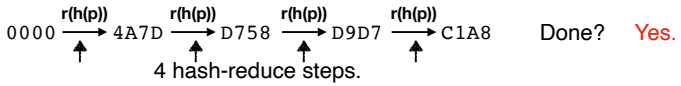
dict

end	start
...	

genPlaintext(i) hash(p) reduce(c,k)

length: 4
start: 0000
end: C1A8

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)



Done? Yes.

dict

end	start
C1A8	0000

...

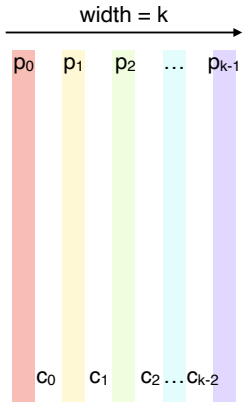
genPlaintext(i) hash(p) reduce(c,k)

```
length: 4
start: 0000
end: C1A8

0000 ← genPlaintext(0)
4A7D1ED414474E4033AC29CCB8653D9B ← hash(0000)
4A7D ← reduce(4A7D1ED414…, 0)
DD758D72AD5293EED9D9D62A8D28EB65 ← hash(4A7D)
D758 ← reduce(DD758D72AD…, 1)
2CD9D7A33E50196D9C1DE7178DB18652 ← hash(D758)
D9D7 ← reduce(2CD9D7A33E…, 2)
D70C1A87E105E14C63C4A3DD02221AB5 ← hash(D9D7)
C1A8 ← reduce(D70C1A87E1…, 3)
```

Think of a table search as two operations:

- Finding the column of the ciphertext.
- Finding the ciphertext within a row.



Recap & Next Class

Today we learned:

User choice in password schemes

PCHC generation

Rainbow table generation

Next class:

Classes of program bugs