

Decryption Activity

Handout 7
CSCI 331: Fall 2023

Precomputed Hash Chains

Is the hash 7F975A56C761DB6506ECA0B37CE6EC87 in the following **precomputed hash chain** table of **width 5**? If so, what is the plaintext? Use the supplied lookup tables. Plaintext characters are drawn from the domain {♥, ★}.

Precomputed hash chain table:

end	start
♥♥★♥	♥♥♥♥
♥★★★★	♥♥♥♥★
★♥★★	★★♥★
★★★★	♥★♥★

Hash function:

plaintext	hash of plaintext
♥♥♥♥	4A7D1ED414474E4033AC29CCB8653D9B
♥♥♥♥★	25BBD06C32D477F7FA1C3E4A91B032
♥♥★♥	FC1198178C3594BFDDA3CA2996EB65CB
♥♥★★	AE2BAC2E4B4DA805D01B2952D7E35BA4
♥★♥♥	DB2F40F24260BC41DB48D82D5E7ABF1D
♥★♥★	814F06AB7F40B2CFF77F2C7BDFFD3415
♥★★♥	2A66ACBC1C39026B5D70457BB71B142B
♥★★★	7D7C45B9A935CF9D845FC75679A41559
★♥♥♥	A9B7BA70783B617E9998DC4DD82EB3C5
★♥♥★	B8C37E33DEFDE51CF91E1E03E51657DA
★♥★♥	1E48C4420B7073BC11916C6C1DE226BB
★♥★★	7F975A56C761DB6506ECA0B37CE6EC87
★★♥♥	1E6E0A04D20F50967C64DAC2D639A577
★★♥★	C6BFF625BDB0393992C9D4DB0C6BBE45
★★★♥	2CBCA44843A864533EC05B321AE1F9D1
★★★★	B59C67BF196A4758191E42F76670CEBA

```
func reducer(c):
```

Convert the first hexadecimal digit of c into a plaintext using the following table:

hex digit	plaintext
0	♥♥♥♥♥
1	♥♥♥♥★
2	♥♥★♥♥
3	♥♥★★★
4	♥★♥♥♥
5	♥★♥★♥
6	♥★★♥♥
7	♥★★★★
8	★♥♥♥♥
9	★♥♥★♥
A	★♥★♥♥
B	★♥★★★
C	★★♥♥♥
D	★★♥★♥
E	★★★♥♥
F	★★★★★

1. Does the table contain a decryption? (circle one)

- Yes.
- No.

2. If **yes**, what is the original plaintext? _____