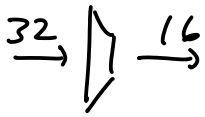
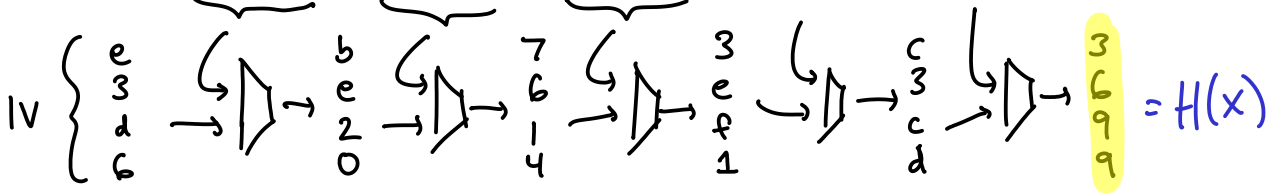
Merkle-Damgård Hashes

Ex: $h: \{0,1\}^{32} \to \{0,1\}^{16}$ (4 bytes → 2 bytes)
(8 nibbles → 4 nibbles)



x = c d 9 5 1 8 f 1 e c 7 2 5 7 (7 bytes)

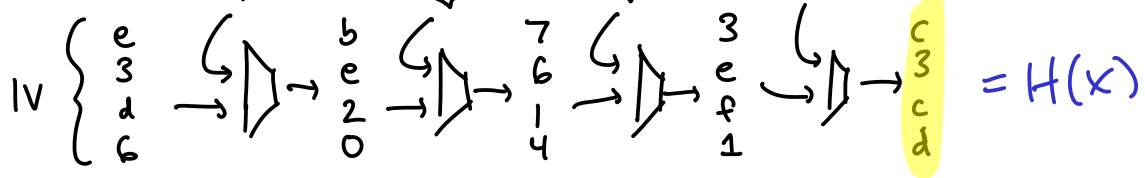
c d 9 5 | 1 8 f 1 | e c 7 2 | 5 7 0 0 | 0 0 0 7



Q: What happens if no length encoding?

x = c d 9 5 1 8 f 1 e c 7 2 5 7 (7 bytes)

c d 9 5 | 1 8 f 1 | e c 7 2 | 5 7 0 0



insecure picture

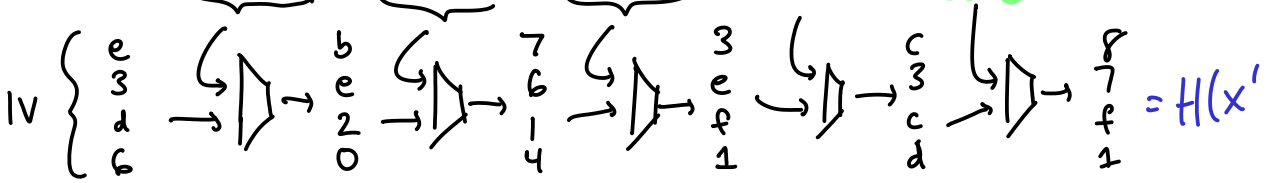
x' = c d 9 5 1 8 f 1 e c 7 2 5 7 0 0

also has same hash (collision!)

---

x' = c d 9 5 1 8 f 1 e c 7 2 5 7 0 0 (8 bytes)

c d 9 5 | 1 8 f 1 | e c 7 2 | 5 7 0 0 | 0 0 0 8



secure picture

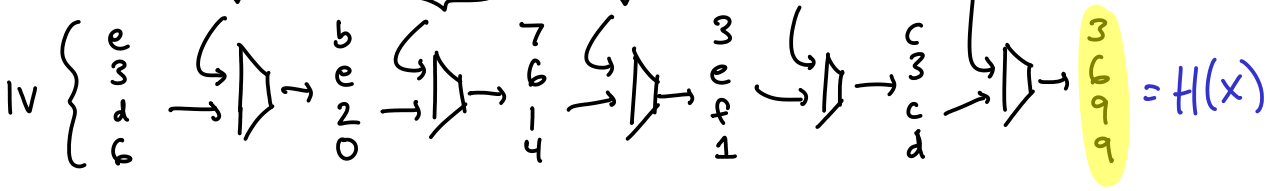
Length Extension Attack

$H(k \| m)$

observation:

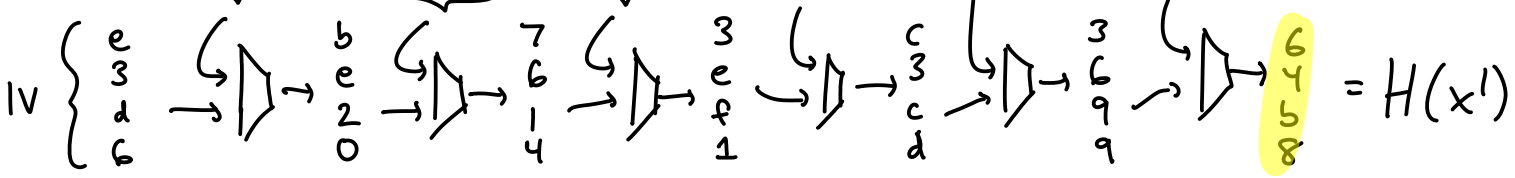
x = cd9518f1ec7257 (7 bytes)

cd95 | 18f1 | ec72 | 5700 | 0007



x' = cd9518f1ec72570000007 (10 bytes)

cd95 | 18f1 | ec72 | 5700 | 0007 | 000a



Bad Idea:

let's use $H(k \| m)$ as a MAC

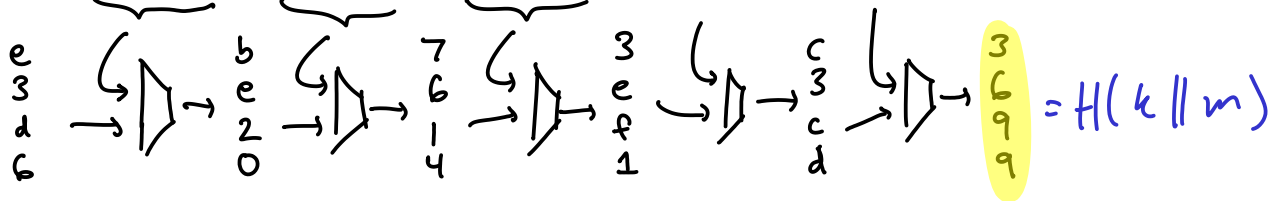
suppose Alice chooses k = cd9518f1

let's ask Alice for MAC of m = ec7257

Alice computes $H(k \| m)$:

k | m | Merkle-Damgård stuff

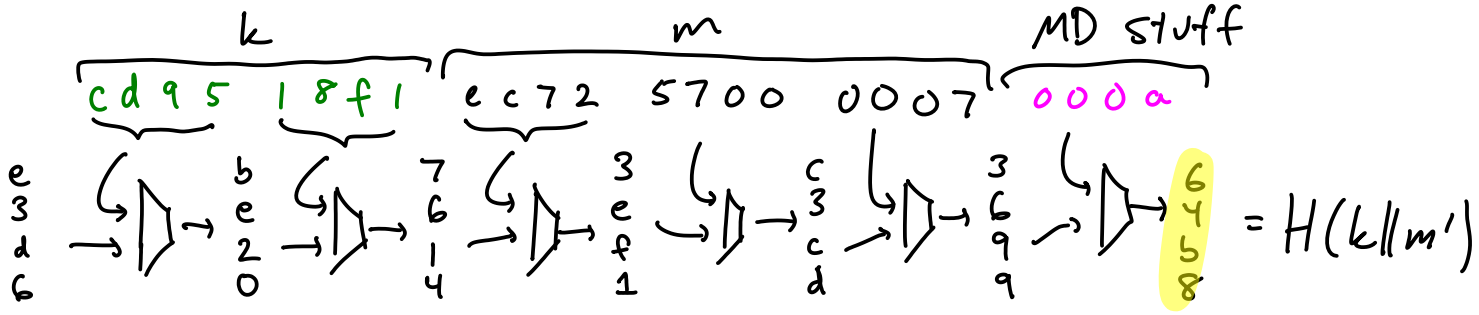
cd95 | 18f1 | ec72 | 5700 | 0007



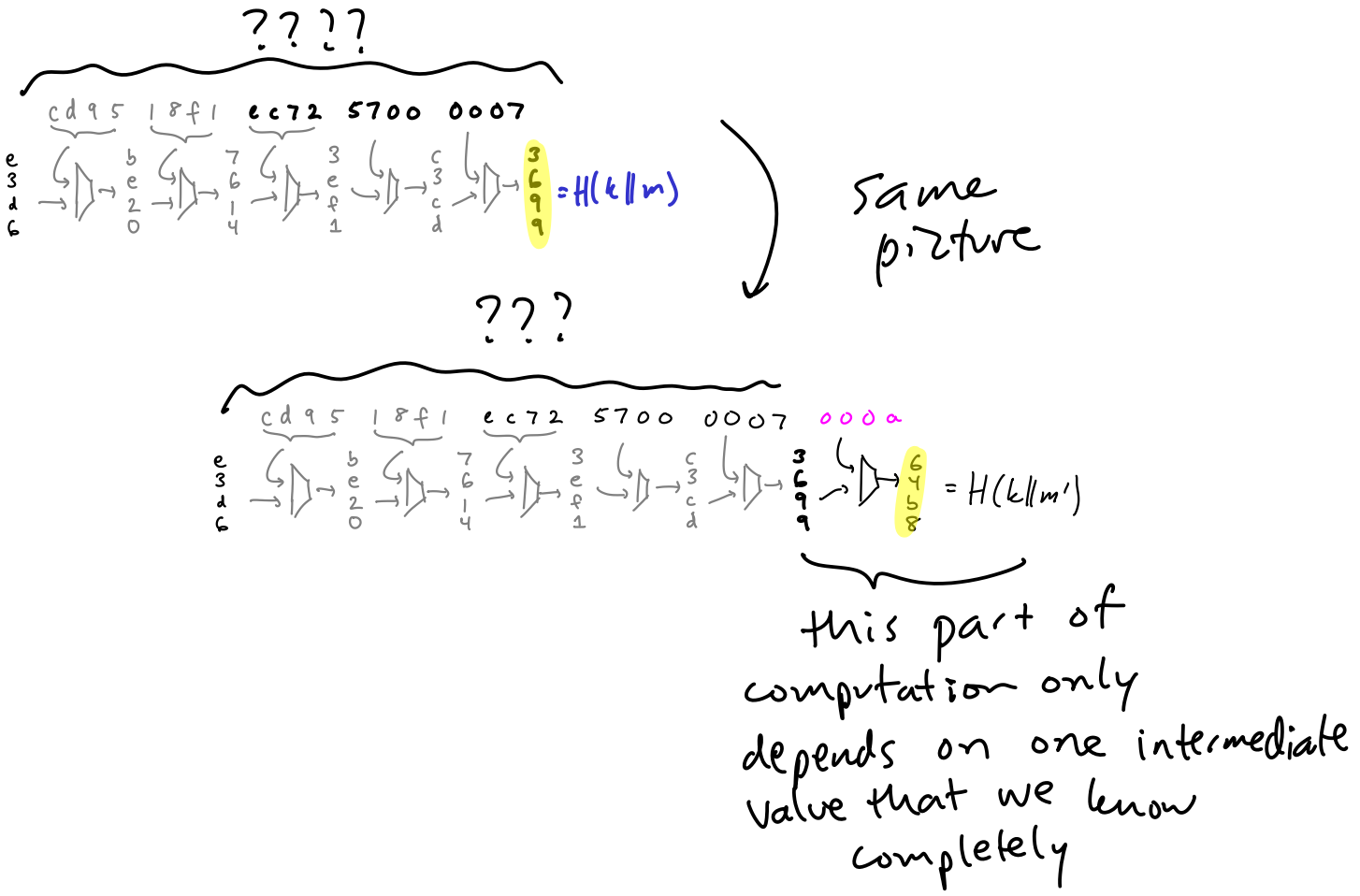
she responds 3699

We can now compute MAC of $m' = ec72\ 5700\ 0007$

What is the correct MAC of this m'?

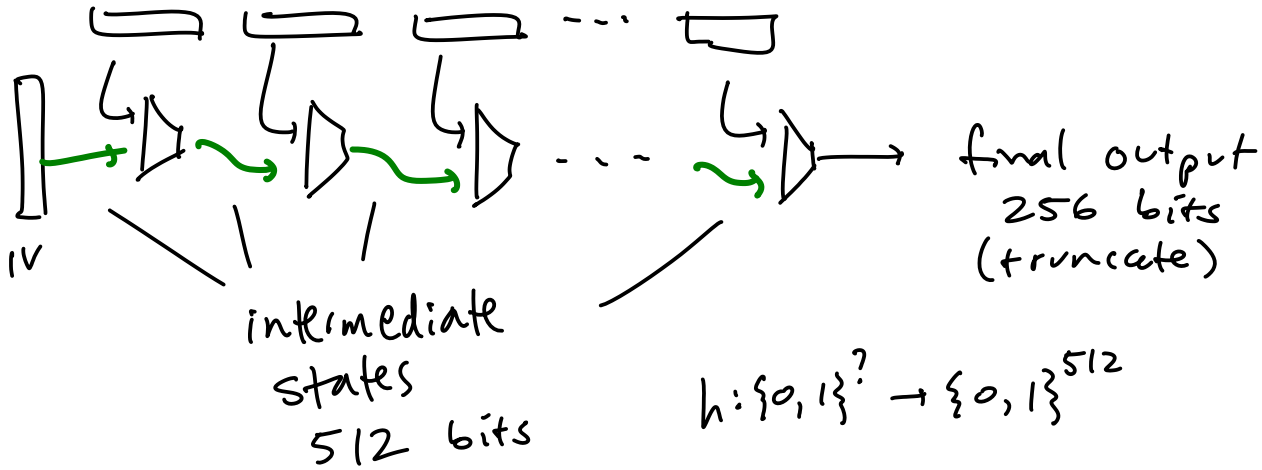


Our perspective:



Bonus thing:

can mitigate with wide-pipe paradigm



$h: \{0,1\}^? \to \{0,1\}^{512}$