TEST 1: Hash Functions

Question 2: Collisions [ID: 477160]

Let S_3 be the set of permutations on the set $\{1,2,3\}$. For each $\pi \in S_3$ let e_π be the corresponding bit permutation on B_3. For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathrm{x}) = e_\pi(\mathrm{x}) \oplus \mathrm{x}$ where $\mathrm{x} \in B_3$.

Question 2: Collisions [ID: 477160]

Let S_3 be the set of permutations on the set $\{1,2,3\}$. For each $\pi \in S_3$ let e_π be the corresponding bit permutation on B_3. For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathrm{x}) = e_\pi(\mathrm{x}) \oplus \mathrm{x}$ where $\mathrm{x} \in B_3$.

Question 2: Collisions [ID: 477160]

Let S_3 be the set of permutations on the set $\{1,2,3\}$. For each $\pi \in S_3$ let e_π be the corresponding bit permutation on B_3. For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathrm{x}) = e_\pi(\mathrm{x}) \oplus \mathrm{x}$ where $\mathrm{x} \in B_3$.

- $S_3 = \{123, 132, 213, 231, 312, 321\}$
- $\mid S_3 \mid = 3! = 1*2*3 = 6$

Question 2: Collisions [ID: 477160]

Let S_3 be the set of permutations on the set $\{1,2,3\}$. For each $\pi \in S_3$ let e_π be the corresponding bit permutation on B_3. For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathrm{x}) = e_\pi(\mathrm{x}) \oplus \mathrm{x}$ where $\mathrm{x} \in B_3$.

- $S_3 = \{123, 132, 213, 231, 312, 321\}$
- $\mid S_3 \mid = 3! = 1*2*3 = 6$

- $B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$
- $\mid B_3 \mid = 2^3 = 8$

Question 2: Collisions [ID: 477160]

Let S_3 be the set of permutations on the set $\{1,2,3\}$. For each $\pi \in S_3$ let e_π be the corresponding bit permutation on B_3. For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathrm{x}) = e_\pi(\mathrm{x}) \oplus \mathrm{x}$ where $\mathrm{x} \in B_3$.

- $S_3 = \{123, 132, 213, 231, 312, 321\}$
- $B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$

- $\pi = 213$ and $\mathrm{x} = 101$, $e_\pi(\mathrm{x}) = e_{(213)}(101) = 011$
- $h_\pi(\mathrm{x}) = e_\pi(\mathrm{x}) \oplus \mathrm{x}$: $e_{(213)}(101) \oplus 101 = 011 \oplus 101 = 110$

Question 2: Collisions [ID: 477160]

For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathsf{x}) = e_\pi(\mathsf{x}) \oplus \mathsf{x}$ where $\mathsf{x} \in B_3$.

- $B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (123)$

$h_{(123)}(\mathsf{x}) = e_{(123)}(\mathsf{x}) \oplus \mathsf{x}$

- $h_{(123)}(101) = e_{(123)}(101) \oplus 101 = 101 \oplus 101 = 000$

Question 2: Collisions [ID: 477160]

For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(\mathsf{x}) = e_\pi(\mathsf{x}) \oplus \mathsf{x}$ where $\mathsf{x} \in B_3$.

- $B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (123)$

$h_{(123)}(\mathsf{x}) = e_{(123)}(\mathsf{x}) \oplus \mathsf{x}$

- $h_{(123)}(101) = e_{(123)}(101) \oplus 101 = 101 \oplus 101 = 000$
- $h_{(123)}(110) = e_{(123)}(110) \oplus 110 = 110 \oplus 110 = 000$

Question 2: Collisions [ID: 477160]

For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(x) = e_\pi(x) \oplus x$ where $x \in B_3$.

- $B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (123)$

$h_{(123)}(x) = e_{(123)}(x) \oplus x$

- $h_{(123)}(101) = e_{(123)}(101) \oplus 101 = (101) \oplus (101) = 000$
- $h_{(123)}(110) = e_{(123)}(110) \oplus 110 = (110) \oplus (110) = 000$
- ...
- $h_{(123)}(001) = e_{(123)}(001) \oplus 001 = (001) \oplus (001) = 000$

Question 2: Collisions [ID: 477160]

$B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (123)$

- $h_{(123)}(101) = e_{(123)}(101) \oplus 101 = 101 \oplus 101 = 000$
- $h_{(123)}(110) = e_{(123)}(110) \oplus 110 = 110 \oplus 110 = 000$
- ...
- $h_{(123)}(001) = e_{(123)}(001) \oplus 001 = 001 \oplus 001 = 000$

The number of collisions:

A. 8

B. 12

C. 28

Question 2: Collisions [ID: 477160]

$B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (123)$

- $h_{(123)}(101) = e_{(123)}(101) \oplus 101 = (101) \oplus (101) = 000$
- $h_{(123)}(110) = e_{(123)}(110) \oplus 110 = (110) \oplus (110) = 000$
- ...
- $h_{(123)}(001) = e_{(123)}(001) \oplus 001 = (001) \oplus (001) = 000$

The number of collisions: ${C^2}_8 = (7*8)/2 = 28$

Question 2: Collisions [ID: 477160]

$B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (132)$

- $h_{(132)}(101) = e_{(132)}(101) \oplus 101 = 110 \oplus 101 = 011$
- $h_{(132)}(110) = e_{(132)}(110) \oplus 110 = 101 \oplus 101 = 011$
- $h_{(132)}(111) = e_{(132)}(111) \oplus 111 = 111 \oplus 111 = 000$
- $h_{(132)}(100) = e_{(132)}(100) \oplus 100 = 100 \oplus 100 = 000$
- $h_{(132)}(000) = e_{(132)}(000) \oplus 000 = 000 \oplus 000 = 000$
- $h_{(132)}(010) = e_{(132)}(010) \oplus 010 = 001 \oplus 010 = 011$
- $h_{(132)}(011) = e_{(132)}(011) \oplus 011 = 011 \oplus 011 = 000$
- $h_{(132)}(001) = e_{(132)}(001) \oplus 010 = 010 \oplus 101 = 011$

Question 2: Collisions [ID: 477160]

$B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$, $\pi = (132)$

- $h_{(132)}(101) = e_{(132)}(101) \oplus 101 = 110 \oplus 101 = 011$
- $h_{(132)}(110) = e_{(132)}(110) \oplus 110 = 101 \oplus 101 = 011$
- $h_{(132)}(111) = e_{(132)}(111) \oplus 111 = 111 \oplus 111 = 000$
- $h_{(132)}(100) = e_{(132)}(100) \oplus 100 = 100 \oplus 100 = 000$
- $h_{(132)}(000) = e_{(132)}(000) \oplus 000 = 000 \oplus 000 = 000$
- $h_{(132)}(010) = e_{(132)}(010) \oplus 010 = 001 \oplus 010 = 011$
- $h_{(132)}(011) = e_{(132)}(011) \oplus 011 = 011 \oplus 011 = 000$
- $h_{(132)}(001) = e_{(132)}(001) \oplus 010 = 010 \oplus 101 = 011$

The number of collisions: ${C^2}_4 + {C^2}_4 = 12$

Question 2: Collisions [ID: 477160]

$S_3 = \{123, 132, 213, 231, 312, 321\}$
$B_3 = \{101, 110, 111, 100, 000, 010, 011, 001\}$

- $\pi = 213$: 12
- $\pi = 231$: $4{*}{C^2}_2 = 4$
- $\pi = 312$: 4
- $\pi = 321$: 12

Question 3: Hash function collisions

Consider the hash function h: $B^* \to B^*$ given by
k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
where a bitstring k is identified with the natural number represented by k and r $\mod 1 =$ r - $\lfloor$ r $\rfloor$, for a positive real number r. Moreover, images are padded by leading zeroes to the maximal possible length of all images of h.

- Determine the maximal length in bits of the images.
- Give a collision of this hash function.

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

$r \mod 1 = r - \lfloor r \rfloor$

Example k = 1

$h(1) = \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

Example k = 1

h(1) $= \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(((1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 \mod 1) \rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

Example k = 1

$h(1) = \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(((1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 - \lfloor 1.61803398875 \rfloor) \rfloor$

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
$r \mod 1 = r - \lfloor r \rfloor$

Example k = 1

$h(1) = \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(((1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 - \lfloor 1.61803398875 \rfloor) \rfloor$
$= \lfloor 10000(1.61803398875 - 1) \rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

Example k = 1

$h(1) = \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(((1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 - \lfloor 1.61803398875 \rfloor) \rfloor$
$= \lfloor 10000(1.61803398875 - 1) \rfloor$
$= \lfloor 10000(0.61803398875) \rfloor$

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

$r \mod 1 = r - \lfloor r \rfloor$

Example k = 1

$h(1) = \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$

$= \lfloor 10000(((1+\sqrt{5})/2) \mod 1) \rfloor$

$= \lfloor 10000(1.61803398875 \mod 1) \rfloor$

$= \lfloor 10000(1.61803398875 - \lfloor 1.61803398875 \rfloor) \rfloor$

$= \lfloor 10000(1.61803398875 - 1) \rfloor$

$= \lfloor 10000(0.61803398875) \rfloor$

$= \lfloor 6180.3398875 \rfloor = 6180$

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

$r \mod 1 = r - \lfloor r \rfloor$

Example k = 1

$h(1) = \lfloor 10000((1(1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(((1+\sqrt{5})/2) \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 \mod 1) \rfloor$
$= \lfloor 10000(1.61803398875 - \lfloor 1.61803398875 \rfloor) \rfloor$
$= \lfloor 10000(1.61803398875 - 1) \rfloor$
$= \lfloor 10000(0.61803398875) \rfloor$
$= \lfloor 6180.3398875 \rfloor = 6180$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1)\rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

k - preimages and h(k) - images

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

The maximal length in bits of the images $\rightarrow$ The maximal of h(k)

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod$ $1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

r $\mod$ $1 = \leq$ r - $\lfloor$ r $\rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

r $\mod 1 = \leq$ r - $\lfloor$ r $\rfloor$

$0 \leq$ r - $\lfloor$ r $\rfloor \leq 0.9999999...$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1)\rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

$0 \leq$ r $\mod 1 \leq 0.9999999...$

$\lfloor$ 10000((k (1+$\sqrt{5}$)/2) $\mod 1)\rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1)\rfloor$
r $\mod$ 1 = r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

0 $\le$ r $\mod$ 1 $\le$ 0.9999999...

$\lfloor$ 10000((k (1+$\sqrt{5}$)/2) $\mod$ 1)$\rfloor$
$\lfloor$10000(0)$\rfloor$ $\le$ $\lfloor$10000((k (1+$\sqrt{5}$)/2) $\mod$ 1)$\rfloor$ $\le$ $\lfloor$ 10000(0.99999999...)$\rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

$0 \leq$ r $\mod 1 \leq 0.9999999...$

$\lfloor 10000((k\ (1+\sqrt{5})/2) \mod 1) \rfloor$
$\lfloor 10000(0) \rfloor \leq \lfloor 10000((k\ (1+\sqrt{5})/2) \mod 1) \rfloor \leq \lfloor$
$10000(0.99999999...) \rfloor$
$\lfloor 0 \rfloor \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq \lfloor 9999.9999... \rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

$0 \leq$ r $\mod 1 \leq 0.9999999...$

$\lfloor$ 10000((k $(1+\sqrt{5})/2) \mod 1) \rfloor$
$\lfloor 10000(0) \rfloor \leq \lfloor 10000(($k $(1+\sqrt{5})/2) \mod 1) \rfloor \leq \lfloor$
$10000(0.99999999...) \rfloor$
$\lfloor 0 \rfloor \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq \lfloor 9999.9999... \rfloor$
$0 \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq 9999$

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
$r \mod 1 = r - \lfloor r \rfloor$

- Determine the maximal length in bits of the images.

$r \mod 1 = \leq r - \lfloor r \rfloor$

$0 \leq r - \lfloor r \rfloor \leq 0.9999999... \rightarrow 0 \leq r \mod 1 \leq 0.9999999...$

$\lfloor 10000((k\ (1+\sqrt{5})/2) \mod 1) \rfloor$

$\lfloor 10000(0) \rfloor \leq \lfloor 10000((k\ (1+\sqrt{5})/2) \mod 1) \rfloor \leq \lfloor 10000(0.99999999...) \rfloor$

$\lfloor 0 \rfloor \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq \lfloor 9999.9999... \rfloor$

$0 \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq 9999$

The maximum of h(k) = 9999

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

$$0 \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq 9999$$

The maximum of h(k) $= 9999 \rightarrow$ the maximal length in bits ?

A. 4

B. 8

C. 14

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Determine the maximal length in bits of the images.

$$0 \leq \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor \leq 9999$$

The maximum of h(k) = 9999 $\rightarrow$ the maximal length in bits ?
9999 $\cong 2^{13.287568103} \rightarrow 2^{13} <$ h(k) $< 2^{14} \rightarrow$ the maximal length in bits = 14

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

$r \mod 1 = r - \lfloor r \rfloor$

- Give a collision of this hash function.

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Give a collision of this hash function.

To find k_1 and k_2 such as
$\lfloor 10000((\mathrm{k}_1(1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((\mathrm{k}_2(1+\sqrt{5})/2) \mod 1) \rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Give a collision of this hash function.

Do you know this number?

$(1+\sqrt{5})/2$

A. yes

B. no

Question 3: Hash function collisions

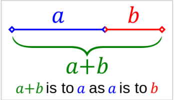
Golden Ratio

In mathematics, two quantities are in the **golden ratio** if their ratio is the same as the ratio of their sum to the larger of the two quantities. The figure on the right illustrates the geometric relationship. Expressed algebraically, for quantities *a* and *b* with $a > b > 0$,

$$\frac{a+b}{a} = \frac{a}{b} \stackrel{\text{def}}{=} \varphi,$$

where the Greek letter phi (φ or ϕ) represents the golden ratio.[a] It is an irrational number that is a solution to the quadratic equation $x^2 - x - 1 = 0$, with a value of:

$$\varphi = \frac{1+\sqrt{5}}{2} = 1.6180339887\ldots.^{[1]}$$



Line segments in the golden ratio

Question 3: Hash function collisions

Fibonacci numbers

In mathematics, the **Fibonacci numbers**, commonly denoted F_n, form a sequence, called the **Fibonacci sequence**, such that each number is the sum of the two preceding ones, starting from 0 and 1. That is,[1]

$$F_0 = 0, \quad F_1 = 1,$$

and

$$F_n = F_{n-1} + F_{n-2},$$

for $n > 1$.

The beginning of the sequence is thus:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \ldots$$ [2]

Question 3: Hash function collisions

Fibonacci numbers

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varphi.$$

Question 3: Hash function collisions

Fibonacci numbers

n	Fibonacci Numbers	Ratio of Adjacent Terms
0	1	-
1	1	1
2	2	2
3	3	1.5
4	5	1.666666667
5	8	1.6
6	13	1.625
7	21	1.615384615
8	34	1.619047619
9	55	1.617647059
10	89	1.618181818
11	144	1.617977528
12	233	1.618055556
13	377	1.618025751
14	610	1.618037135
15	987	1.618032787
16	1597	1.618034448
17	2584	1.618033813
18	4181	1.618034056
19	6765	1.618033963
20	10946	1.618033999
21	17711	1.618033985
22	28657	1.61803399
23	46368	1.618033988

Question 3: Hash function collisions

$\mathrm{k} \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r mod $1 =$ r - $\lfloor$ r $\rfloor$

- Give a collision of this hash function.

To find k_1 and k_2 such as
$\lfloor 10000((\mathrm{k}_1(1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((\mathrm{k}_2(1+\sqrt{5})/2) \mod 1) \rfloor$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Give a collision of this hash function.

To find k_1 and k_2 such as
$\lfloor 10000((\mathrm{k}_1(1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((\mathrm{k}_2(1+\sqrt{5})/2) \mod 1) \rfloor$

Question 3: Hash function collisions

$k \mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$

$r \mod 1 = r - \lfloor r \rfloor$

- Give a collision of this hash function.

To find k_1 and k_2 such as

$\lfloor 10000((k_1(1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((k_2(1+\sqrt{5})/2) \mod 1) \rfloor$

Considering four numbers after decimal

Question 3: Hash function collisions

- Give a collision of this hash function.

Choose $k_1 = 1$
$\lfloor 10000((1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((\mathrm{k}_2(1+\sqrt{5})/2) \mod 1) \rfloor$
k_2 ?

$\frac{a}{b}$ and $\frac{a}{b}$ *(b + 1) = a + $\frac{a}{b}$
If a is a nature number, $\frac{a}{b}$ - $\lfloor \frac{a}{b} \rfloor$ = a + $\frac{a}{b}$ - $\lfloor$ a + $\frac{a}{b}$ $\rfloor$
($\frac{a}{b}$ mod 1 = (a + $\frac{a}{b}$) mod 1)

Question 3: Hash function collisions

Fibonacci numbers

	A	B	C
1	n	Fibonacci Numbers	Ratio of Adjacent Terms
2	0	1	-
3	1	1	1
4	2	2	2
5	3	3	1.5
6	4	5	1.666666667
7	5	8	1.6
8	6	13	1.625
9	7	21	1.615384615
10	8	34	1.619047619
11	9	55	1.617647059
12	10	89	1.618181818
13	11	144	1.617977528
14	12	233	1.618055556
15	13	377	1.618025751
16	14	610	1.618037135
17	15	987	1.618032787
18	16	1597	1.618034448
19	17	2584	1.618033813
20	18	4181	1.618034056
21	19	6765	1.618033963
22	20	10946	1.618033999
23	21	17711	1.618033985
24	22	28657	1.61803399
25	23	46368	1.618033988

Question 3: Hash function collisions

- Give a collision of this hash function.

Choose $k_1 = 1$

$\lfloor 10000((1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((\mathrm{k}_2(1+\sqrt{5})/2) \mod 1) \rfloor$

k_2 ?

- $\frac{17711}{10946} \cong \frac{1+\sqrt{5}}{2}$
- $\frac{17711}{10946} \mod 1 = (10946 + 1)*\frac{17711}{10946} \mod 1 = (1 + \frac{17711}{10946}) \mod 1$

Question 3: Hash function collisions

- Give a collision of this hash function.

Choose $k_1 = 1$

$\lfloor 10000((1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000((\mathrm{k}_2(1+\sqrt{5})/2) \mod 1) \rfloor$

k_2 10947

$$\lfloor 10000(10947(1+\sqrt{5})/2) \mod 1) \rfloor = \lfloor 10000(10947\tfrac{17711}{10946} \mod 1) \rfloor$$
$$= \lfloor 10000((10946+1)\tfrac{17711}{10946} \mod 1) \rfloor = \lfloor 10000((1+\tfrac{17711}{10946}) \mod 1) \rfloor$$

$$= \lfloor 10000(\tfrac{17711}{10946} \mod 1) \rfloor$$
$$\cong \lfloor 10000((1+\sqrt{5})/2 \mod 1) \rfloor$$

Question 3: Hash function collisions

k $\mapsto \lfloor 10000((k(1+\sqrt{5})/2) \mod 1) \rfloor$
r $\mod 1 =$ r - $\lfloor$ r $\rfloor$

- Give a collision of this hash function.

a collision $(k_1, k_2) = (1, 10947)$

Question 4: Hash function from compression function

Explain the construction of a hash function from a compression function for the concrete case of $r=1$.

Question 4: Hash function from compression function

Merkle-Damgaard procedure

Let $f : B^m \to B^n$ be a compression function and let $r = m - n \geq 2$.
The goal is to construct a hash function $h : B^* \to B^n$ from f.

m = n + r and $B^* \to B^m$

Question 4: Hash function from compression function

Merkle-Damgaard procedure

Let $f : B^m \to B^n$ be a compression function and let $r = m - n \geq 2$.
The goal is to construct a hash function $h : B^* \to B^n$ from f.

m = n + r and $B^* \to B^m$

Preprocessing Step 1

Given $x \in B^*$, prepend the minimal number $0 \leq k < r$ of zeroes such that the new length is a multiple of r and append 0^r. Result: $x' = 0^k \| x \| 0^r$

Question 4: Hash function from compression function

Merkle-Damgaard procedure

Let $f : B^m \to B^n$ be a compression function and let $r = m - n \geq 2$.
The goal is to construct a hash function $h : B^* \to B^n$ from f.

m = n + r and $B^* \to B^m$

Preprocessing Step 1

Given $x \in B^*$, prepend the minimal number $0 \leq k < r$ of zeroes such that the new length is a multiple of r and append 0^r. Result: $x' = 0^k \| x \| 0^r$

Preprocessing Step 2

Calculate the binary representation b of the original length of x and prepend zeroes such that its length is divisible by $r - 1$. Starting at the beginning insert 1 at every $r - 1$st position of the resulting string. The length of the resulting string b' is a multiple of r.

Question 4: Hash function from compression function

Merkle-Damgaard procedure

Let $f : B^m \rightarrow B^n$ be a compression function and let $r = m - n \geq 2$.
The goal is to construct a hash function $h : B^* \rightarrow B^n$ from f.

m = n + r and $B^* \rightarrow B^m$

Preprocessing Step 1

Given $x \in B^*$, prepend the minimal number $0 \leq k < r$ of zeroes such that the new length is a multiple of r and append 0^r. Result: $x' = 0^k \| x \| 0^r$

Preprocessing Step 2

Calculate the binary representation b of the original length of x and prepend zeroes such that its length is divisible by $r - 1$. Starting at the beginning insert 1 at every $r - 1$st position of the resulting string. The length of the resulting string b' is a multiple of r.

Preprocessing Step 3

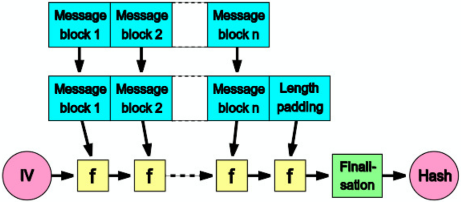
Prepend b' to obtain a string $b' \| 0^k \| x \| 0^r$ of length $t \cdot r$. Decompose into $x_1 \| x_2 \| \ldots \| x_t$ with $x_i \in B^r$

Constructing the hash function

Definition

Define $h(x) = H_t$ where

- $x_1 \| x_2 \| \dots \| x_t$ with $x_i \in B^r$ is the result of preprocessing $x \in B^*$.
- $H_0 = 0^n$ (or a different, but fixed initialization vector).
- $H_i = f(H_{i-1} \| x_i)$ for $1 \le i \le t$.



Question 4: Hash function from compression function

Preprocessing Step 1

Given $x \in B^*$, prepend the minimal number $0 \leq k < r$ of zeroes such that the new length is a multiple of r and append 0^r. Result: $x' = 0^k \| x \| 0^r$

x || 0

Question 4: Hash function from compression function

Preprocessing Step 2

Calculate the binary representation b of the original length of x and prepend zeroes such that its length is divisible by $r - 1$. Starting at the beginning insert 1 at every $r - 1$st position of the resulting string. The length of the resulting string b' is a multiple of r.

b || x || 0

Question 4: Hash function from compression function

Preprocessing Step 3

Prepend b' to obtain a string $b' \| 0^k \| x \| 0^r$ of length $t \cdot r$. Decompose into $x_1 \| x_2 \| \ldots \| x_t$ with $x_i \in B^r$.

b || x || 0. Decompose into
$x_1 \| x_2 \| \ldots \| x_t$ with $x_i \in B^1$.
t = len(x) + len(b) + 1

Question 4: Hash function from compression function

Preprocessing Step 3

Prepend b' to obtain a string $b' \| 0^k \| x \| 0^r$ of length $t \cdot r$. Decompose into $x_1 \| x_2 \| \ldots \| x_t$ with $x_i \in B^r$.

b || x || 0. Decompose into
$x_1 \| x_2 \| \ldots \| x_t$ with $x_i \in B^1$.
t = len(x) + len(b) + 1

Constructing the hash function

Definition

Define $h(x) = H_t$ where

- $x_1 \| x_2 \| \dots \| x_t$ with $x_i \in B^1$ is the result of preprocessing $x \in B^*$.
- $H_0 = 0^n$ (or a different, but fixed initialization vector).
- $H_i = f(H_{i-1} \| x_i)$ for $1 \le i \le t$.