

YouTube x Messenger x WhatsApp x Manage Saniti x sha1 - Google x SHA-1 - Wikipe x sha1 algorithm x How Does SHA x New Tab

youtube.com/watch?v=kmHojGMUn0Q

# How SHA-1 Works

1. Take input text and split it into an array of the characters' ASCII codes

'A Test'

[A, , T, e, s, t]

```
function sha1(text) {  
  const asciiText = text.split('')  
  .map((letter) => utils.charToASCII(letter));  
}
```

[65, 32, 84, 101, 115, 116]

**FULLSTACK**  
ACADEMY of CODE

8:48 / 12:15

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views • 27 Jan 2017

572 53 SHARE SAVE

Fullstack Academy

Type here to search

How Does SHA-256 Work?

learnmeabitcoin  
26K views • 8 months ago

22:59

All Algorithms Functions Related

Hashing Algorithms and Security - Computerphile

Computerphile  
1M views • 7 years ago

8:12

Cryptocurrencies

But how does bitcoin actually work?

3Blue1Brown  
5.6M views • 3 years ago

26:21

157920892731619542  
3570907853  
2699840394  
57584007941296

How secure is 256 bit security?

3Blue1Brown  
1.7M views • 3 years ago

5:06

Lecture 21: SHA-1 Hash Function by Christof Paar

Introduction to Cryptography by C...  
35K views • 6 years ago

1:18:35

SHA: Secure Hashing Algorithm - Computerphile

Computerphile  
772K views • 3 years ago

10:21

Deen I learned Super-Samlinn

1629  
17-01-2021

YouTube x Messenger x WhatsApp x Manage Saniti x sha1 - Google x SHA-1 - Wikipe x sha1 algorithm x How Does SHA x New Tab

youtube.com/watch?v=kmHojGMUn0Q

# How SHA-1 Works

2. Convert ASCII codes to binary

3. Pad zeros to the front of each until they are 8 bits long

[65, 32, 84, 101, 115, 116]

```
let binary8bit = asciiText  
  .map((num) => utils.asciiToBinary(num))  
  .map((num) => utils.padZero(num, 8));
```

[01000001, 00100000,  
01010100, 01100101,  
01110011, 01110100]

**FULLSTACK**  
ACADEMY of CODE

9:03 / 12:15

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views • 27 Jan 2017

572 53 SHARE SAVE

Fullstack Academy

Type here to search

How Does SHA-256 Work?

learnmeabitcoin  
26K views • 8 months ago

22:59

All Algorithms Functions Related

Hashing Algorithms and Security - Computerphile

Computerphile  
1M views • 7 years ago

8:12

Cryptocurrencies

But how does bitcoin actually work?

3Blue1Brown  
5.6M views • 3 years ago

26:21

157920892731619542  
3570907853  
2699840394  
57584007941296

How secure is 256 bit security?

3Blue1Brown  
1.7M views • 3 years ago

5:06

Lecture 21: SHA-1 Hash Function by Christof Paar

Introduction to Cryptography by C...  
35K views • 6 years ago

1:18:35

SHA: Secure Hashing Algorithm - Computerphile

Computerphile  
772K views • 3 years ago

10:21

Deen I learned Super-Samlinn

1629  
17-01-2021







YouTube x Messenger x WhatsApp x Manage Saniti x sha1 - Google x W SHA-1 - Wikiped x sha1 algorithm x YouTube How Does x New Tab x

youtube.com/watch?v=kmHojGMU0Q

YouTube

Search

11. loop through each 'chunk' array of sixteen 32-bit 'words' and extend each array to 80 'words' using bitwise operations

```
//chunkWords is an array of 'chunk' subarrays
const words80 = chunkWords.map(chunk => {
  //we start with a 'chunk' array of 16 32-bit 'words'
  for (let i = 16; i <= 79; i++) {
    //take four words from that chunk using
    //your current i in the loop
    const wordA = chunk[i - 3];
    const wordB = chunk[i - 4];
    const wordC = chunk[i - 14];
    const wordD = chunk[i - 15];

    //perform consecutive XOR bitwise
    //operations going through each word
    const word = utils.xor(wordA, wordB);
    const wordC = utils.xor(wordC, wordD);
    const wordD = utils.xor(wordC, word);

    //left rotate by one
    const newWord = utils.leftRotate(wordC, 1);
    //append to the array and continue the loop
    chunk.push(newWord);
  }
  return array;
});
```

**FULLSTACK**  
ACADEMY of CODE

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views • 27 Jan 2017

572 53 SHARE SAVE

Fullstack Academy

How Does SHA-256 Work?

learnmeabitcoin  
26K views • 8 months ago

22:59

All Algorithms Functions Related

Hashing Algorithms and Security - Computerphile

Computerphile  
1M views • 7 years ago

8:12

Cryptocurrencies

But how does bitcoin actually work?

3Blue1Brown  
5.6M views • 3 years ago

26:21

15792089931619542

3570007853

26998440394

5758400731296

How secure is 256 bit security?

3Blue1Brown  
1.7M views • 3 years ago

5:06

Lecture 21: SHA-1 Hash Function by Christof Paar

Introduction to Cryptography by C...

35K views • 6 years ago

1:18:35

SHA: Secure Hashing Algorithm - Computerphile

Computerphile  
772K views • 3 years ago

10:21

Deen I earned Super-Samlinn

1633

17-01-2021

YouTube x Messenger x WhatsApp x Manage Saniti x sha1 - Google x W SHA-1 - Wikiped x sha1 algorithm x YouTube How Does x New Tab x

youtube.com/watch?v=kmHojGMU0Q

YouTube

Search

12. initialize some variables

```
let h0 = '01100111010001010010001100000001';
let h1 = '111011110010101010110001001';
let h2 = '100100010110101011001111110';
let h3 = '000100000110010101000110110';
let h4 = '110000111010010111000011110000';
let a = h0;
let b = h1;
let c = h2;
let d = h3;
let e = h4;
```

**FULLSTACK**  
ACADEMY of CODE

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views • 27 Jan 2017

572 53 SHARE SAVE

Fullstack Academy

How Does SHA-256 Work?

learnmeabitcoin  
26K views • 8 months ago

22:59

All Algorithms Functions Related

Hashing Algorithms and Security - Computerphile

Computerphile  
1M views • 7 years ago

8:12

Cryptocurrencies

But how does bitcoin actually work?

3Blue1Brown  
5.6M views • 3 years ago

26:21

15792089931619542

3570007853

26998440394

5758400731296

How secure is 256 bit security?

3Blue1Brown  
1.7M views • 3 years ago

5:06

Lecture 21: SHA-1 Hash Function by Christof Paar

Introduction to Cryptography by C...

35K views • 6 years ago

1:18:35

SHA: Secure Hashing Algorithm - Computerphile

Computerphile  
772K views • 3 years ago

10:21

Deen I earned Super-Samlinn

1634

17-01-2021



YouTube Messenger WhatsApp Manage Sanitiz sha1 - Google SHA-1 - Wikipe sha1 algorithm How Does New Tab

youtube.com/watch?v=kmHojGMUn0Q

13. looping through each chunk: bitwise operations and variable reassignment

```
for (let i = 0; i < chunks.length; i++) {
  for (let j = 0; j < 80; j++) {
    let b;
    if (i < 20) {
      const chunk = utila.add(utila.add(h, chunk), chunk);
      b = utila.add(chunk, chunk);
    } else if (i < 40) {
      const chunk = utila.add(chunk, chunk);
      b = utila.add(chunk, chunk);
    } else if (i < 60) {
      const chunk = utila.add(chunk, chunk);
      b = utila.add(chunk, chunk);
    } else if (i < 80) {
      const chunk = utila.add(chunk, chunk);
      b = utila.add(chunk, chunk);
    }
    const result = utila.add(chunk, b);
    h = utila.add(h, result);
    const temp = utila.add(h, result);
    h = utila.add(h, temp);
    const temp2 = utila.add(h, temp);
    h = utila.add(h, temp2);
    const temp3 = utila.add(h, temp2);
    h = utila.add(h, temp3);
    const temp4 = utila.add(h, temp3);
    h = utila.add(h, temp4);
    const temp5 = utila.add(h, temp4);
    h = utila.add(h, temp5);
    const temp6 = utila.add(h, temp5);
    h = utila.add(h, temp6);
    const temp7 = utila.add(h, temp6);
    h = utila.add(h, temp7);
    const temp8 = utila.add(h, temp7);
    h = utila.add(h, temp8);
    const temp9 = utila.add(h, temp8);
    h = utila.add(h, temp9);
    const temp10 = utila.add(h, temp9);
    h = utila.add(h, temp10);
    const temp11 = utila.add(h, temp10);
    h = utila.add(h, temp11);
    const temp12 = utila.add(h, temp11);
    h = utila.add(h, temp12);
    const temp13 = utila.add(h, temp12);
    h = utila.add(h, temp13);
    const temp14 = utila.add(h, temp13);
    h = utila.add(h, temp14);
    const temp15 = utila.add(h, temp14);
    h = utila.add(h, temp15);
    const temp16 = utila.add(h, temp15);
    h = utila.add(h, temp16);
    const temp17 = utila.add(h, temp16);
    h = utila.add(h, temp17);
    const temp18 = utila.add(h, temp17);
    h = utila.add(h, temp18);
    const temp19 = utila.add(h, temp18);
    h = utila.add(h, temp19);
    const temp20 = utila.add(h, temp19);
    h = utila.add(h, temp20);
    const temp21 = utila.add(h, temp20);
    h = utila.add(h, temp21);
    const temp22 = utila.add(h, temp21);
    h = utila.add(h, temp22);
    const temp23 = utila.add(h, temp22);
    h = utila.add(h, temp23);
    const temp24 = utila.add(h, temp23);
    h = utila.add(h, temp24);
    const temp25 = utila.add(h, temp24);
    h = utila.add(h, temp25);
    const temp26 = utila.add(h, temp25);
    h = utila.add(h, temp26);
    const temp27 = utila.add(h, temp26);
    h = utila.add(h, temp27);
    const temp28 = utila.add(h, temp27);
    h = utila.add(h, temp28);
    const temp29 = utila.add(h, temp28);
    h = utila.add(h, temp29);
    const temp30 = utila.add(h, temp29);
    h = utila.add(h, temp30);
    const temp31 = utila.add(h, temp30);
    h = utila.add(h, temp31);
    const temp32 = utila.add(h, temp31);
    h = utila.add(h, temp32);
    const temp33 = utila.add(h, temp32);
    h = utila.add(h, temp33);
    const temp34 = utila.add(h, temp33);
    h = utila.add(h, temp34);
    const temp35 = utila.add(h, temp34);
    h = utila.add(h, temp35);
    const temp36 = utila.add(h, temp35);
    h = utila.add(h, temp36);
    const temp37 = utila.add(h, temp36);
    h = utila.add(h, temp37);
    const temp38 = utila.add(h, temp37);
    h = utila.add(h, temp38);
    const temp39 = utila.add(h, temp38);
    h = utila.add(h, temp39);
    const temp40 = utila.add(h, temp39);
    h = utila.add(h, temp40);
    const temp41 = utila.add(h, temp40);
    h = utila.add(h, temp41);
    const temp42 = utila.add(h, temp41);
    h = utila.add(h, temp42);
    const temp43 = utila.add(h, temp42);
    h = utila.add(h, temp43);
    const temp44 = utila.add(h, temp43);
    h = utila.add(h, temp44);
    const temp45 = utila.add(h, temp44);
    h = utila.add(h, temp45);
    const temp46 = utila.add(h, temp45);
    h = utila.add(h, temp46);
    const temp47 = utila.add(h, temp46);
    h = utila.add(h, temp47);
    const temp48 = utila.add(h, temp47);
    h = utila.add(h, temp48);
    const temp49 = utila.add(h, temp48);
    h = utila.add(h, temp49);
    const temp50 = utila.add(h, temp49);
    h = utila.add(h, temp50);
    const temp51 = utila.add(h, temp50);
    h = utila.add(h, temp51);
    const temp52 = utila.add(h, temp51);
    h = utila.add(h, temp52);
    const temp53 = utila.add(h, temp52);
    h = utila.add(h, temp53);
    const temp54 = utila.add(h, temp53);
    h = utila.add(h, temp54);
    const temp55 = utila.add(h, temp54);
    h = utila.add(h, temp55);
    const temp56 = utila.add(h, temp55);
    h = utila.add(h, temp56);
    const temp57 = utila.add(h, temp56);
    h = utila.add(h, temp57);
    const temp58 = utila.add(h, temp57);
    h = utila.add(h, temp58);
    const temp59 = utila.add(h, temp58);
    h = utila.add(h, temp59);
    const temp60 = utila.add(h, temp59);
    h = utila.add(h, temp60);
    const temp61 = utila.add(h, temp60);
    h = utila.add(h, temp61);
    const temp62 = utila.add(h, temp61);
    h = utila.add(h, temp62);
    const temp63 = utila.add(h, temp62);
    h = utila.add(h, temp63);
    const temp64 = utila.add(h, temp63);
    h = utila.add(h, temp64);
    const temp65 = utila.add(h, temp64);
    h = utila.add(h, temp65);
    const temp66 = utila.add(h, temp65);
    h = utila.add(h, temp66);
    const temp67 = utila.add(h, temp66);
    h = utila.add(h, temp67);
    const temp68 = utila.add(h, temp67);
    h = utila.add(h, temp68);
    const temp69 = utila.add(h, temp68);
    h = utila.add(h, temp69);
    const temp70 = utila.add(h, temp69);
    h = utila.add(h, temp70);
    const temp71 = utila.add(h, temp70);
    h = utila.add(h, temp71);
    const temp72 = utila.add(h, temp71);
    h = utila.add(h, temp72);
    const temp73 = utila.add(h, temp72);
    h = utila.add(h, temp73);
    const temp74 = utila.add(h, temp73);
    h = utila.add(h, temp74);
    const temp75 = utila.add(h, temp74);
    h = utila.add(h, temp75);
    const temp76 = utila.add(h, temp75);
    h = utila.add(h, temp76);
    const temp77 = utila.add(h, temp76);
    h = utila.add(h, temp77);
    const temp78 = utila.add(h, temp77);
    h = utila.add(h, temp78);
    const temp79 = utila.add(h, temp78);
    h = utila.add(h, temp79);
    const temp80 = utila.add(h, temp79);
    h = utila.add(h, temp80);
  }
}
```

h0 = 01100111010001010010001100000001  
h1 = 11101111100101010101010110001001  
h2 = 1001000101010101010101011000111110  
h3 = 00010000001100100101010001110110  
h4 = 11000011110100101110000111110110

h0 = 10001111000011000000100001010101  
h1 = 1001000101010100011001111000100  
h2 = 101001111011110000110010000110  
h3 = 10001011001110000111010011001000  
h4 = 100100000011101111000001000011

Fullstack Academy

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views · 27 Jan 2017

572 53 SHARE SAVE

YouTube Messenger WhatsApp Manage Sanitiz sha1 - Google SHA-1 - Wikipe sha1 algorithm How Does New Tab

YouTube Messenger WhatsApp Manage Sanitiz sha1 - Google SHA-1 - Wikipe sha1 algorithm How Does SHA New Tab

youtube.com/watch?v=kmHojGMUn0Q

14. convert each of the five resulting variables to hexadecimal  
15. join them together and return it!

```
return [h0, h1, h2, h3, h4].map((string) => utila.binaryToHex(string)).join("");
```

h0 = 8f0c855  
h1 = 915633e4  
h2 = a7de1946  
h3 = 8b3874c8  
h4 = 901df043

Fullstack Academy

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views · 27 Jan 2017

572 53 SHARE SAVE

YouTube Messenger WhatsApp Manage Sanitiz sha1 - Google SHA-1 - Wikipe sha1 algorithm How Does SHA New Tab

YouTube Messenger WhatsApp Manage Saniti sha1 - Google SHA-1 - Wikip sha1 algorithm How Does New Tab

youtube.com/watch?v=kmHojGMUn0Q

YouTube

Your hash value!

8f0c0855915633e4a7de19468b3874c8901df043

FULLSTACK ACADEMY of CODE

How Does SHA-1 Work - Intro to Cryptographic Hash Functions and SHA-1

36,458 views • 27 Jan 2017

572 53 SHARE SAVE

Fullstack Academy

How Does SHA-256 Work? learnmeabitcoin 26K views • 8 months ago 22:59

Hashing Algorithms and Security - Computerphile Computerphile 1M views • 7 years ago 8:12

Cryptocurrencies But how does bitcoin actually work? 3Blue1Brown 5.6M views • 3 years ago 26:21

How secure is 256 bit security? 3Blue1Brown 1.7M views • 3 years ago 5:06

Lecture 21: SHA-1 Hash Function by Christof Paar Introduction to Cryptography by C... 35K views • 6 years ago 1:18:35

SHA: Secure Hashing Algorithm - Computerphile Computerphile 772K views • 3 years ago 10:21

Deen I earned Siner-Samnlinn 16:35 17-01-2021

Link to video: <https://www.youtube.com/watch?v=kmHojGMUn0Q>