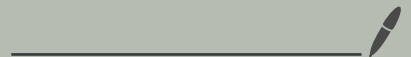


Name - Jay Shah
Nikhil Raina

Homework # 8



1.

a) The hash function takes an input and then performs the hash that will be explained below:

```
hash (input)
```

```
    if input isEmpty:
```

```
        return hex(10) // default value to return if input  
                        is empty.
```

```
    else :
```

```
        x = unicode point of input[0] // ord(input[0])
```

```
        m = 10 // custom power value.
```

```
        for c in input:
```

```
            x = generate_32_bit((x * m) ^ ord(c))
```

```
        x = x ^ length(input)
```

```
        if x == -1 :
```

```
            x = -2
```

```
        return hex(abs(x))[2:] // avoids '0x'
```

```
generate_32_bit (value) :
```

```
    // converts the value to a 32 bit integer.
```

```
    x = value % (232) // to keep the number within  
                      232 bits.
```

```
    if x > 231 :
```

```
        x = x - 232 // same reason as above.
```

```
    return int(x)
```

b)

```

-----
Collision Occurred [ 1 ]
Input 1 = 125107 , with Binary: 11110100010110011
Input 2 = 166052 , with Binary: 101000100010100100
32-bit Hash: 7ad5eec6

Collision Occurred [ 2 ]
Input 1 = 125095 , with Binary: 11110100010100111
Input 2 = 166064 , with Binary: 101000100010110000
32-bit Hash: 7ad63132

Total time taken to find the collisions: 1.662555456161499 seconds
-----

```

c)

collisions = 0

input = 0

hex-values = dictionary()

while True:

 convert input to binary

 hex-result = hash(converted-binary)

 if hex-result in hex-values:

 collisions += 1 // collision occurred

 else

 add hex-result as key with the
 converted-binary as the value.

 increment input += 1

d)

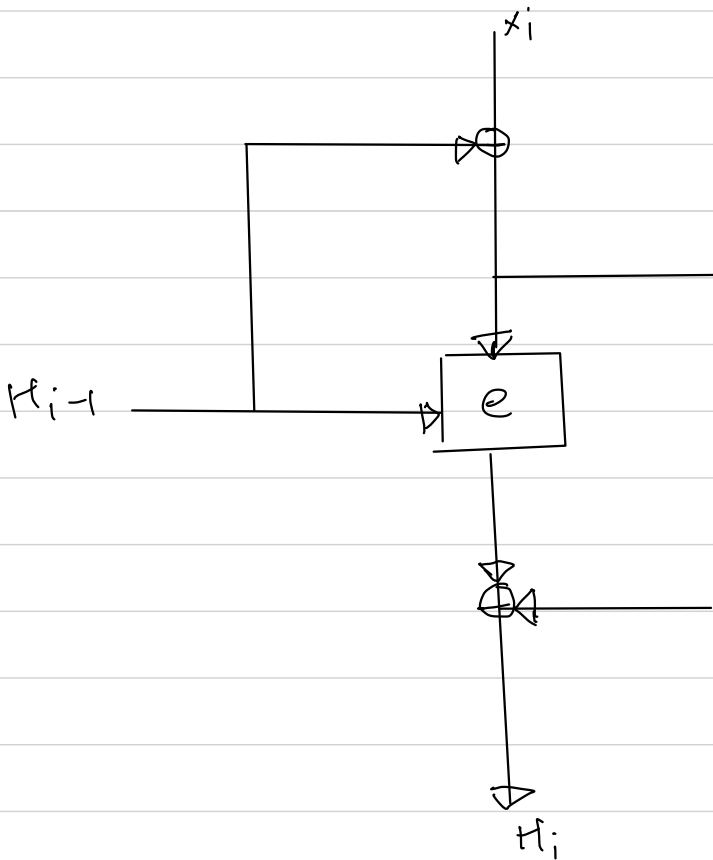
```

Total time taken to find the collisions: 1.662555456161499 seconds
-----

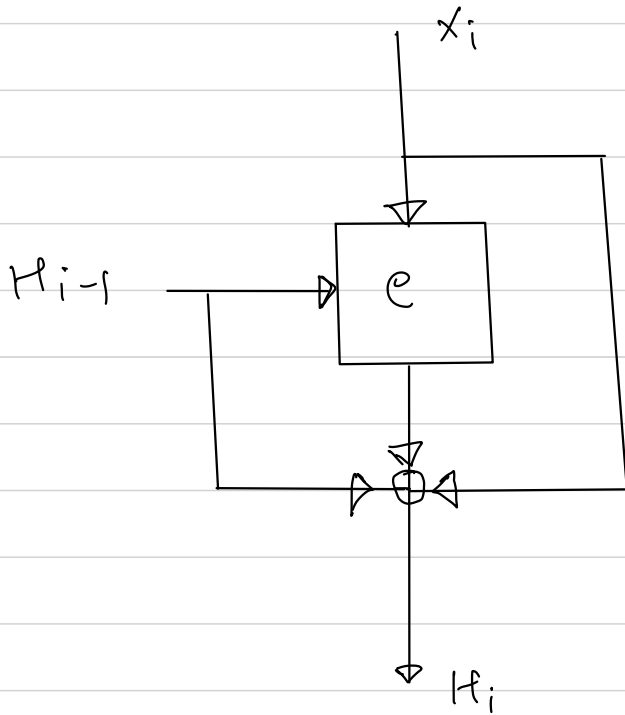
```

11.3 Draw a block diagram for the following hash functions.

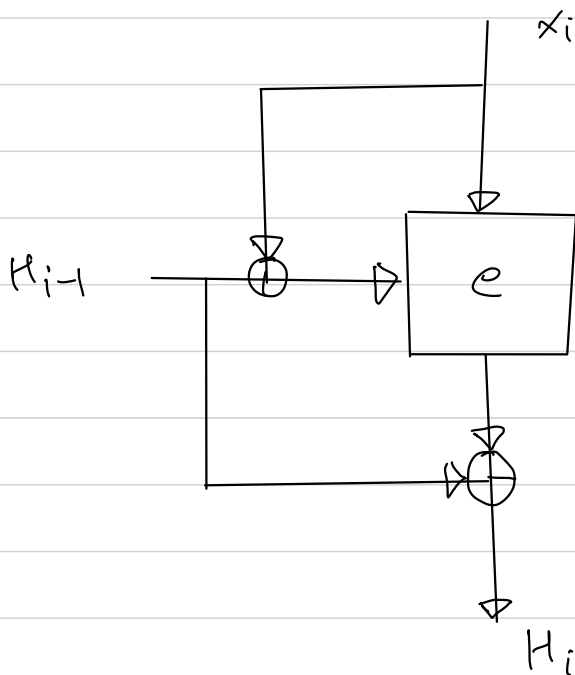
1. $e(H_{i-1}, x_i) \oplus x_i$



$$2. \quad e(H_{i-1}, x_i \oplus H_{i-1}) \oplus x_i \oplus H_{i-1}$$



$$3. \quad E(H_{i-1}, x_i) \oplus x_i \oplus H_{i-1}$$



4. $E(x_i \oplus H_{i-1}, x_i) \oplus H_{i-1}$

