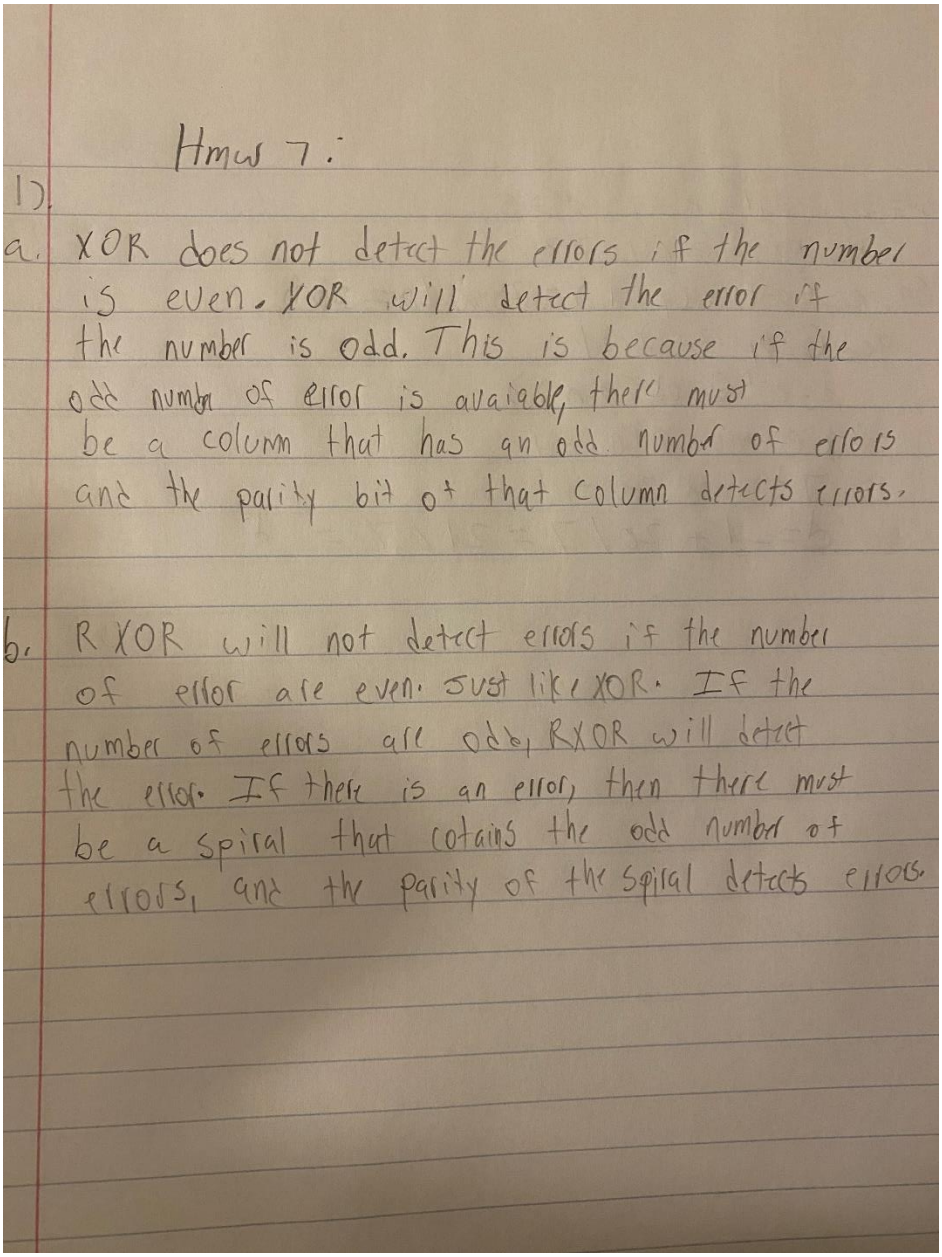
Issa Odeh

Homework 7

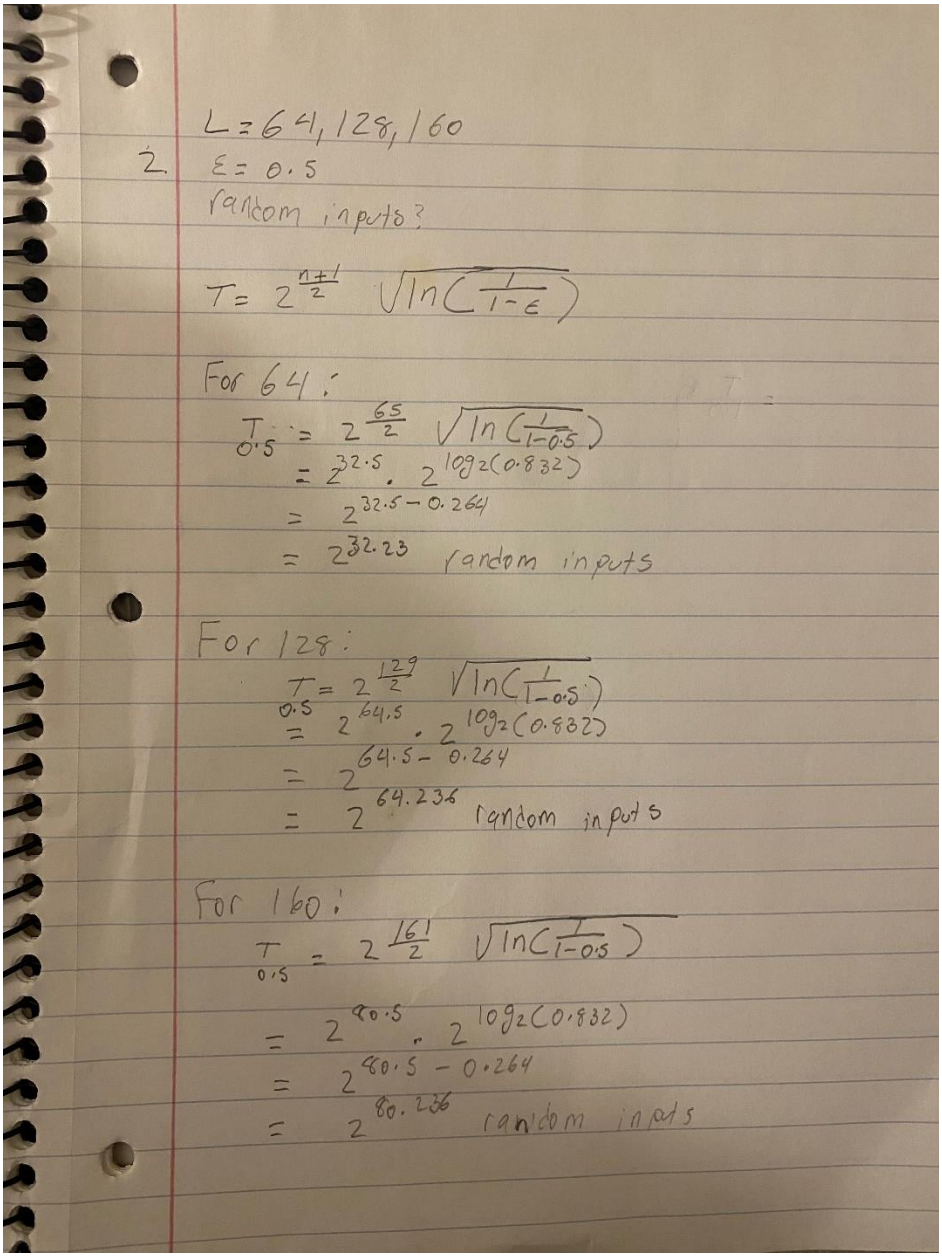


Hmw 7:

1).

a. XOR does not detect the errors if the number is even. XOR will detect the error if the number is odd. This is because if the odd numbr of error is avaiable, there must be a column that has an odd number of errors and the parity bit of that column detects errors.

b. RXOR will not detect errors if the number of error are even. Just like XOR. If the number of errors are odd, RXOR will detect the error. If there is an error, then there must be a spiral that cotains the odd number of errors, and the parity of the spiral detects errors.



3.

a).

L(1,2) = 01020304H.

New L(1,2) = (01020304H +1) * (01020304H+2) / 2

= 52051165665H

b).

L(1,2)

New x and y in L(1,2) after pi step = 2 , 1

c).

L(2,0) = 01020304H

New L(2,0) after chi step = 01020304H

4.

Bitcoin is uses a hash algorithm that is used by a lot of other cryptocurrencies and it is SHA-256 algorithm. This hash functions takes the length of the data that is arbitrary, then turns the data to a fixed length. This algorithm uses 256 bits to work. It is a one-way function meaning you cannot decrypt backwards. This algorithm makes the hashed data completely unreadable by anyone else. This algorithm is used in a lot of applications where information is kept from everyone. It is one of the most secure hashing functions out there, if not the most secure. This algorithm uses a block cipher for encryption and decryption. This algorithm can be used to secure and store passwords for more security. It uses the hash values of the passwords to store. Only the person wo has the key has access to all the information being stored. This algorithm is very efficient, it doesn't take a long time for the hash to compute. No collision attacks can happen to SHA-256 because it is hard to find the distinct inputs that is the same result as when it is already been hashed. The hash is also always random, so it will never duplicate the same numbers if there is the same inputs.

https://en.bitcoinwiki.org/wiki/Hash

https://www.investopedia.com/terms/t/target-hash.asp#:~:text=Bitcoin%20uses%20the%20SHA%2D256,amount%20of%20computer%20processing%20power.