ENGR 13300
Python Project Resource – XOR Cipher

XOR Cipher:

The XOR cipher follows the same procedure to encrypt and to decrypt a pixel value:

1. For a single pixel value (A) and the key for that pixel (K), we first convert those numbers into binary format.
2. Apply bitwise XOR operation between pixel value (A) and the corresponding element of the key (K). and we will get a binary value (B).
3. Covert B back to decimal format. That's the true pixel value/cipher value.

For example, if you want to encrypt the plain text/pixel 24_{10} using Key 32_{10}

1. Convert those numbers into binary format
   $A=[24]_{10}=[00011000]_2$ and $Key=[32]_{10}=[00100000]_2$
2. Apply bitwise XOR operation
   $[00011000]_2$ **XOR** $[00100000]_2 = [00111000]_2$
3. Covert the result back to decimal format
   $B=[00111000]_2=[56]_{10}$

If you want to decrypt the ciphertext B, you will need to follow the same procedure using the same key

1. Convert those numbers into binary format
   $B=[56]_{10}=[00111000]_2$ and $Key=[32]_{10}=[00100000]_2$
2. Apply bitwise XOR operation
   $[00111000]_2$ **XOR** $[00100000]_2 =[00011000]_2$
3. Covert the result back to decimal format
   $A=[00011000]_2=[24]_{10}$

Convert decimal to binary:

Conversion of the decimal number to a binary number can be done by dividing the decimal number by 2 repeatedly until the final result is 0.

For example, if you want to convert 233_{10} to binary, you can follow the conversion table, and the results should be 11101001_2.

Division of Decimal Number by 2	Quotient	Remainder	Binary
233//2	116	1	1 (Least Significant Bit)
116/2	58	0	0
58/2	29	0	0
29/2	14	1	1
14/2	7	0	0
7/2	3	1	1
3/2	1	1	1
1/2	0	1	1 (Most Significant Bit)

If you want to convert the 11101001_2 back to decimal, you can do the following calculation:

$233_{10}=1\times2^7+1\times2^6+1\times2^5+0\times2^4+1\times2^3+0\times2^2+0\times2^1+1\times2^0$

XOR logic gate

The XOR (eXclusive OR) logic gate is one of the common logic gates that are widely used in different types of computational circuits. The rule of output from the XOR gate can be summarized by the truth table below:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0