STEGANOGRAPHY:

Hiding the data into some other form, eg: hinding a text in an image, is called steganography.

This is not an encryption scheme.

In cryptography we convert the message to unintelligible form while here we hid the message.

EXAMPLE:

Hiding text inside text,

Lets say the message is :Simply encrypt correct reading exactly twice.

Here if we look at the first letters of all the words in sentences

Simply ----->> S
encrypt ----->> e
correct ----->> c
reading ----->> r
exactly ------>> e
twice -------->> t

So here the text is hidden in the text.

LSB STEGANOGRAPHY:

LSB means least significant bits. Now lets take a byte (made up of 8 bits).

11111000>>This is a byte which contain 8 bits

So in a byte the value of bits are :

```
128   64  32  16   8   4   2   1
  1   1   0   1   0   0   0   1
```

Now looking to the first bit from left holds the value of 128, second holds 64, thord holds 32, all so on all the way to 1. So making changes to the first bits from left will make a greater change in data compared to the last ones as they hold the lowest values.

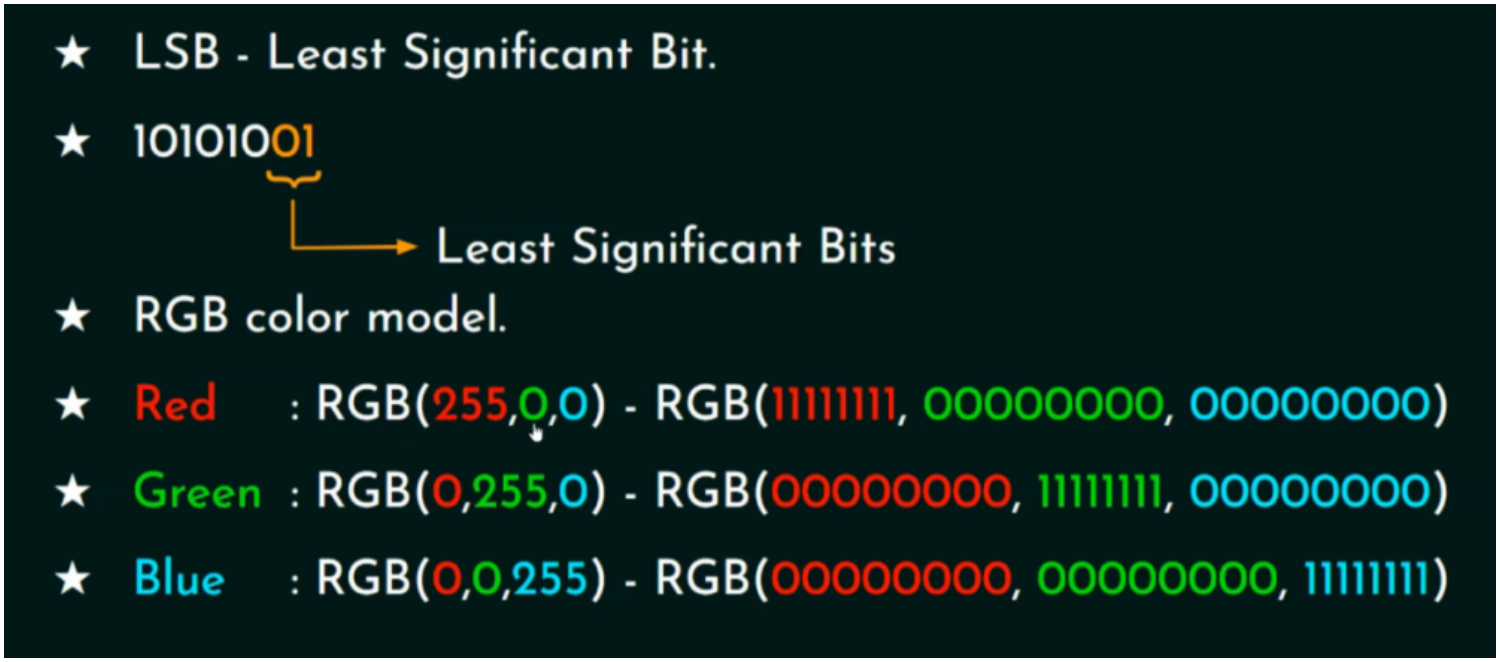
For example :

00000111
10000000

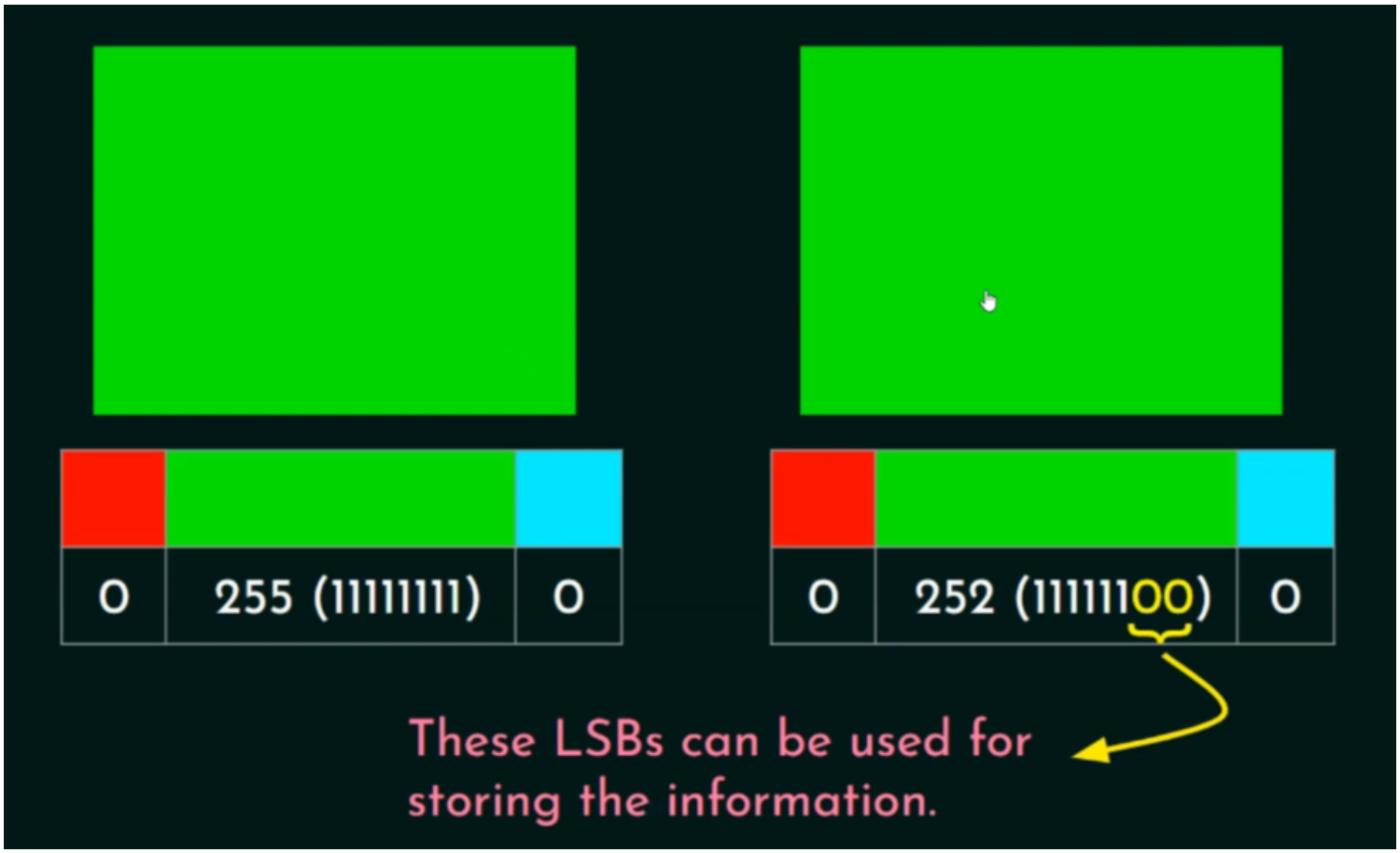
The above are the two bytes. Looking at the first byte there are three ones in the last whose values are, 4, 2, and 1. Now this is the bit representation on the number 7. So making changes to the last 3 bits made seven.

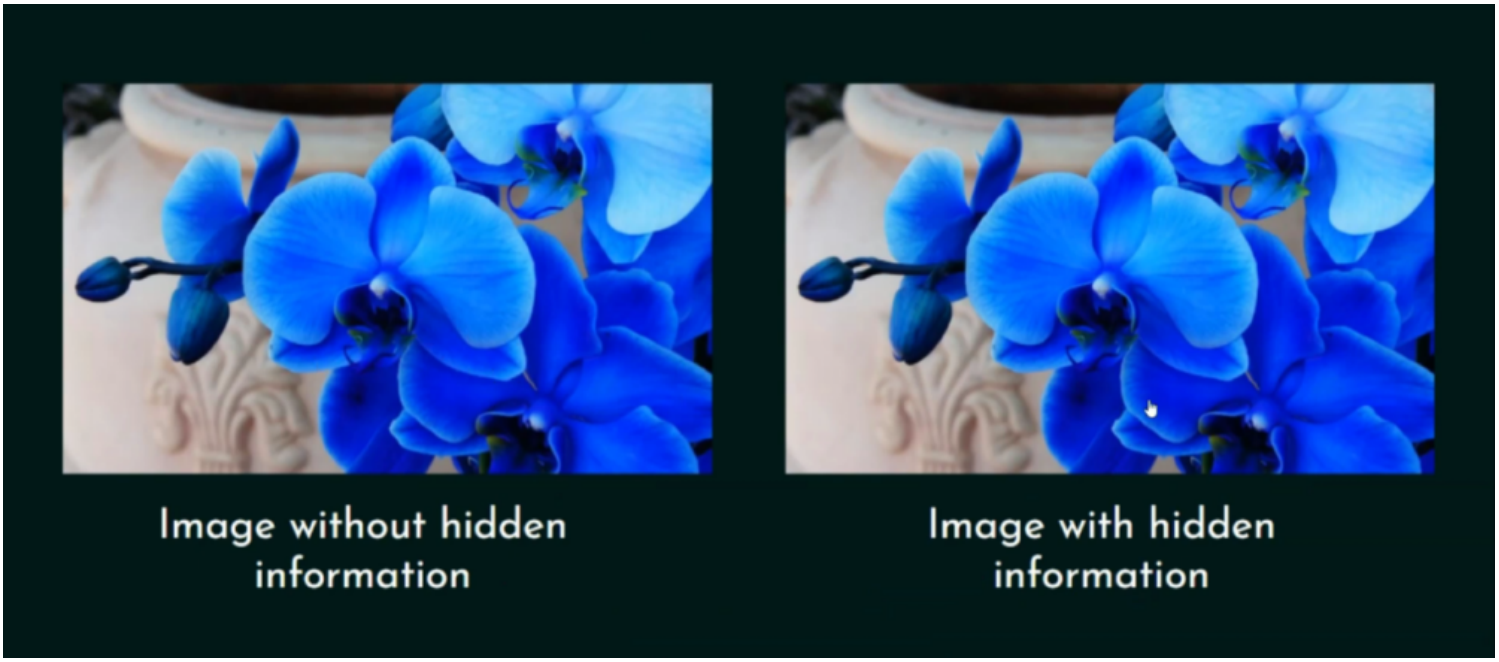
But in the second example, we just made change to the 1st bit and the value returns as zero. So this is the most significant bit.
Shortly, this most significant bit is having a higher value more than 10 times than the 3 bits of LS bits. So thats why these bits are called LSB.

Now if we make use of it to store some data, the form of data will not experience any high change. This is what LSB steganography is, that we store our confidential data in these kind of bits, so that our data is also stored and the real image or whatever we are hiding our data in, that runs on the principles of bits also does not seem that they are changed.



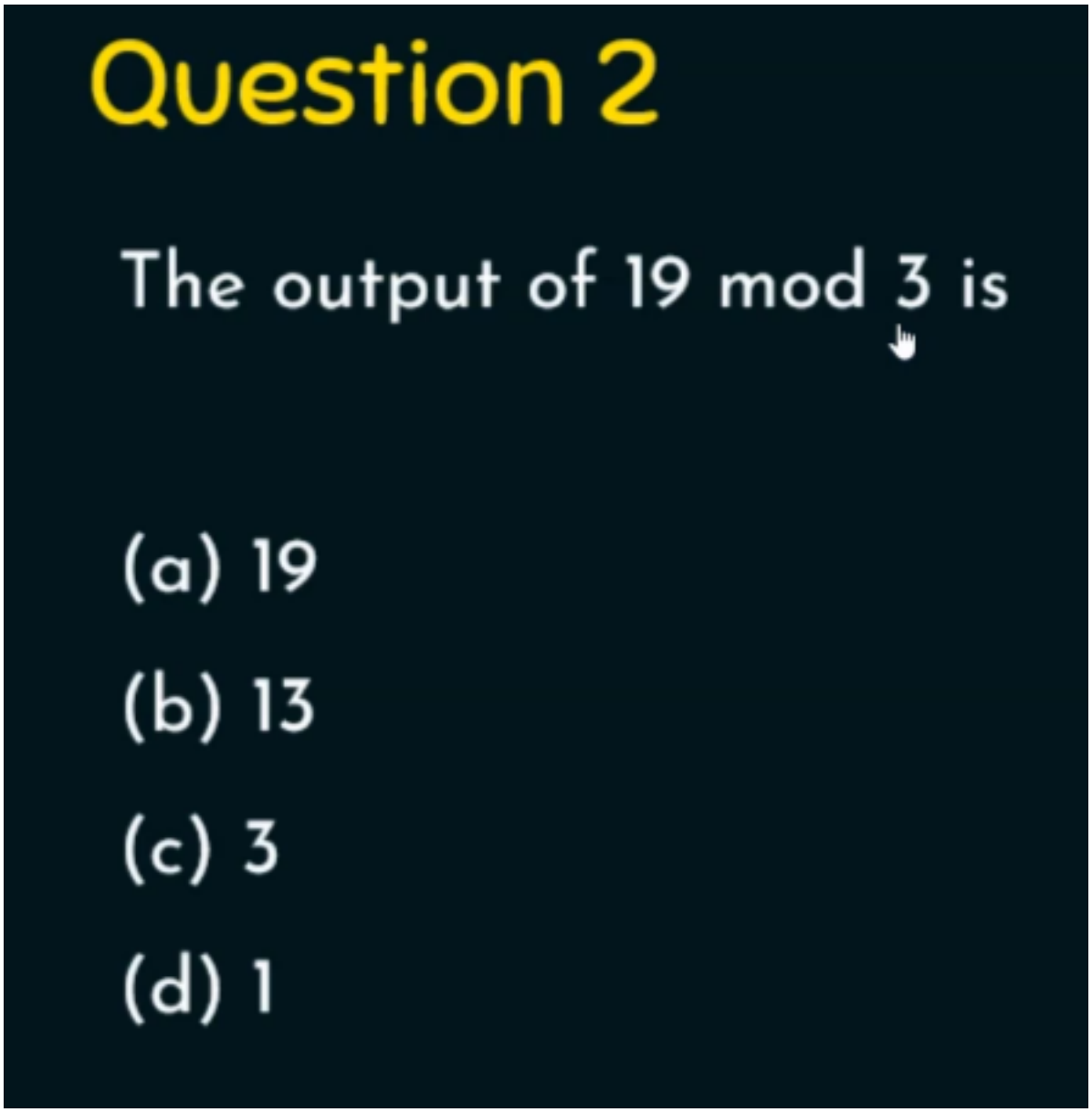
And similarly other color are also produced from RGB by selecting the desired of bits.





We can use softwares like "OpenStego Tool" to perfome steganography.

QUESTIONS ON CRYPTOGRAPHY:



SOLUTION:

Answer is 13 and 1

Quotients = 2, 6.

Question 3

An attacker sits between the sender and receiver and captures the information and retransmits to the receiver after some time without altering the information. This attack is called as _____.

[UGC NET CS 2016]

(a) Denial of Service attack

(b) Masquerade attack

(c) Simple attack

(d) Complex attack

Actually it is a replay attack, but as here is no replay attack option so we are going to search for the closest option, here when the attacker captures the packet, the receiver is denied of the service. The example for this scenario is capturing the handshake file in WPA2 security of WiFi.

The other reason for this to be the closest option is that when the attacker captures the packets and keeps on retransmitting, the target system may get overloaded and face a DOS attack that is the receiver system crashes so he cannot continue any furthur work with it nor receive any legit data.

Question 4

In a columnar transposition cipher, the plain text is "the tomato is a plant in the night shade family", keyword is "TOMATO". The cipher text is

[ISRO CS 2020]

(a) "TINESAX / EOAHTFX / HTLTHEY / MAIIAIX / TAPNGDL / OSTNHMX"

(b) "TINESAX / EOAHTFX / MAIIAIX / HTLTHEY / TAPNGDL / OSTNHMX"

(c) "TINESAX / EOAHTFX / HTLTHEY / MAIIAIX / OSTNHMX / TAPNGDL"

(d) "EOAHTFX / TINESAX / HTLTHEY / MAIIAIX / TAPNGDL / OSTNHMX"

t	o	m	a	t	o
4	3	2	1	4	3
t	h	e	t	o	m
a	t	o	i	s	a
p	l	a	n	t	i
n	t	h	e	n	i
g	h	t	s	h	a
d	e	f	a	m	i
l	y	x	x	x	x

So the correct option is a.

• As two colunms are of value 3 and 2 of 4. So here start from left to right.
• Also the key is extracted from the "TOMATO" keyword by alphabetically conting the alphabets and then assigning them value based on their alphabetical order.
• Like a comes first in alphabetical order, then b, then c but here as they are not present so we assign that to m as like this number all the aphabets in the keyword.

Question 5

Suppose that everyone in a group of N people wants to communicate secretly with the N - 1 others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is

[GATE CS 2015]

(a) 2N

(b) $N(N-1)$

(c) $\frac{N(N-1)}{2}$

(d) $(N-1)^2$

No of people	Keys
1	0
2	1
3	3
4	6
5	10