

## Day 31, Cryptology and Steganography

### Lock Box Example

Cryptology is the study of codes, both creating and solving them.

Cryptography is the art of creating codes, or encryption.

Cryptanalysis is the art of breaking codes, or decryption

(<https://militaryembedded.com/comms/encryption/cryptology-cryptography-and-cryptanalysis#:~:text=Cryptology%20is%20the%20study%20of,the%20art%20of%20creating%20codes>).

So, Cryptology = Cryptography + Cryptanalysis.

For the codes to be useful, they should be relatively easy to encrypt messages, but very difficult to decrypt for those the messages are NOT intended for (and of course relatively easy to decrypt for the those the message IS intended for). They should be **invertible**.

Many of the techniques we will discuss rely on modular arithmetic. Consider the following:

*When **N** items in a basket are removed 5 at a time, ultimately none remain. However, if these **N** items are removed 2 at a time, then 1 remains. If removed 4 at a time, then 3 remain. What is the smallest possible value of **N**?*

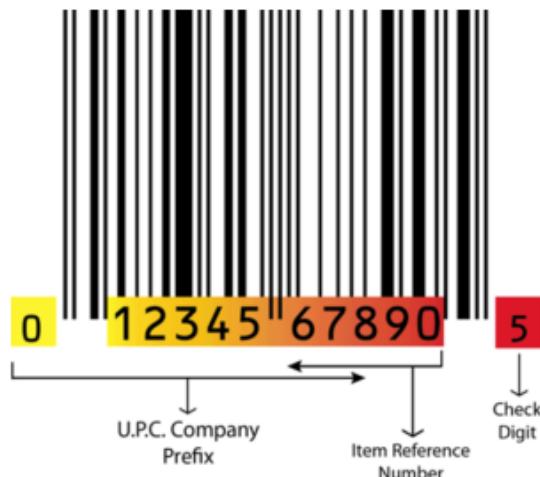
First, write this scenario mathematically, using appropriate symbols:

$$\begin{array}{llllllllll} N \% 5 = 0 & \rightarrow & 5 & 10 & 15 & 20 & 25 & 30 & 35 & 40 & \dots \\ N \% 2 = 1 & \rightarrow & 5 & 10 & 15 & 20 & 25 & 30 & 35 & 40 & \dots \\ N \% 4 = 3 & \rightarrow & 5 & 10 & 15 & 20 & 25 & 30 & 35 & 40 & \dots \end{array}$$

What would be the next smallest value of **N** which satisfies the above conditions? Can you explain this?

For another example of modular arithmetic, let's consider the Universal Product Codes (UPC) we are so familiar with when scanning items we are purchasing. The most widely used barcode in the US retail industry is the UPC-A or UPC-12, an example of which is shown below

(<https://www.createbarcodes.com/create-upc-barcode>).



The check digit is calculated using a formula based on modular arithmetic. You take all the digits in odd positions (the positions start at 1), sum them, and multiply that sum by 3. Add to this the digits in the even positions, except for the last digit. For this sum, “mod” it with 10. If it is not 0, subtract this from 10. That should be the check digit.

Following this algorithm on the example above:

$$\begin{aligned} 3 * (0 + 2 + 4 + 6 + 8 + 0) &= 3 * (20) = 60 \\ 1 * (1 + 3 + 5 + 7 + 9) &= 25 \\ \rightarrow (60 + 25) \% 10 &= 85 \% 10 = 5 \quad \rightarrow 10 - 5 = 5 \end{aligned}$$

For more on check codes, you can read: [https://www.barcode.graphics/gtin-12/?srsltid=AfmBOoolJ\\_6D-cCpc16BtfgNgbOl-icmWxIbToLOU6fmG0vCKDRWSuX](https://www.barcode.graphics/gtin-12/?srsltid=AfmBOoolJ_6D-cCpc16BtfgNgbOl-icmWxIbToLOU6fmG0vCKDRWSuX)

Calculate the check digit for the following UPC-12 code?

0 89126 74350   ?

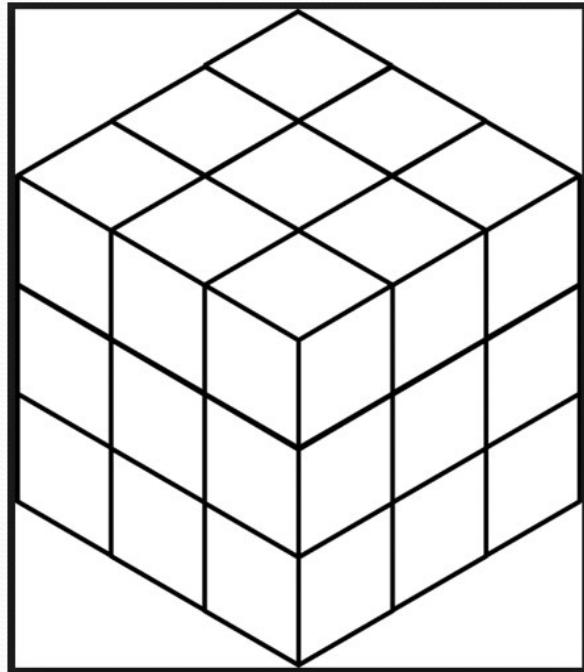
$$\begin{aligned} 3 * (0 + 9 + 2 + 7 + 3 + 0) &= 3 * (21) = 63 \\ 1 * (8 + 1 + 6 + 4 + 5) &= 24 \\ \rightarrow (63 + 24) \% 10 &= 87 \% 10 = 7 \quad \rightarrow 10 - 7 = 3 \end{aligned}$$

Besides overtly encrypting a secret message, another approach is “hiding in plain sight,” or **Steganography**. One of the first examples of this was from Julius Caesar. He would have a messenger shave their head, the message was tattooed on their head, and when their hair grew back, they were sent to deliver it. Not super timely, but pretty effective.

## Steganography – Hiding in Plain Sight

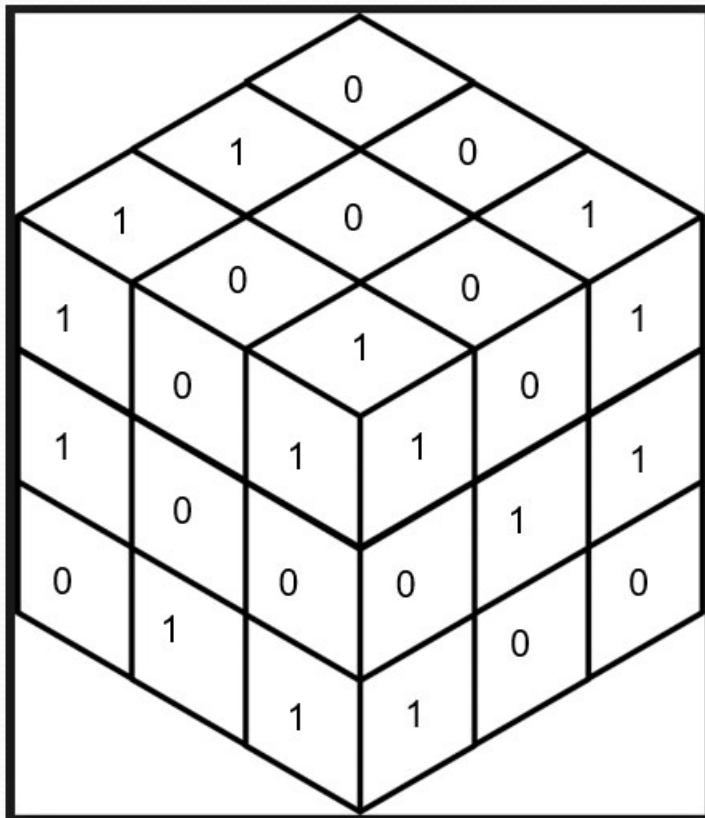
- 1) Whisper a message...
- 2) Did you want to get in on the “secret message?”
- 3) If no one knows that you are sending a message, then they are less likely to pay attention to your communications.
- 4) A technique Julius Caesar used to send messages.

## Steganography – Hiding in Plain Sight



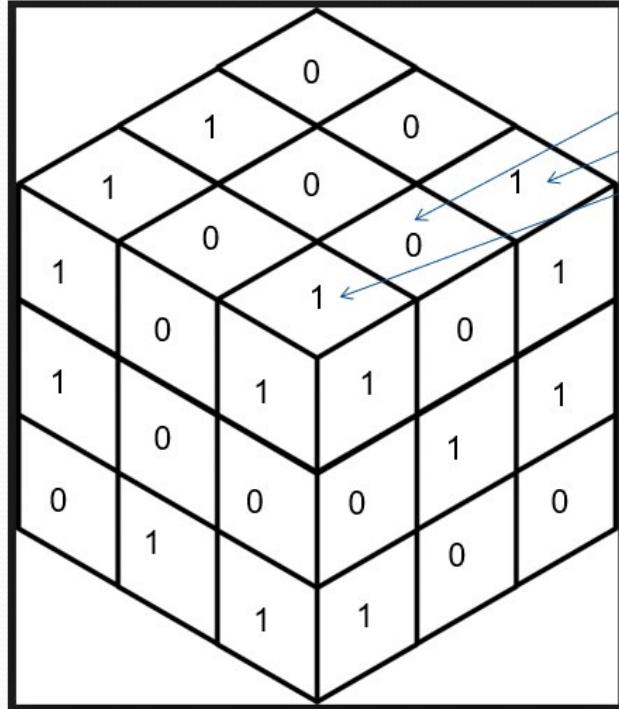
## Steganography – Hiding in Plain Sight

Consider this representation of an image



## Steganography – Hiding in Plain Sight

Consider this representation of an image

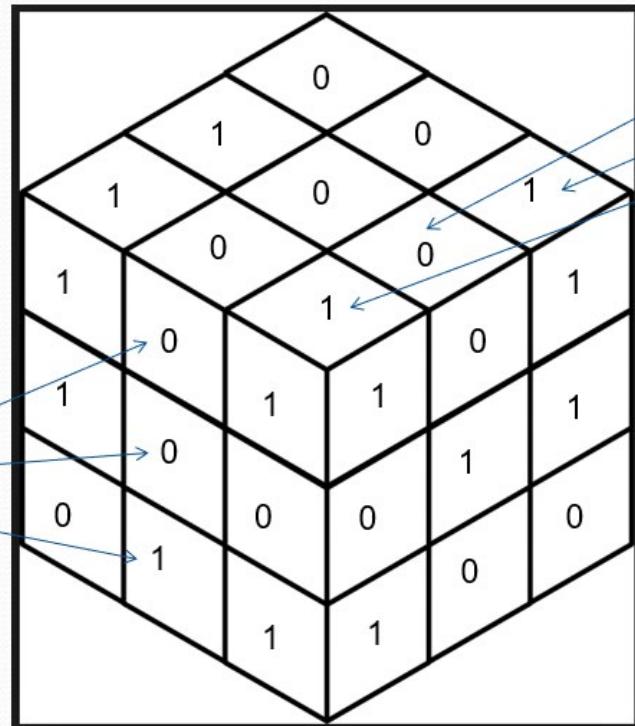


Each "column" is one pixel

## Steganography – Hiding in Plain Sight

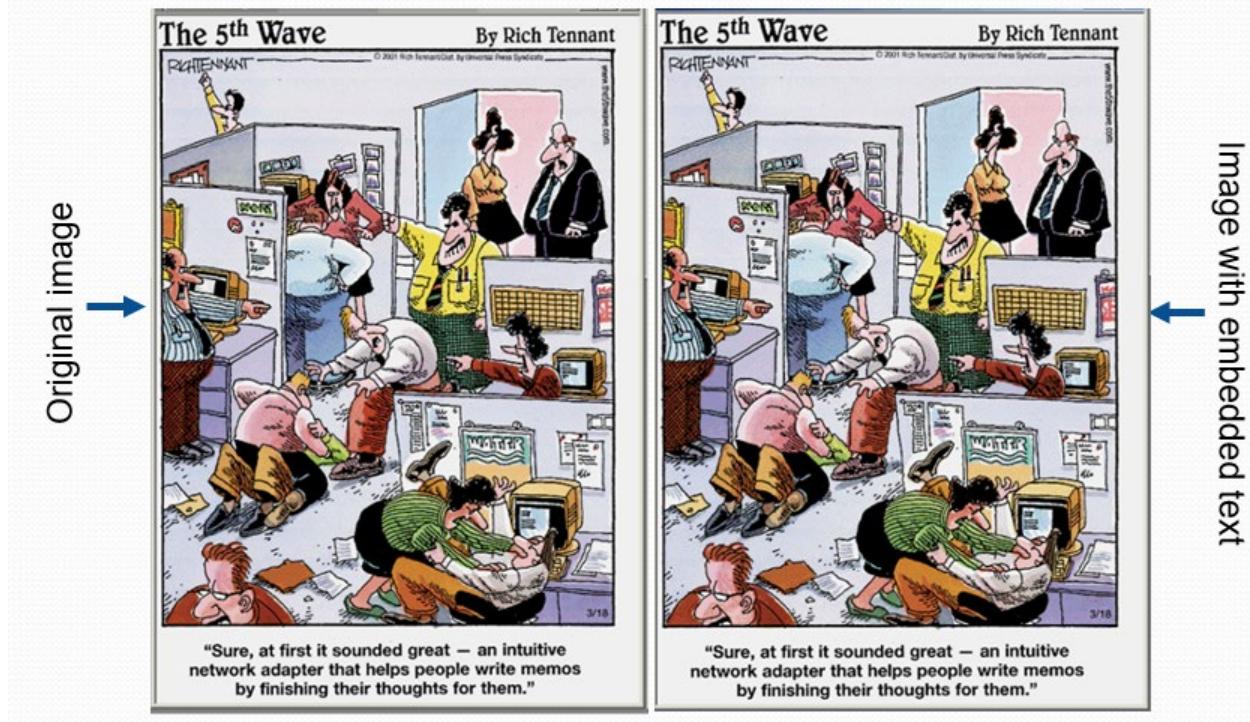
Consider this representation of an image

If each color is 8 bits, then there would be 8 "layers"

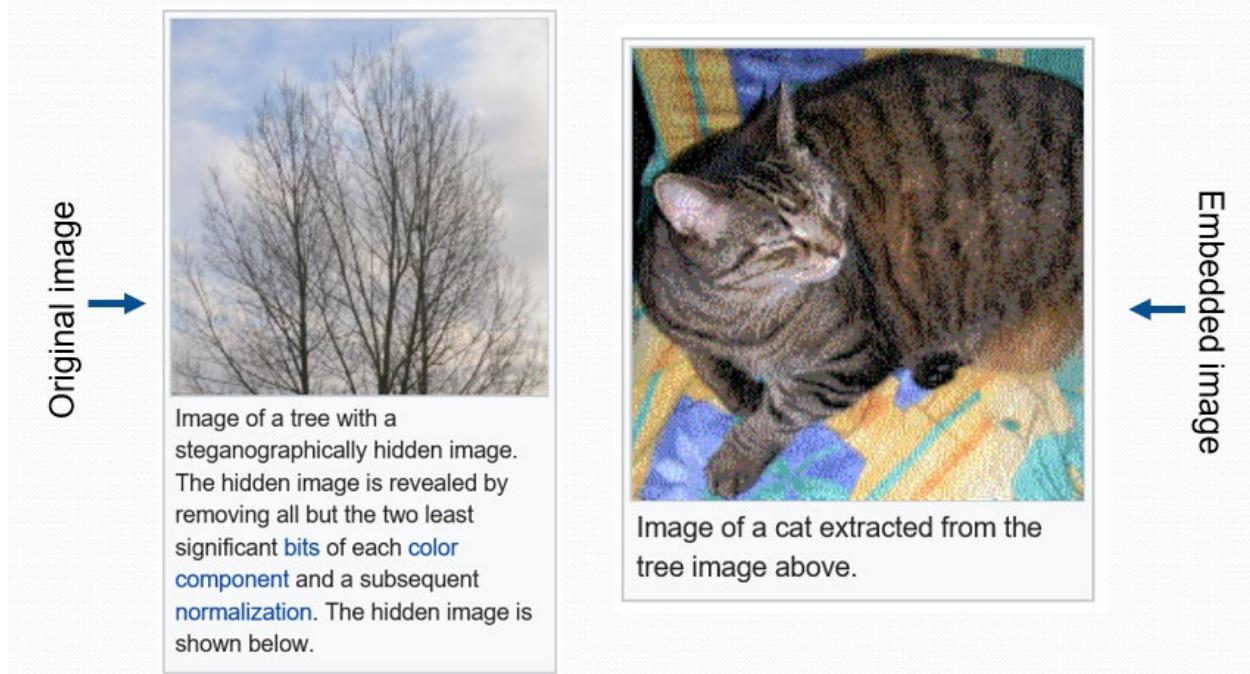


Each "column" is one pixel

If you remove the least significant “layer” of each pixel, and replace it with a message, the image doesn’t change much



If you remove the least significant “layer” of each pixel, and replace it with a message, the image doesn’t change much



# faculty.juniata.edu/kruse

<http://jcsites.juniata.edu/faculty/kruse/>

Gerald Kruse's Home Page

<https://jcsites.juniata.edu/faculty/kruse/>

Gmail YouTube Maps Imported

Gerald W. Kruse, Ph. D.

green dot

John '54 and Irene '58 Dale Professor of Information Technology, Computer Science, and Mathematics  
Department of Mathematics and Department of Information Technology & Computer Science  
Juniata College

[These Are A Few of My Favorite Links](#)

If I have agreed to write you a letter of recommendation:  
[Instructions for Recommendations](#)

Helpful advice on summer research and graduate school in Computer Science:  
[Computing Community Consortium](#)

Where our IT-CS students end up:  
[IT-CS Department Post Graduation Placements](#)

Fall 2023 Courses:

Course Number	Course Title	Course Syllabus
MA 116 and CS 116 (4 credits w/QS)	Discrete Structures	<a href="#">MA 116 syllabus</a>
Computer Science 315	Analysis and Algorithms	<a href="#">CS 315 syllabus</a>
CS 480 / 481	CS and IT Seminar	<a href="#">CsItSeminar syllabus</a>
IT 496		
CS 485	CS and IT Research	<a href="#">CsItResearch syllabus</a>
IT 497		



## Source code for jcsites.juniata.edu/faculty/kruse

view-source:https://jcsites.juniata.edu/faculty/kruse/

Gmail YouTube Maps Imported

Line wrap

```
<!DOCTYPE PUBLIC "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
<meta http-equiv="Content-Type"
      content="text/html; charset=iso-8859-1">
<meta name="GENERATOR"
      content="Mozilla/4.76 [en] (WinNT; U) [Netscape]">
<title>Gerald Kruse's Home Page</title>
</head>
<body text="#000000" bgcolor="#ffffff" link="#1010ff" vlink="#800080"
alink="#ff0000" face="Times New Roman">
![Kruske_Gerald.JPG](Kruske_Gerald.JPG)
<font face="Times New Roman"><font color="#000080"><font size="3">Gerald
W. Kruse, Ph. D.</font></font><font border="0" height="55" width="55">
![GreenDot.gif](GreenDot.gif)
```