**CHAPTER 1**

1. 10 - a:

The Germans knew their enigma was broken, it might not do well to stop all communication with the machines. Perhaps they could purposely obstruct the allies with faulty info using the enigma. Or another approach could be they go with the scorch earth method and cease all communications with the machine since the main point of the machine was defunct.

b:

The Nazis may have continued to use the Enigma because they did not know it had been cracked. The allies were very secretive about the whole project and great care was taken into not letting the Germans know that they had broken the enigma. Also, the Germans may have known it that it was broken but perhaps not to what extent. They maybe thought that changing a few pads or code books was sufficient. Another reason why they would continue to use it is they didn’t have another cryptography solution for their communications. I think it would be worse to have no replacement.

1. a:

Depending on what your organization is and what it’s doing, then certain aspects might be more important. If for example you were a part of a top-secret project where the information is very important, then confidentiality would be the most important thing, and something like “availability” would take a backseat. However, on the flip side if you are doing something that is supposed to save life’s like emergency broadcasts or other things like that, it would be best to take availability a little bit more seriously.

b:

Some situations where strengthening one thing might weaken another could be if you make your users have very complex passwords, you’re strengthening the integrity of the system but weakening the availability or vice versa. Another situation could be a system where no one except a select few knows how it really works, the confidentiality of it would be very strong but could you as a user trust the validity of your info? You just have to blindly trust the system for it to work, open source software/systems could be an answer to that problem.

**CHAPTER 2**

1. 8 - a:

The terms confusion in cryptography means basically the amount of “obscuring” happening in between the plaintext and the cipher text. While the term diffusion means “spreading” the stats of the plaintexts “through” the cipher.

b:

The classic cipher which employs only confusion is a simple substitution cipher and a one-time pad.

c:

The classic cipher which employs only diffusion is a double transposition.

d:

The cipher which employs both is DES

1. 19 -

a.

The key for thrill is

t h r i l l

plain 111 001 101 010 100 100

key 100 010 000 100 000 100

cipher 011 010 101 110 100 000

K I T L K E

b.

The key for tiller is

t i l l e r

plain 111 010 100 100 000 101

key 100 000 001 010 100 101

cipher 011 010 101 110 100 000

K I T L K E

29 –

1. a:

2^40th

b:

She would know if the cipher text is readable and looks like plaintexy and depending on how long the ciphertext is, the chances of it being a false alarm would be pretty low.

c:

The amount of work needed would be unfeasible

d:

1. a: The keyspace is 2^10

b:

c: