Name: Whitney Chng
UOWNo: 6956865
TutGrp: T01

csci262 Assignment 2

Q1

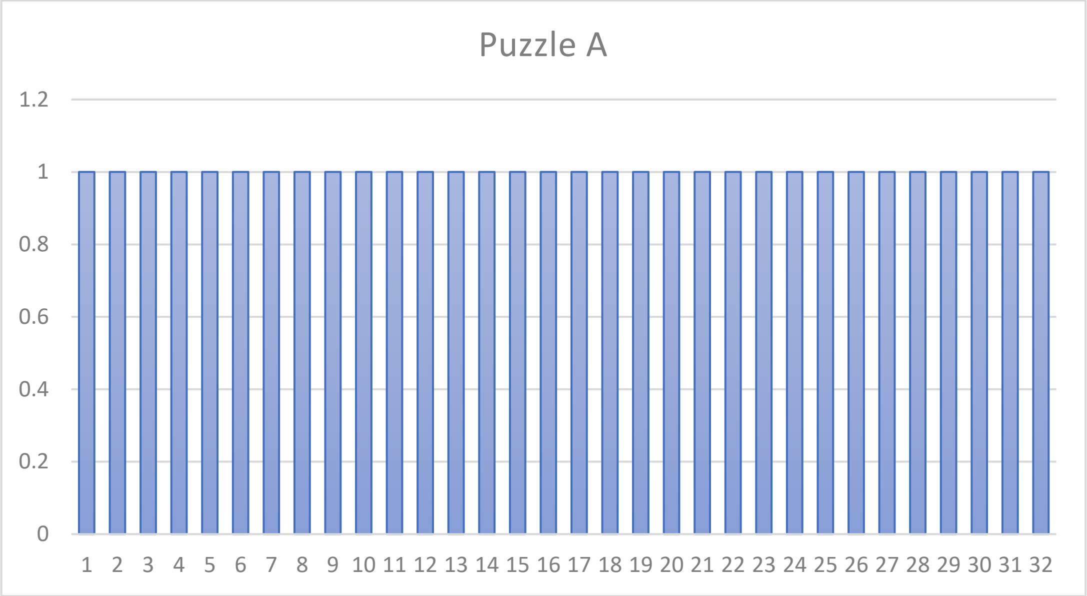
a)

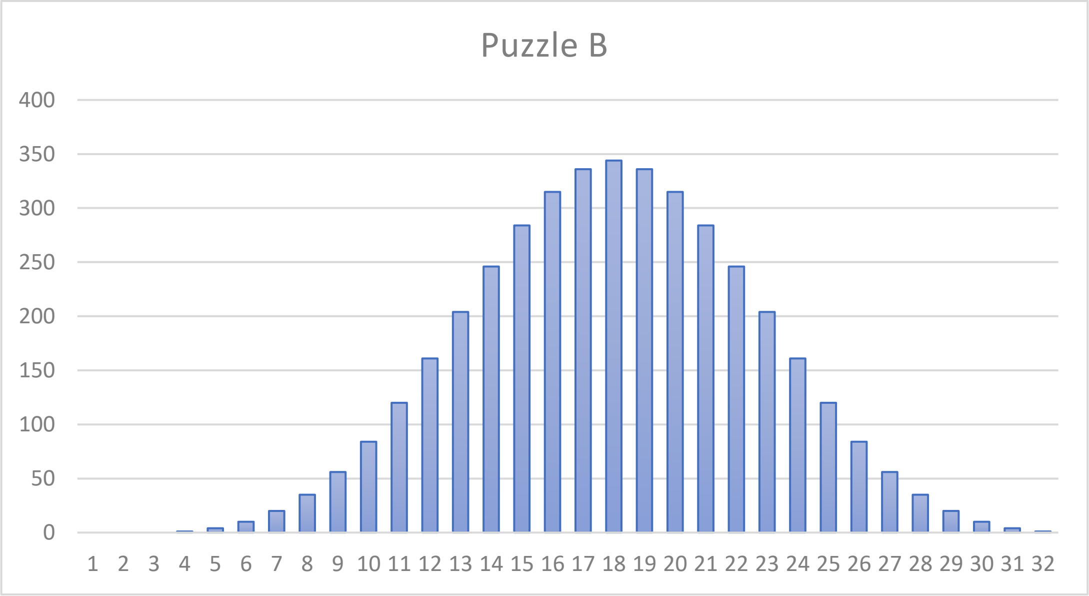
No. of hash	Puzzle A	Puzzle B
1	1	0
2	1	0
3	1	0
4	1	1
5	1	4
6	1	10
7	1	20
8	1	35
9	1	56
10	1	84
11	1	120
12	1	161
13	1	204
14	1	246
15	1	284
16	1	315
17	1	336
18	1	344
19	1	336
20	1	315
21	1	284
22	1	246
23	1	204
24	1	161
25	1	120
26	1	84
27	1	56
28	1	35
29	1	20
30	1	10
31	1	4
32	1	1

b) I wrote a python program that calculates the number of frequencies based on the number of hashes needed. The program consists of nested for loops which firstly loops through 32 hashes in total first and then loops from 1-8 four times in total. The last loop will then calculate the total value and then check if this sum equals to a variable called "x". If true, the frequency counter will increase.

Name: Whitney Chng
UOWNo: 6956865
TutGrp: T01 **csci262 Assignment 2**

c)





d)

Avg no. of hashes

Puzzle A :

worst no. of hashes : $m \times 2^k$

$= 1 \times 2^5$

$= 32$

avg. hashes : $\dfrac{\frac{n(n+1)}{2}}{n}$

$= \dfrac{\frac{32(32+1)}{2}}{32}$

$= \dfrac{528}{32}$

$= 16.5$ hashes #

Puzzle B:

worst no. of hashes : $m \times 2^k$

$= 1 \times 2^3$

$= 8$

avg. hashes : $\dfrac{\frac{n(n+1)}{2}}{n}$

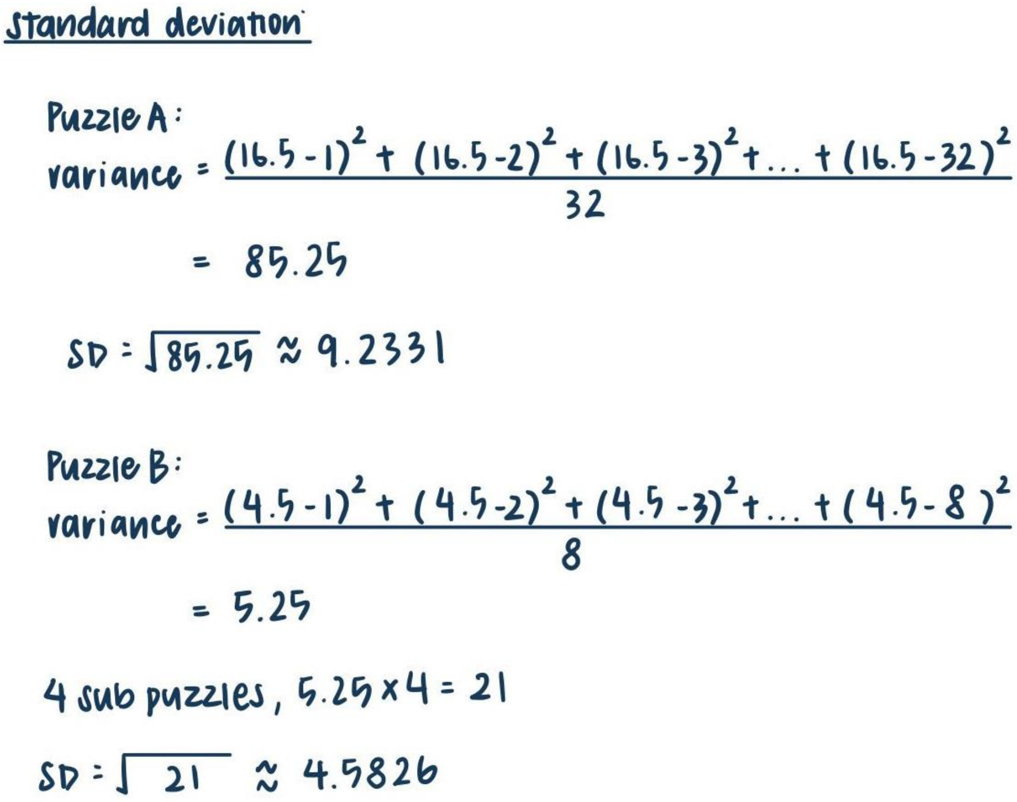
$= \dfrac{\frac{8(8+1)}{2}}{8}$

$= \dfrac{36}{8}$

$= 4.5$

There are 4 sub-puzzles so $4.5 \times 4 = 18$ hashes #

e)



Standard deviation

Puzzle A:

$$\text{variance} = \frac{(16.5-1)^2 + (16.5-2)^2 + (16.5-3)^2 + \ldots + (16.5-32)^2}{32}$$

$$= 85.25$$

$$SD = \sqrt{85.25} \approx 9.2331$$

Puzzle B:

$$\text{variance} = \frac{(4.5-1)^2 + (4.5-2)^2 + (4.5-3)^2 + \ldots + (4.5-8)^2}{8}$$

$$= 5.25$$

4 sub puzzles, $5.25 \times 4 = 21$

$$SD = \sqrt{21} \approx 4.5826$$

Q2

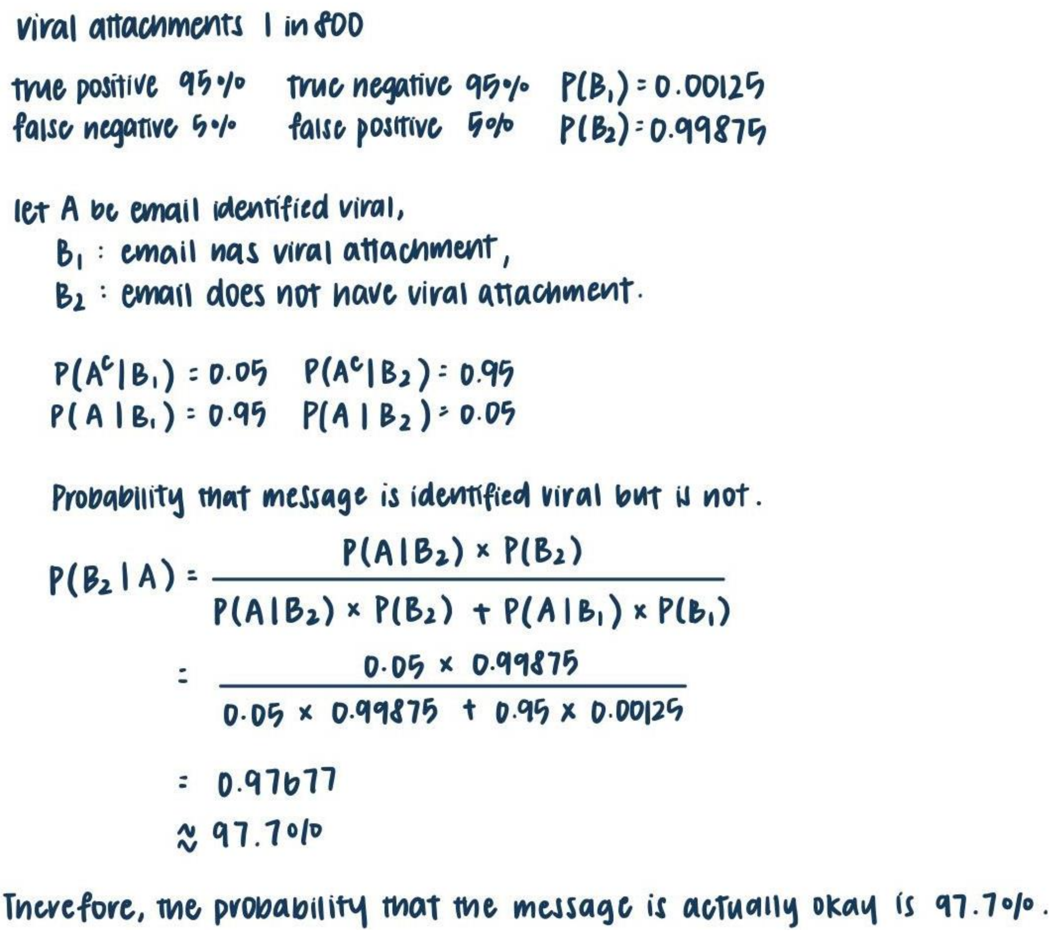
Original code violated “default deny, not default allow” principle. Because it is only checking if the user is not granted access before stopping it fromm running the function.

Modified pseudo-code:

```
permit = CheckAccess( )
IF (permit == Access Granted)
    Print “Access Granted”
    Run Function( )
ELSE
    Print “Access Denied”
```

Name: Whitney Chng
UOWNo: 6956865
TutGrp: T01 **csci262 Assignment 2**

Q3



viral attachments 1 in 800

true positive 95% true negative 95% $P(B_1) = 0.00125$
false negative 5% false positive 5% $P(B_2) = 0.99875$

let A be email identified viral,
B_1 : email has viral attachment,
B_2 : email does not have viral attachment.

$P(A^c | B_1) = 0.05$ $P(A^c | B_2) = 0.95$
$P(A | B_1) = 0.95$ $P(A | B_2) = 0.05$

Probability that message is identified viral but is not.

$$P(B_2 | A) = \frac{P(A|B_2) \times P(B_2)}{P(A|B_2) \times P(B_2) + P(A|B_1) \times P(B_1)}$$

$$= \frac{0.05 \times 0.99875}{0.05 \times 0.99875 + 0.95 \times 0.00125}$$

$$= 0.97677$$

$$\approx 97.7\%$$

Therefore, the probability that the message is actually okay is 97.7%.

Q4 IT Administrator caused $800,000 in damages to his former company

Former employee, Charles E. Taylor was first hired as a system administrator for a wholesaler that specializes in lumber and building materials. He used his knowledge to remotely log into the company's network with encryption to hide himself from the system's security. He then used this opportunity to change router passwords which are being utilized in many of the company's warehouses. Following the first attack, Taylor issued a shutdown command to cripple the company's central communication system. This affected the customer ordering procedure and caused employees to take orders through traditional methods by using their personal phones to contact.

Taylor did not need to implement a big malware because he was already knowledgeable about the company's information so he just had to take this knowledge into his advantage and had to only implement a hack which will not be easily detected by the security system.

Outcome:

The expected impact of this attack is significant sum of money lost due to the inability to recover communication systems and the lack of sales. Taylor's actions caused a $800,000 damage to his former company. The routers had to be replaced at a cost of $100,000 and the company's IT team needed two days to resolve and restore the communication server and network and this costed more than $700,000.

Taylor launched this attack back in 2018 and after some jail term, supervised release, and home detention, he finally pleaded guilty and was convicted of computer fraud in 2020.

Name: Whitney Chng
UOWNo: 6956865
TutGrp: T01

csci262 Assignment 2

Q5

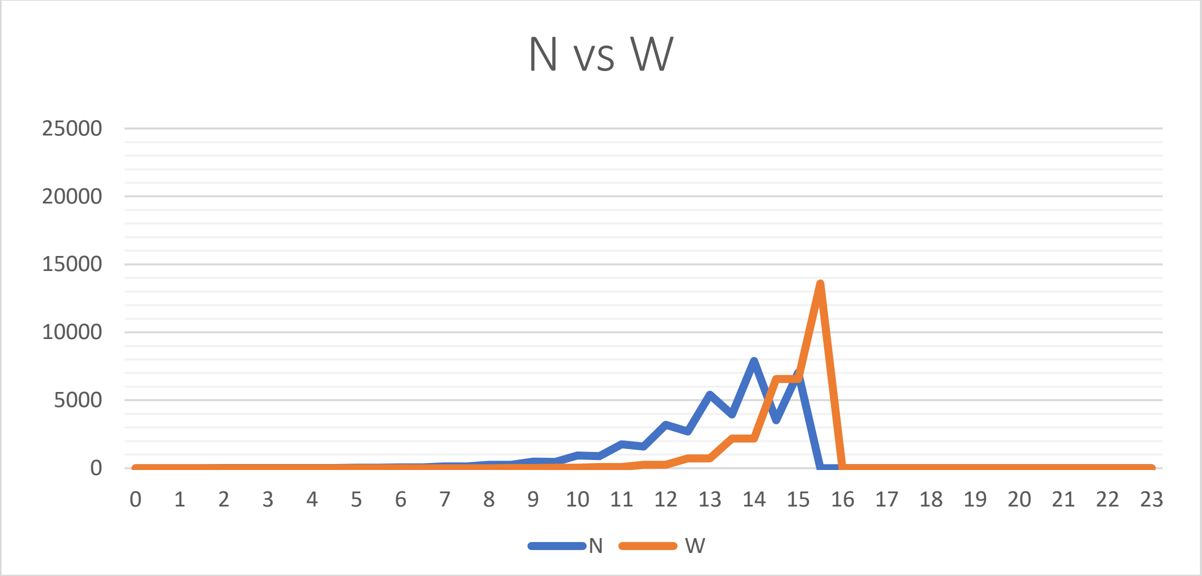
a)

Time	N
0	1
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	2048
12	4096
13	8192
14	16384
15	32768
16	65536
17	131072
18	262144
19	524288
20	1048576
21	2097152
22	4194304
23	8388608

b)

Time	N	W
0	1	0
0.5	1	0
1	2	0
1.5	2	0
2	4	0
2.5	4	0
3	8	0
3.5	8	0
4	16	0
4.5	16	0
5	32	0
5.5	32	0
6	64	0
6.5	63	1
7	126	1
7.5	124	3
8	248	3
8.5	242	9
9	484	9
9.5	466	27
10	932	27
10.5	878	81
11	1756	81
11.5	1594	243
12	3188	243
12.5	2702	729
13	5404	729
13.5	3946	2187
14	7892	2187
14.5	3518	6561
15	7036	6561
15.5	0	13597
16	0	0
16.5	0	0
17	0	0
17.5	0	0
18	0	0
18.5	0	0
19	0	0
19.5	0	0
20	0	0
20.5	0	0
21	0	0
21.5	0	0
22	0	0
22.5	0	0
23	0	0

c)



Because counter worm W spreads to two X infected hosts provided such hosts are available, W will stop spreading at 16 because at 15.5, W has cleaned all infected hosts and there are none to clean afterwards.

d) When we infer to the graph plotted above, at t = 9, there are already 484 infected computers and W has only cleaned 9 computers. In the case where X evolves, X infects computers at a much faster rate and W will not be able to keep up with the exponential increase of infection. In conclusion, there is no stopping of the infection from X.

Q6

(a) An XML bomb is a message that is created to crash or hang a program that runs it. It is usually sent into a HTTP server. It works by utilizing the XML parser to process the XML bomb, from this the data will start feeding on itself and grows exponentially. The nature of this attack is to shutdown a website or Internet Service Provider.

(b) Bluesmack is an attack that is directed to Bluetooth enabled devices. It is similar to ping flood as it utilizes L2CAP ping to transfer an oversized packet to these devices to overloads it, resulting in degrading the performance of the device such as crashing the device due to overload or even making the device unusable.

(c) Mydoom is one of the most destructive computer viruses that exists and mainly affects Windows Operating Systems. It is a viral worm that travels easily through computer systems through emails. This virus will collect email addresses from the infected windows device and then sending a new version of itself to victims as an attachment. Once opened, their device will be infected and the cycle repeats. This virus protects itself by preventing users from running their anti-virus software. It is a Distributed Denial of Service (DDoS) attack.

(d) Torpig is a type of robot network that spread through systems that were compromised by Mebroot (a Trojan horse that can hide itself from the user). It mainly targets computers that run on Windows Operating Systems and as more devices get infected, it will form a network of infected computers that are under control of single attacking parties. This virus usually scans the system for important information such as accounts, passwords, credit cards etc. It is also capable of modifying data on the computer, web pages, and transactional information.

References:

Ferguson, S., & Ross, R. (n.d.). *Former IT administrator sentenced in insider threat case*. Bank Information Security. Retrieved November 6, 2021, from https://www.bankinfosecurity.com/former-administrator-sentenced-in-insider-threat-case-a-14358.