CSCI262 Assignment 2

# Q1

## a.

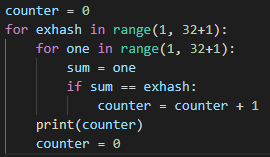
Puzzle A: Puzzle B:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Expected hash ( E ) | Frequency ( F ) |  | Expected hash ( E ) | Frequency ( F ) |
| 1 | 1 |  | 1 | 0 |
| 2 | 1 |  | 2 | 0 |
| 3 | 1 |  | 3 | 0 |
| 4 | 1 |  | 4 | 1 |
| 5 | 1 |  | 5 | 4 |
| 6 | 1 |  | 6 | 10 |
| 7 | 1 |  | 7 | 20 |
| 8 | 1 |  | 8 | 35 |
| 9 | 1 |  | 9 | 56 |
| 10 | 1 |  | 10 | 84 |
| 11 | 1 |  | 11 | 120 |
| 12 | 1 |  | 12 | 161 |
| 13 | 1 |  | 13 | 204 |
| 14 | 1 |  | 14 | 246 |
| 15 | 1 |  | 15 | 284 |
| 16 | 1 |  | 16 | 315 |
| 17 | 1 |  | 17 | 336 |
| 18 | 1 |  | 18 | 344 |
| 19 | 1 |  | 19 | 336 |
| 20 | 1 |  | 20 | 315 |
| 21 | 1 |  | 21 | 284 |
| 22 | 1 |  | 22 | 246 |
| 23 | 1 |  | 23 | 204 |
| 24 | 1 |  | 24 | 161 |
| 25 | 1 |  | 25 | 120 |
| 26 | 1 |  | 26 | 84 |
| 27 | 1 |  | 27 | 56 |
| 28 | 1 |  | 28 | 35 |
| 29 | 1 |  | 29 | 20 |
| 30 | 1 |  | 30 | 10 |
| 31 | 1 |  | 31 | 4 |
| 32 | 1 |  | 32 | 1 |

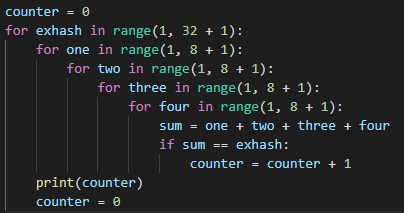
## b.

I created a for loop to loop within the range of the size of the bit-string from the requirements of the puzzle and in each loop for the number of sub puzzles in the puzzle.

Puzzle A:

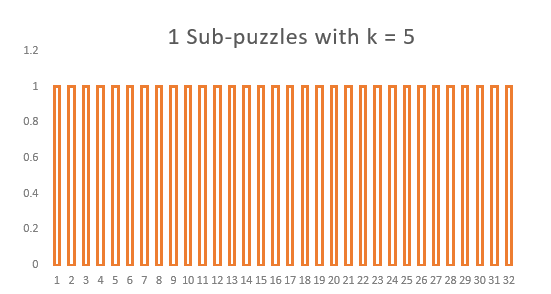


Puzzle B:

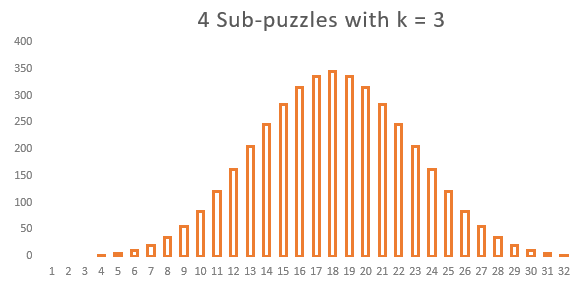


## c.

Puzzle A:

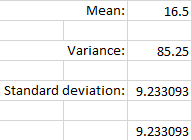
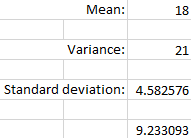


Puzzle B:



## c. and d.

Puzzle A Puzzle B

# Q2.

The original code allows the default output to grant access to the user. This fails the default deny principle of general secure coding. The code should base access decisions on permission rather than exclusion, hence allowing the default output to be an access denied message to prevent any unauthorised access to ensure security.

The amended pseudocode should be as follows:



# Q3.

# Q4. Former Cisco employee purposely damaged cloud infrastructure.

A former Cisco employee, Sudhish Kasaba Ramesh, gained unauthorized access to the company's cloud infrastructure and used malicious malware to remove 456 virtual machines that were utilized by Cisco's Webex Teams service. As a result, some 16,000 Webex customers were unable to access their accounts for two weeks.

**The Impact and the Malware**

He entered Cisco's AWS cloud infrastructure without authorisation a few months after resigning from the tech giant and deployed malicious code from his Google Cloud Project account that erased 456 virtual machines related with the Cisco Webex Teams application, which offered video conferencing, video chat, file sharing, and other collaboration features. The malware was highly an injection script instructed to shut down and delete the files and machines on the cloud infrastructure. He further stated that in deploying the code, he behaved carelessly and wilfully ignored the significant danger that his actions may hurt Cisco.

**Outcome of Cisco and Ramesh**

Cisco spent roughly $1,400,000 in staff time to repair the damage to the system and reimburse over $1,000,000 to impacted customers after Webex Teams accounts were shut down for up to two weeks. However, no consumer data was compromised.

On July 13, 2020, Ramesh was charged with one count of Intentionally Accessing a Protected Computer Without Authorization and Recklessly Causing Damage. On 9th December 2020, he was sentenced to 24 months in prison. In addition to the prison sentence, he is sentenced to a one-year period of supervised release and a $15,000 fine. His sentence begins on 10th February 2021.

# Q5.

# Q6

## XML Bomb

XML Bomb is a type of Denial-of-Service attack that affects a website's availability. The eXtensible Markup Language (XML) is a markup language that was created for the purpose of storing and transmitting structured data. Before being processed, data files might be examined by a parser library. The validation and comparison criteria for the type of data that occurs in the XML file are then performed using XML schemas and Document Type Definitions (DTDs) files. When the parser library is not configured properly, inline DTDs can be misused, resulting in an XML bomb, also known as an Entity Expansion XML bomb. The "Billions Laugh Effect" is a well-known XML bomb example. This form of attack can list entity definitions in a densely layered XML file, resulting in parsing and extremely huge files. Because these processed XML files are so huge, they might cause a server to crash.

## BlueSmack

BlueSmack is a type of DoS attack that targets Bluetooth-enabled devices and the Bluetooth protocol specifically. It's comparable to the Windows 95's 'Ping of Death' exploit, in which a l2ping data packet (approximately 600 bytes) is sent to a Bluetooth device with a larger maximum packet size. This renders the gadget inoperable and has the potential to deplete the device's battery. The l2ping packet is included in the BlueZ utility package that comes standard with Linux.

## Mydoom

Mydoom is a type of computer worm that was found in 2004 and distributed by email, affecting Microsoft Windows PCs. It attacked PCs by copying itself to shared folders on P2P KaZaA clients, and its payload included a backdoor Remote Access component on TCP port 3127. The worm was able to gather email addresses from the system and then deliver itself as an attachment from the host email server using SMTP protocols. Mydoom's original edition is the fastest-growing spam email worm ever discovered, and it has also been found to avoid sending itself to particular domain addresses, including Rutgers, MIT, Stanford, UC Berkeley, Microsoft, and Symantec. Other worm variants were then created to employ infected hosts as zombies in a Distributed Denial-of-Service assault against the SCO Group and Microsoft.

## Torpig

Torpig is a botnet that targets Windows-based computers. It attacks users by masquerading as a Trojan horse and installing the Mebroot rootkit via a drive-by-download server. The Mebroot rootkit changes the infected system's Master Boot Record (MBR), which subsequently installs the rootkit when the system is rebooted. The virus updates its modules by communicating with a Command and Control (C&C) server through HTTP via an encrypted protocol. Computers that have been infected become members of the botnet. Torpig is a type of spyware that compromises the integrity and security of systems by examining data from impacted applications (such as Service Control Managers, email clients, the file manager, and others) in order to collect online account and password details.