# BISM3205 - Assignment 2

D)

The has given in the question is:

694430bed946b0330e4d15e9bc3931123c122166da6d353bad32d4c09da3788c

Using Crackstation.net, this is a known encryption of **universityofqueensland**  with a sha-456 encryption algorithm.

Ordinarily, we would not be able to decrypt a hashed result besides using a brute force technique or looking up hashes in a repository, as we have done.

E) Salted passwords

f) The numbers written in hexadecimal were transformed to base 10 and then looked up on the ASCII table provided in the week 6 tutorial to decipher the question:

What is it called when 2 strings have the same hash digest?

---

G)

F5 CA 4F 93 5D 44 B8 5C 43 1A 8B F7 88 C0 EA CA

H) and I)

MD5 hash of the image plane: 253dd04e87492e4fc3471de5e776bc3d

MD5 hash of the image ship: 253dd04e87492e4fc3471de5e776bc3d

J)

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAucU+u7phfIspqebNE+LR0pZYb0WaaNaX5WNTamO41MdSExiSuG7vTVIb+P4Vw0+BE+ElYFE7oYxyr+BPmsnNA986D3+RwrrELkfohLUDkhETGzE7hwl4FHTgQ0o3RLDFsjjAqiqoQVQpItWAo4JYWi09C0MvfaclZLll3wL20FnZc867TndMhr11qw68HB9daW0BLkZk/loJy0FFjl1nU/ujBhVPkOvCCrZOLT0ZUXZnIST4kV5bVJ5kniIEOAmZVMo893gDAXTkrCJrPwYGheTSNwzbyXtbuSvPV/C+YBhBTV2sdTA0WTYckFE6FYxLzjt9OMehIyMeXWFmT/TLKQIDAQAB

iE0E5eO/QYgiTuYiiHlTv60nxr1Q6gKV2LjVWca4Qbp4uw98qjpdxJV+trQO+ZRG2WZBGDQg/kRMVShVy/AEaG4TGK9SZL1elbmLrVn0+AXCAwJaPovYhV7c62eg67XKO/Fk+ThQc/0PnulIJgu7ALOXr3aULuvIVGUm5u030fi2vwrjaCFfQl4QtxlfhFSP1/p0ftDsJPuj3NNx7ylIuAkTmcSc8fZ3/12xyz1a72y+ASG3OTLwNACci/mZcr2gq7p/LkNFeHAYmUMh+ty5cijH9m+hgNWfw3TL0p2GMhLjNsDMdjTonqBKZhFLsnCRj2z+ggBF88ay4L/XVlMjzA==

Data must not be longer than 256 bytes

# Q2:

**Part A and B:**

What is the two-digit integer number in decimal notation that is greater than 0?

<https://alexpudmenzky.com/BISM3205/sad.jpg>

Sad face emoji consists of a colon ‘:’ and an opening parenthesis ‘(‘ which on the ASCII table correspond to decimal numbers 58 and 40, respectively.

Combined, this number would be 98, which is a single two-digit number, grater than 0, in decimal notation.

**Part C:**

An IP address is segmented into host and network portions via the use of a subnet mask, which is a series of bits which differentiate which section of the IP address represent the network and which part represent the host.

Bits in the subnet mask that are 1 represent the network portion, so the subnet mask 255.255.128, represented in binary form, i.e.

255.255.128.0 = 11111111.11111111.10000000.00000000 (binary)

Indicating that the first 17 bits represent the network portion of the IP address. A bitwise AND operation can be used to yield the relevant network bits.

11000000.10101000.00000101.00000010 (IP Address) AND

11111111.11111111.10000000.00000000 (Subnet mask)

11000000.10101000.00000000.00000000 (Network portion) = 192.168.0.0

Similarly, a bitwise NAND operation can be used to determine the computer (host) portion of the IP address:

11000000.10101000.00000101.00000010 (IP Address) NAND

11111111.11111111.10000000.00000000 (Subnet mask)

00000000.00000000.00000101.00000010 (Network portion) = 0.0.5.2

**Part D:**

This is more likely an encrypted message than it is a salted and hashed password. Some reasons are outlined below.

1. 127 bits – odd length of a hash. Typically an index of 2 – e.g 64, 128, 256 (for SHA-256)
2. Password Hashes typically do not need to be this long – even a SHA-256 hash in base 64 (which this seems to be) would only be 64 bits long. 127 bits seems too much

# Q3

Part A:

Part D:

The best option is (3) – hand the USD stick to your IT department or security team.

1. USB Sticks Can Be a Security Threat: Plugging unknown USB devices into your computer is a significant risk because the USB stick may contain malicious software, such as viruses, ransomware, or malware, that can compromise your company's network and sensitive data.
2. IT or Security Teams Are Trained to Handle Such Situations: The IT or security team has the necessary tools and expertise to safely investigate the contents of the USB stick without putting the network or devices at risk. They can check if the USB contains any malware or determine if it's safe to access.

Why Not the Other Options?

* Option 1: Plugging the USB stick into your computer:
* Dangerous: This could lead to a security breach, data theft, or malware infection that could compromise sensitive company data.
* Option 2: Leaving the USB stick where you found it:
* Not Responsible: Someone else might pick it up and plug it into their computer, putting the network and systems at risk.
* Option 4: Taking the USB stick home to investigate:
* Risky: This option still carries the potential of infecting your home devices and, even worse, exposing sensitive company data if you access it from home.
* Option 5: Throwing the USB stick in the trash:
* Ineffective: The USB could still be found and potentially used by someone else, leading to the same security risks.

Part E)

* An Intrusion Detection System (IDS) raises alerts when suspicious activity is detected. However, two types of errors can occur:
* False Positive:
* An alert is triggered for legitimate activity mistaken as a threat.
* Impact: A nuisance that wastes IT staff's time investigating non-threats, contributing to alert fatigue.
* False Negative:
* The IDS fails to detect a real attack.
* Impact: Serious, as actual threats go unnoticed, leaving the system vulnerable.
* Security Perspective: Least Desirable
* A false negative is far worse than a false positive. While false positives are inconvenient, false negatives mean real threats go undetected, potentially causing severe harm.
* Key Terminology:
* False Positive: A false alarm due to a false attack stimulus, adding to normal noise in network traffic.
* False Negative: A missed attack, which is very bad and must be avoided with high IDS accuracy.