**CS2IS Final Assessment**

**Ayshah Malik - 200089520**

1ai) An infected file will contain the binary code of the virus. In most cases, the executable code for each instance of the virus is the same, meaning it uses the same copies of malicious code. After identifying and analysing a virus, the antivirus software developers store characteristic byte sequences of the virus (the virus signature) in a database. The antivirus software executes pattern-matching. This is when it scans the disk of a computer to match byte sequences on the disk with the virus signature.

1aii) A polymorphic virus is a virus that changes form each time it inserts its code into another program. This is to prevent detection by changing their "signature" or the code used for decrypting routine. This makes it harder to impose anti virus software because it cannot carry out pattern-matching as easily. Even if the new signature is identified and added to antivirus solutions’ signature database, polymorphic malware can continue to change signatures and carry out attacks without being detected.

1b) Opens up the risk of a spear phishing attack.The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets' device with malware. This implementation can lead to the hacker locating the hash passwords, exporting them and then using tables of string and hash pairs to look for matches.

2a) Plaintext: THE MESSAGE IN THE POST

2bi) The main change would be in the key. The length of the key must be at least as long as the message.

2bii) The new key would also be decided and agreed to beforehand

2biii) The main difficulty would be exchanging the key securely

3a) The 3 main components of an authenticationsystem:

* **Authentication information:** what users provide to prove their identity, in this case the user’s email address and password
* **Complementary information:** stored on the computer and is used to validate the *authentication information*, in this case it’s the stored RSA encrypted passwords
* **Complementation function**: generates the *complementary* *information* from the *authentication information*, in this case its the encrypted function: RSA cipher.

3b) 3 problems:

* System tells the user which information (the username or password) was incorrect which makes it easier to hack.
* Exponential backoff alone can cause excessive traffic and isn’t that effective because instead of spreading the workload over time, they have dispersed periods with more idle time. Instead, X corporation should employ jitter to break the synchronisation and avoid collisions.
* The RSA cipher does not support forward secrecy, is slow and can be broken using statistical attacks.

3c) Anderson’s formula estimates the probability of guessing a password. By requiring long passwords, the number of possible passwords to guess from (N) increases which in turn brings down the probability of guessing the password. In addition to this, by prolonging the delay between each retry, the number of time units, T, in which someone can guess a password is limited.

So when T\*G is kept minimal and N is a large number, P will be low (the probability of guessing the password will be low). This can slow down attacks like slowing on-line dictionary attacks.