1. **Work Percentage of Both**

I have opted to work individually on this course work as I was finding it difficult to manage time to complete the other coursework's and to follow the lectures. I took help of my friends to understand the coursework and the requirements to be completed.

As I am comfortable in JAVA, I had decided to build the application JAVA. I was able to programme a command line based application to verify the signature and produce relevant outputs. I would like to further develop this application, which would include GUI and compatibility to verify various pfx files and other types of signature files as well.

2. **Security solution:**

Pretty Good Privacy (PGP) and X.509 uses public-key cryptography to help with communication between two individuals without sharing the same secret key securely. In PGP users can generate two keys (Private key, Public Key) to encrypt and decrypt the data. X.509 authenticates users, devices and resources using digital certificates.

This solution proposed must be evaluated in various terms to conclude if it's apt or not because PGP and X.509 are vulnerable to attacks like man-in-the-middle attacks, key spoofing or brute force attack.

The security of any solution, including the proposed one, should be evaluated in terms of the type of data being exchanged, the communication protocols used, the encryption algorithms employed, and the key management strategies implemented. These factors can all affect the overall security of the solution and should be carefully considered when designing and implementing it.

PGP and X.509 are both encryption systems that use public-key cryptography, symmetric encryption algorithms, digital signatures, and message authentication codes to protect communications. Both systems use digital certificates to ensure the identity of the sender and recipient. However, PGP and X.509 differ in the specific details of their implementation. PGP uses its own proprietary algorithms and protocols,

while X.509 is a standardized system that uses the X.509 certificate format and is widely used in many different applications.

Both PGP and X.509 are effective at protecting communications against various security threats, such as man-in-the-middle attacks, eavesdropping, and data tampering. However, no single security system is foolproof, and organizations should implement good security practices to further strengthen their security. This may include regularly changing passwords and using multi-factor authentication when available. Additionally, regular audits and tests can help organizations ensure the security of their systems.

3. **Impact of performing these attacks partially or fully online**

Performing PGP and X.509 operations partially or fully online can provide enhanced security and faster transaction speeds, but there are also risks to consider. Online encryption and authentication can reduce the chances of unauthorized access or manipulation, but there is still the potential for malicious actors to intercept and tamper with data. There may also be technical issues that can be difficult to troubleshoot. Additionally, using PGP and X.509 requires training for users and can be more expensive than traditional methods. Organizations should carefully weigh the potential benefits and risks before implementing online PGP and X.509 operations.