**Question #1**

**Confidentiality**

* Bank Pin ̶ Ensures confidentiality by only giving data access to those who have the pin.
* Triple DES encryption ̶ The main encryption algorithm used by ATM’s. This ensures that confidentiality is achieved when the data is transmitted through the network.

**Integrity**

* ATM bank processing is mostly done on the server side. The servers are backed up and secure. And in the event the data is ever compromised, the integrity can be restored.
* ATM uses a digital signature. A one-way hash is created from the server thereby making it difficult to compromise the integrity of data.

**Availability**

* ATM software allows for availability. If there is a fault in the system, they will automatically reboot themselves to ensure they are available to the public for use. Additionally, they are always being upgraded with faster processors and redundancy control.
* ATM system has an offline mode. In the event a network connection cannot be created the atm can still serve customers.

**Question 2  
A webserver (owned and managed by an organization) that hosts public information.**

* Low for loss of confidentiality since the information is already public. There is no confidentiality.
* Low for loss of availability since the information is not critical to anything. Being a webserver that provides public information does prevent anything important.
* Moderate for loss of integrity since the information is made public. Losing integrity from the server can cause the information to be inaccurate and mislead the public.

**A government agency managing sensitive investigative information.**

* High for loss of confidentiality since the information is sensitive to the government agency. If that information were to be leaked it could be used in the wrong way.
* High for loss of availability since investigative information is critical for the government to make progress on their investigations. By not being available, their investigation may come to a halt and buy time for the party being investigated.
* High for loss of integrity since the information can mean a lot to the investigation. If it becomes inaccurate, wrong parties may be accused of something they didn’t do.

**An IT system in a financial organization performs routine (not privacy-related information) administrative information.**

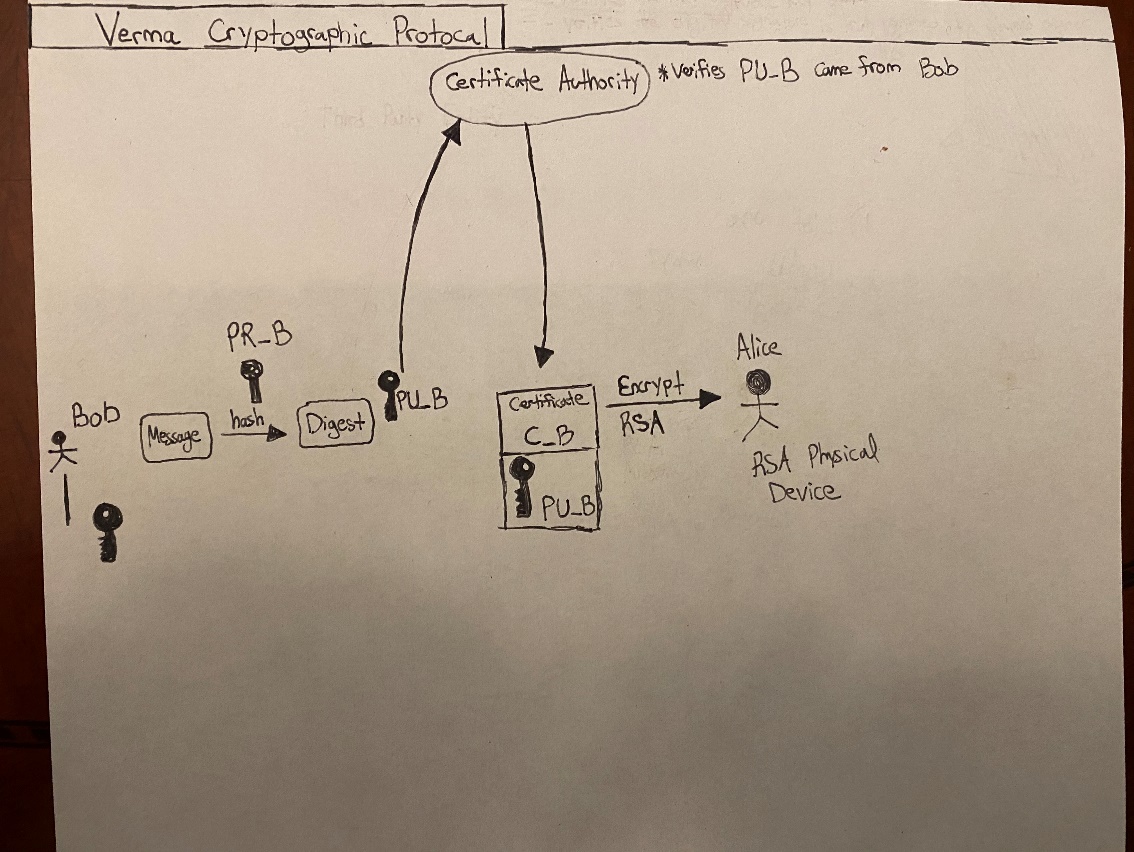
* Moderate for loss of confidentiality since the information is not privacy-related information. However, since it is part of a financial organization it may effect certain part of the business.
* Moderate for loss of availability since the information does not seem critical to the business. However, it may slow down the business by not being available.
* Moderate for loss of integrity since the information is not sensitive. A change in the information could negatively impact the business, however, it is moderate since it is only administrative information.

**Question 3**

The protocol I created is a combination of a digital certificate, and a physical authentication factor. The sender Bob creates a message, and using a hash function creates a digest using his private key. This is now the certificate (message, digest), and along with Bob’s public key the certificate is authenticated by a certified authority. This is to prove the authenticity of bob and his public key. The signed certificate is then encrypted using an RSA encryption. The encrypted message is then sent to Alice. Alice has a physical RSA device that generates a new code every few minutes. When she enters the generated key, the certificate is unlocked, and since it was signed by the authority, she can trust the authenticity of Bob. Using Bob’s public key, she can now compare the digest to ensure that the message was not tampered with during transmission. Thereby preserving confidentiality and authenticity. Additionally, if the message is not opened within a certain time frame, it will destroy the data.

The major assumption in this protocol is that the certified authority is trustworthy. If not trustworthy, there is no way to verify that the message came from Bob. The risk factor is low since the authority is usually determined and tested in advance. The only risk is if an intruder pretends to be the authority and changes Bob’s public key.

Another assumption is that Bob’s certificate to the authority is not compromised. If it is compromised, the intruder may be able to decode the message. It is likely the message is encrypted, but still possible to intercept. This risk factor is low since we have very good encryption algorithms and the data will self destruct before it is decoded.



**Question 4**

Due to the speed and efficiency of quantum computers, post-quantum cryptography is concerned with the development of cryptographic algorithms that are secure against the potential development of quantum computers. Specifically, it is concerned with the security and vulnerability of asymmetric cryptographic algorithms such as digital signatures, encryption, and key-establishment mechanisms.

**Question 5**

1. Cyber attacks on the Canadian health system
   * Cyber criminals trying to access patient information and other data.
   * LifeLabs was a victim of a cyber attack.
   * Sensitive patient data was compromised which can lead to identity theft.
   * Credit card and email information also compromised.
   * High impact on confidentiality since there was a lot of sensitive patient data that was compromised.
   * High impact on information availability since LifeLabs could not access the information to serve their patients until a third-party audit team approved.
   * <https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422>
2. Simplii Financial Breach (CIBC)
   * Personal and account banking information was compromised.
   * Approximately 40,000 of clients were affected.
   * Bank pins, credit card information, and personal details were stolen. People reported money taken from their account.
   * High impact on confidentiality since the personal details can be used to steal an identity.
   * Moderate impact on information availability since banks continuously performs audits and backups of their servers. They can restore their systems to a previous state and fix the breaches quickly. This allows for their information to be available for use very quick.
   * https://www.onserve.ca/two-canadian-banks-report-cyber-attacks-over-the-weekend-2/
3. Facebook Hack
   * 419 million Facebook users’ phone numbers linked to their accounts were compromised on an unencrypted database.
   * Many profiles were targeted maliciously.
   * Low impact on confidentiality since the purpose of Facebook is to connect and share with others. There is not much damage one can do with just a phone number. Other than selling it to telemarketing companies.
   * Low impact on availability. The website and users were still able to use the platform for their daily tasks.