**Cryptography**

**Describe the main techniques:**

* **Hashing:** converts any form of data into a unique string of text, always at the same length determined by the specific hashing algorithm.
* **Asymmetric (public key):** uses a pair of related keys; one public and one secret key, to encrypt and decrypt a message and protect it from unauthorized use or access.
* **Symmetric encryption:** only one key (a secret key) is used to both encrypt and decrypt a message, so the key must be shared between the sharing entities so it can be used in the decryption process.

**Describe the significance of key management:**

* Strong data encryption requires key management.
* Being able to own and manage your encryption keys is crucial to meet compliance standards and to satisfy regulatory requirements.
* Ensures regulatory compliance.
* Secures sensitive data from unauthorized access which could lead to entire systems being compromised and rendered unusable until a resolution was found.

**Generation:**

* **DES (Data Encryption Standard):** was used from 1977 to encrypt and decrypt data groups of up to 64 message bits, but is considered too weak due to the processing power of modern computers.
* **AES (Advanced Encryption Standard): established in 2001, replacing DES. AES cipher has a block size of 128 bits, but can have 3 different key lengths – AES-128/192 or 256.**
* **RSA:** is a public key algorithm originating also from the 70’s, but still widely used due to key sizes of 2048 to 4096.

**Distribution:** Key distribution of public keys is done through public key servers or by email. One key is kept private and the other key (public key) is uploaded to a server where it can be accessed by anyone so send a private encrypted message.

**Use/Purpose:** To lock (encrypt) data so that only someone with the right key can unlock it.

**Storage:** Stored on the key management server in the key storage database.

**Rotation:** This is when an encryption key is retired and replaced with a new one. How often depends on the user or purpose, but if a key is rotated every day, only that day of information can be decrypted by an attacker.

**Backup/Recovery:** very important because if the only copy of a key is lost then there is no way to access the data held within that key. Backing up creates a complete copy of the key file and also all the encryption keys held within.

**Revocation:** Securely removing keys that are known to be compromised.

**Destruction:** If a key is no longer needed or has been compromised the administrator of the key can delete it entirely and all data held within will also be deleted.

**Appreciate the legal issues:**

* **Export Control Issues:** The US government treats certain forms of cryptographic software and hardware as weaponry and as such has placed them under export control.
* **Import Control Issues:** Certain countries restrict the use of certain types of cryptography.
* **Patent Related Issues:** Avoid using patented algorithms or use algorithms whose patents have expired, that are licensed for royalty free use or whose license you have obtained.