**TASK 11**

**Explore the java classes related to Digital Certificates.**

In Java, the classes related to digital certificates are primarily found in the **java.security** package. These classes and interfaces are used for managing and working with digital certificates and public key infrastructure (PKI). Here are some important classes related to digital certificates in Java:

1. **java.security.cert.Certificate** - This is an abstract class that serves as the base class for all types of public key certificates.
2. **java.security.cert.X509Certificate** - This class represents the functionality of an X.509 certificate. It is used for retrieving and verifying information from X.509 certificates.
3. **java.security.cert.CertificateFactory** - This class provides the functionality to generate certificate, CRL (Certificate Revocation List), and certification path objects from their encoded form. It is used for reading and parsing certificates from input streams.
4. **java.security.KeyStore** - This class represents a storage facility for cryptographic keys and certificates. It can be used to store and manage certificates and their corresponding private keys.
5. **java.security.KeyStore.TrustedCertificateEntry** - This class represents a trusted certificate entry in a keystore.
6. **java.security.KeyStore.PrivateKeyEntry** - This class represents a private key entry in a keystore.
7. **java.security.KeyPair** - This class represents a public/private key pair. It is commonly used in generating digital signatures and encryption in conjunction with certificates.
8. **java.security.Signature** - This class provides the functionality for generating and verifying digital signatures. It is commonly used in conjunction with certificates for data integrity and authenticity verification.

These classes are commonly used in Java applications for implementing digital certificate-based security mechanisms, including authentication, data integrity, and secure communication.

**Digital certificate vs digital signature :**   
Digital signature is used to verify authenticity, integrity, non-repudiation ,i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus, digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of their users

| **Feature** | **Digital Signature** | **Digital Certificate** |
| --- | --- | --- |
| **Basics / Definition** | Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity. | Digital certificate is a file that ensures holder’s identity and provides security. |
| **Process / Steps** | Hashed value of original message is encrypted with sender’s secret key to generate the digital signature. | It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation. |
| **Security Services** | **Authenticity** of Sender, **integrity** of the document and **non-repudiation**. | It provides security and **authenticity** of certificate holder. |
| **Standard** | It follows Digital Signature Standard (DSS). | It follows X.509 Standard Format |