Name: Deep Ghadiyali

Roll Number: CS17B011

Cybersecurity Assignment 1

1. Practical Examples from daily life:

    a. **Large amount of cash withdrawal from ATM**:
        i. Debit/ATM Card for the bank account
        ii. Card PIN
        iii. OTP from the bank

    b. **Payment apps and UPIs for example Google Pay, BHIM UPI, Amazon Pay**:
        i. Binding of phone number (SIM card) associated with bank account and device id of mobile that uses the payment app
        ii. Finger print or 4-digit pin to enter the payment app
        iii. OTP at the time of transaction

    c. Online trading account money withdrawal:
        i. Username/Password for accessing the account
        ii. Adharcard and Pancard proof
        iii. OTP sent to the mobile number associated to account

2. Different Authentication factors used by APIs

    a. Twitter REST APIs:
        i. *OAuth 1.0a:* Allows to access private account information
        ii. *OAuth 2.0 Bearer Token:* Allows to access publicly available information on Twitter
        iii. *Basic Authentication:* Many twitter's enterprise APIs require the use of HTTP basic authentication.

    b. **Stack Exchange REST API v2.2:** Access token generated by login request on stack exchange

    c. **LinkedIn REST API v2:** Oauth2

d. **Flickr API:** OAuth 1 with username and password

e. **Box API:** Access tokens for Authorization
   i. Client side: OAuth 2.0
   ii. Server side: JWT

3. Certificate Details:

a. **Website:** https://www.google.com/
   i. Version: V3
   ii. Serial Number: `00c4ea98ea7e5e1f430200000000870182`
   iii. Signature algorithm: sha256RSA
   iv. Signature hash algorithm: sha256
   v. Issuer:

```
CN = GTS CA 1O1
O = Google Trust Services
C = US
```

   vi. Valid from: 19 January 2021 13:27:09
   vii. Valid to: 13 April 2021 13:27:08
   viii. Subject:

```
CN = *.google.com
O = Google LLC
L = Mountain View
S = California
C = US
```

   ix. Public key parameters: ECDSA_P256

b. **Website:** https://www.iittp.ac.in/
   i. Version: V3
   ii. Serial Number: `5760c30073c36efde5460c6b`
   iii. Signature algorithm: sha256RSA
   iv. Signature hash algorithm: sha256
   v. Issuer:

```
CN = GlobalSign RSA OV SSL CA 2018
O = GlobalSign nv-sa
C = BE
```

   vi. Valid from: 22 September 2020 14:52:02
   vii. Valid to: 03 October 2021 17:36:02
   viii. Subject:

```
CN = *.iittp.ac.in
O = Indian Institute of Technology Tirupati
L = Tirupati
S = Andhra Pradesh
C = IN
```

   ix. Public key parameters: `05 00`

c. **Website:** https://twitter.com/
   i. Version: V3
   ii. Serial Number: `0b5897d85529ec36e528bebe1ae34765`
   iii. Signature algorithm: sha256RSA
   iv. Signature hash algorithm: sha256
   v. Issuer:

```
CN = DigiCert SHA2 High Assurance Server CA
OU = www.digicert.com
O = DigiCert Inc
C = US
```

   vi. Valid from: 26 March 2020 05:30:00
   vii. Valid to: 25 March 2021 17:30:00
   viii. Subject:

```
CN = twitter.com
OU = tyo3
O = Twitter, Inc.
L = San Francisco
S = California
C = US
```

   ix. Public key parameters: `05 00`

d. **Website:** https://stackoverflow.com/
   i. Version: V3
   ii. Serial Number: `04c38c809a58abb1e57e1f66334b97c0c016`
   iii. Signature algorithm: sha256RSA
   iv. Signature hash algorithm: sha256
   v. Issuer:

```
CN = R3
O = Let's Encrypt
C = US
```

   vi. Valid from: 01 February 2021 19:44:19
   vii. Valid to: 02 May 2021 19:44:19
   viii. Subject:

```
CN = *.stackexchange.com
```

   ix. Public key parameters: `05 00`

e. **Website:** https://github.com/
   i. Version: V3
   ii. Serial Number: `0557c80b282683a17b0a114493296b79`
   iii. Signature algorithm: sha256RSA
   iv. Signature hash algorithm: sha256
   v. Issuer:

CN = DigiCert SHA2 High Assurance Server CA
OU = www.digicert.com
O = DigiCert Inc
C = US

vi. Valid from: 05 May 2020 05:30:00
vii. Valid to: 10 May 2022 17:30:00
viii. Subject:

CN = github.com
O = GitHub, Inc.
L = San Francisco
S = California
C = US

ix. Public key parameters: `05 00`

4. Root Certificates:
   a. **AAA Certificate Services**
      i. Version: V3
      ii. Serial Number: `01`
      iii. Signature algorithm: sha1RSA
      iv. Signature hash algorithm: sha1
      v. Issuer:

CN = AAA Certificate Services
O = Comodo CA Limited
L = Salford
S = Greater Manchester
C = GB

      vi. Valid from: 01 January 2004 05:30:00
      vii. Valid to: 01 January 2029 05:29:59
      viii. Subject:

CN = AAA Certificate Services
O = Comodo CA Limited
L = Salford
S = Greater Manchester
C = GB

      ix. Public key parameters: `05 00`

   b. **Certum CA**
      i. Version: V3
      ii. Serial Number: `010020`
      iii. Signature algorithm: sha1RSA
      iv. Signature hash algorithm: sha1
      v. Issuer:

CN = Certum CA
O = Unizeto Sp. z o.o.
C = PL

      vi. Valid from: 11 June 2002 16:16:39
      vii. Valid to: 11 June 2027 16:16:39
      viii. Subject:

CN = Certum CA
O = Unizeto Sp. z o.o.
C = PL

ix. Public key parameters: `05 00`

c. DST Root CA X3

i. Version: V3
ii. Serial Number: `44afb080d6a327ba893039862ef8406b`
iii. Signature algorithm: sha1RSA
iv. Signature hash algorithm: sha1
v. Issuer:

CN = DST Root CA X3
O = Digital Signature Trust Co.

vi. Valid from: 01 October 2000 02:42:19
vii. Valid to: 30 September 2021 19:31:15
viii. Subject:

CN = DST Root CA X3
O = Digital Signature Trust Co.

ix. Public key parameters: `05 00`

5. Different ways through which non-repudiation can be achieved:

a. **Digital Signatures:** A digital signature is generated using the private key of a key pair, which is public-key cryptography. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.
b. **Authenticated encryption:** If confidentiality is also required, then a=n encryption scheme can be combined with the digital signature, or some form of authenticated encryption could be used. Verifying the digital origin means that the certified/signed data likely came from someone who possesses the private key corresponding to the signing certificate.
c. **Biometrics:** Biometric of the sender can also be taken, as biometrics are very hard to replicate.

6. Personally Identifiable Information (PII) includes:

a. "Any information that can be used to distinguish or trace an individual's identity, such as name, social security number,

date and place of birth, mother's maiden name, or biometric records"

b. "Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

c. Examples of PII include, but are not limited to:
    i. Name: full name, maiden name, mother's maiden name, or alias
    ii. Personal identification numbers: social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number
    iii. Personal address information: street address, or email address
    iv. Personal telephone numbers
    v. Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting
    vi. Biometric data: retina scans, voice signatures, or facial geometry
    vii. Information identifying personally owned property: VIN number or title number
    viii. Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person