Rodrigo Brasil 11/2023

1. Name the three main components which make up PKI.
   1. Private key, public key and certificate authority
2. How would you explain, to a non-technical friend, the role PKI plays in protecting traffic between your browser and a web server.
   1. We will use the analogy of sending a letter. The envelope represents encryption, ensuring that only the intended recipient can open and read the message. The sender's unique stamp on the envelope is like a digital signature, proving that the message came from them. The certificate authority (CA) is like the post office, verifying the sender's identity before issuing the stamp. The registration authority (RA) acts as an assistant to the post office, double-checking the sender's identity.
3. What is the main weakness of the PKI architecture?
   1. The main weakness of the PKI architecture is it relies on Certificate Authorities to issue and verify digital certificates. The trustworthiness of the entire system depends on the integrity and security practices of these CAs. If a CA is compromised, it can lead to the issuance of fraudulent certificates, enabling malicious activities like man-in-the-middle attacks.