

# (Applied) Cryptography

## Tutorial #11

Bernardo Portela (bernardo.portela@fc.up.pt) Rogério Reis (rogerio.reis@fc.up.pt)

December 6th, 2024

1. In the context of PKI
  - (a) Describe what is the accepted procedure of a client when receives a public-key certificate from a web server?
  - (b) Describe the process of certificate revocation and what are the possible reasons to apply it.
2. In a Paillier's scheme channel, with private key  $n = 620496404349687915307910174617$ , we intercepted the cyphered message

$$c = 358624662650643040547102063483144791182626860568435345308004$$

- . Can you recover the original plaintext?
3. Write the python/Sage procedures that behave as follows:
  - `genPrivate(sz)` that outputs a triple  $(n, p, q)$  in the conditions to be used as  $(n)$  the public key of a Paillier's scheme and  $n = pq$ , being  $p, q$  primes of size `sz` bits;
  - `voteYes(fileName, n)` that append to file `fileName` a vote yes (=1) using Paillier's scheme and public key `n`.
  - `voteNo(fileName, n)` that append to file `fileName` a vote no (=0) using Paillier's scheme and public key `n`.
  - `getResults(fileName, n, phi)` that prints the result of the polling written in `fileName` being `n` the public key used and `phi` the Euler's totient value corresponding to the public key.