7-2: Basic use of OpenSSL and ring

Artem Pavlov, TII, Abu Dhabi, 11.05.2024

Create new crate

- Create new branch in the repository p72
- Create new library crate p72
- Check that p72 is listed as a member of the workspace in the root Cargo.toml

File encryption using openssl

- Create two binaries in the bin/ folder:
  - openssl_enc: accepts input file path, output file path, and key as a hex-encoded string. Reads the input file, encrypts it using an AEAD algorithm, and saves it to the output file
  - openssl_dec: accepts input file path, output file path, and key as a hex-encoded string. Reads the input file, decrypts it, and saves it to the output file.
- Use random nonces generated with getrandom
- Append generated nonces to encrypted files

File encryption using ring

- Create two binaries in the bin/ folder:
  - ring_enc: accepts input file path, output file path, and key as a hex-encoded string. Reads the input file, encrypts it using an AEAD algorithm, and saves it to the output file
  - ring_dec: accepts input file path, output file path, and key as a hex-encoded string. Reads the input file, decrypts it, and saves it to the output file.
- Use random nonces generated with getrandom
- Append generated nonces to encrypted files