SRP Lab 4

- U prvom dijelu ovih vježbi smo dovršili zadatak iz prošlih vježbi

▼ Svatko je imao personalizirani file s izazovom, a zadatak je bio utvrditi koja je slika iz filea autentična

```
#KOD KOJI SAM KORISTIO
from inspect import signature
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes
from cryptography.exceptions import InvalidSignature

def load_public_key():
    with open("public.pem", "rb") as f:
        PUBLIC_KEY = serialization.load_pem_public_key(
            f.read(),
            backend=default_backend()
        )
    return PUBLIC_KEY

def verify_signature_rsa(signature, message):
    PUBLIC_KEY = load_public_key()
    try:
        PUBLIC_KEY.verify(
            signature,
            message,
            padding.PSS(
                mgf=padding.MGF1(hashes.SHA256()),
                salt_length=padding.PSS.MAX_LENGTH
            ),
            hashes.SHA256()
        )
    except InvalidSignature:
        return False
    else:
        return True

public_key = load_public_key()
print(public_key)

with open("image_1.png","rb") as file:
    image1 = file.read()
with open("image_1.sig","rb") as file:
    signature1 = file.read()

is_authentic = verify_signature_rsa(signature1, image1)
print(f'Image1 {"Is" if is_authentic else "Is not"} authentic')

with open("image_2.png","rb") as file:
    image2 = file.read()
with open("image_2.sig","rb") as fie:
    signature2 = file.read()
```

```
is_authentic = verify_signature_rsa(signature2, image2)
print(f'Image2 {"Is" if is_authentic else "Is not"} authentic')
```

- U drugom dijelu vježbi smo započeli s lozinkama

▼ Samo smo napisali kod koji predstavlja sporu hash funkciju