Lab 4

izazov 3 - nastavak lab 3

Cilj je odrediti autentičnost slike koju je profesor potpisao svojim privatnim ključem.

Poznati su nam javni ključ i fotografije su dostupne na lokalnom poslužitelju.

Prvo smo učitali ključ iz datoteke:

```
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
```

Funkcija koju koristimo za provjeru autentičnosti, prima argumente: digitalni potpis i poruka (u našem slučaju slika). Ukoliko je slika autentična, ispisat će se "true", ukoliko nije "false". Samo jedna od fotografija je autentična.

```python
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

 # Reading from a file
with open("image_1.sig", "rb") as file:
    signature = file.read()
with open("image_1.png", "rb") as file:
    image = file.read()
is_authentic = verify_signature_rsa(signature, image)
print(is_authentic)
```

Lab 4

U okviru vježbe upoznali smo se pobliže sa osnovnim konceptima relevantnim za sigurnu pohranu lozinki. Usporediti ćemo klasične (*brze*) kriptografske *hash* funkcije sa specijaliziranim (*sporim* i *memorijski zahtjevnim*) kriptografskim funkcijama za sigurnu pohranu zaporki i izvođenje enkripcijskih ključeva (*key derivation function (KDF)*).

Analizirali smo **Linux Hash** funkciju. Početnu vrijednost broja iteracija smo postavili na 5000. Zatim smo testirali vrijeme izvršavanje te funkcije za 5000 i za 1 000 000**(rounds=10**6)** iteracija.

```
(sara_c) C:\Users\A507\sara_c\sara_c\Scripts>password_hashing.py
+----------+----------------------+
| Function | Avg. Time (100 runs) |
+----------+----------------------+
| AES      |       0.000477       |
+----------+----------------------+


+----------+----------------------+
| Function | Avg. Time (100 runs) |
+----------+----------------------+
| HASH_MD5 |       3.1e-05        |
| AES      |       0.000477       |
+----------+----------------------+


+-------------+----------------------+
| Function    | Avg. Time (100 runs) |
+-------------+----------------------+
| HASH_SHA256 |       2.9e-05        |
| HASH_MD5    |       3.1e-05        |
| AES         |       0.000477       |
+-------------+----------------------+


+-----------------+----------------------+
| Function        | Avg. Time (100 runs) |
+-----------------+----------------------+
| HASH_SHA256     |       2.9e-05        |
| HASH_MD5        |       3.1e-05        |
| AES             |       0.000477       |
| Linux_CRYPTO_5k |       0.006825       |
+-----------------+----------------------+


+-----------------+----------------------+
| Function        | Avg. Time (100 runs) |
+-----------------+----------------------+
| HASH_SHA256     |       2.9e-05        |
| HASH_MD5        |       3.1e-05        |
| AES             |       0.000477       |
| Linux_CRYPTO_5k |       0.006825       |
```

Sara Ćurak

Računarstvo 120