

Ivan Legac Rudan

Izveštaj s trećih laboratorijskih vježbi

Na trećim laboratorijskim vježbama smo uz pomoć pythona i biblioteke cryptography za izazov 1 računali mac vrijednost za dani text file i provjeravali integritet tog filea ukoliko je integritet netaknut funkcija bi vraćala vrijednost true u suprotnome false. Naknadnom izmjenom filea smo se uvjerali da je narušen integritet kada bi funkcija ispislala false.

U drugom izazovu smo uz pomoć funkcije za određivanje integriteta trebali iz deset zadanih poruka i njihovih sig fileova odrediti kojim porukama je narušen integritet a kojima nije. Za to smo morali modificirati prethodno napisan kod za izazov 1.

```
26         return False
27     else:
28         return True
29
30
31 if __name__ == "__main__":
32     key = "legac_rudan_ivan".encode()
33
34     path = os.path.join("challenges", "legac_rudan_ivan", "mac_challenge")
35
36     for ctr in range(1, 11):
37         msg_filename = f"order_{ctr}.txt"
38         file_path_msg = os.path.join(path, msg_filename)
39         sig_filename = f"order_{ctr}.sig"
40         file_path_sig = os.path.join(path, sig_filename)
41
42         with open(file_path_msg, "rb") as file:
43             content_file = file.read()
44
45         with open(file_path_sig, "rb") as file:
46             signature = file.read()
47
48         is_authentic = verify_MAC(key, signature, content_file)
49
50         print(f'Message {content_file.decode():>45} {"OK" if is_authentic else "NOK"}')
51
52     # with open("tekst.txt", "rb") as file:
53     #     content = file.read()
54     # mac = generate_MAC(key, content)
55     # with open("poruka.sig", "wb") as file:
56     #     file.write(mac)
```

```
Message Sell 84 shares of Tesla (2021-11-11T20:31) OK
Message Sell 75 shares of Tesla (2021-11-10T03:33) OK
Message Sell 63 shares of Tesla (2021-11-15T07:48) NOK
Traceback (most recent call last):
  File "C:\Users\A507\iLegac\iLegac\mess.py", line 66, in <module>
    print(fpath)
NameError: name 'fpath' is not defined

(iLegac) C:\Users\A507\iLegac\iLegac>python mess.py
Message Sell 93 shares of Tesla (2021-11-10T05:01) NOK
Message Sell 13 shares of Tesla (2021-11-12T14:53) OK
Message Buy 20 shares of Tesla (2021-11-10T19:55) OK
Message Buy 3 shares of Tesla (2021-11-15T22:18) NOK
Message Sell 52 shares of Tesla (2021-11-12T19:50) OK
Message Sell 34 shares of Tesla (2021-11-15T04:16) OK
Message Buy 79 shares of Tesla (2021-11-11T20:31) OK
Message Buy 84 shares of Tesla (2021-11-10T03:33) OK
Message Sell 75 shares of Tesla (2021-11-15T07:48) NOK
Message Sell 63 shares of Tesla (2021-11-15T14:10) OK

(iLegac) C:\Users\A507\iLegac\iLegac>
```