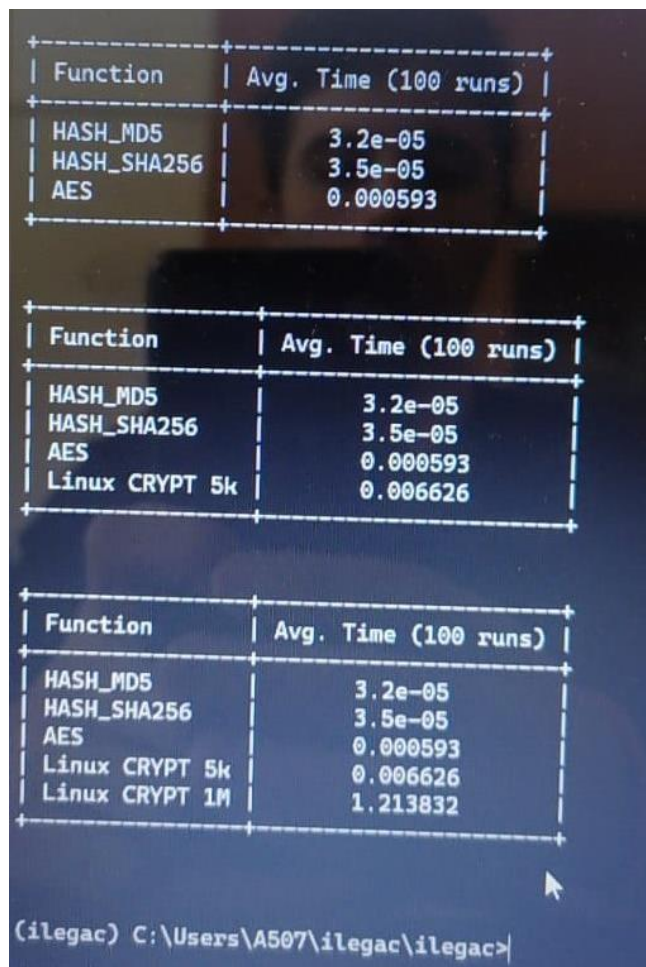


Ivan Legac Rudan

Izveštaj s četvrtih laboratorijskih vježbi

Na četvrtim laboratorijskim vježbama smo dovršili još jedan zadatak iz provjere digitalnog potpisa i autentičnosti slike koristeći RSA kriptosustav iz pythonove biblioteke cryptography.

U sljedećem zadatku smo koristili razne hash funkcije SHA256, MD5, AES i Linux CRYPT pomoću kojih smo iterativno hashirali neki izraz proizvoljan broj puta. Rezultati su ispisani na konzoli uz pomoć prettytable radi lakše komparacije rezultata. Naravno zadnja funkcija je imala najsporiji rezultat zbog velikog broja iteracija zato je i najsigurnija za korištenje od ostalih navedenih ali ujedno i najviše utječe na performanse sustava. Poanta pronalaženja idealne hash funkcije i broja iteracija je u kompromisu između performansi i sigurnosti



Function	Avg. Time (100 runs)
HASH_MD5	3.2e-05
HASH_SHA256	3.5e-05
AES	0.000593

Function	Avg. Time (100 runs)
HASH_MD5	3.2e-05
HASH_SHA256	3.5e-05
AES	0.000593
Linux CRYPT 5k	0.006626

Function	Avg. Time (100 runs)
HASH_MD5	3.2e-05
HASH_SHA256	3.5e-05
AES	0.000593
Linux CRYPT 5k	0.006626
Linux CRYPT 1M	1.213832

(ilegac) C:\Users\A507\ilegac\ilegac>