

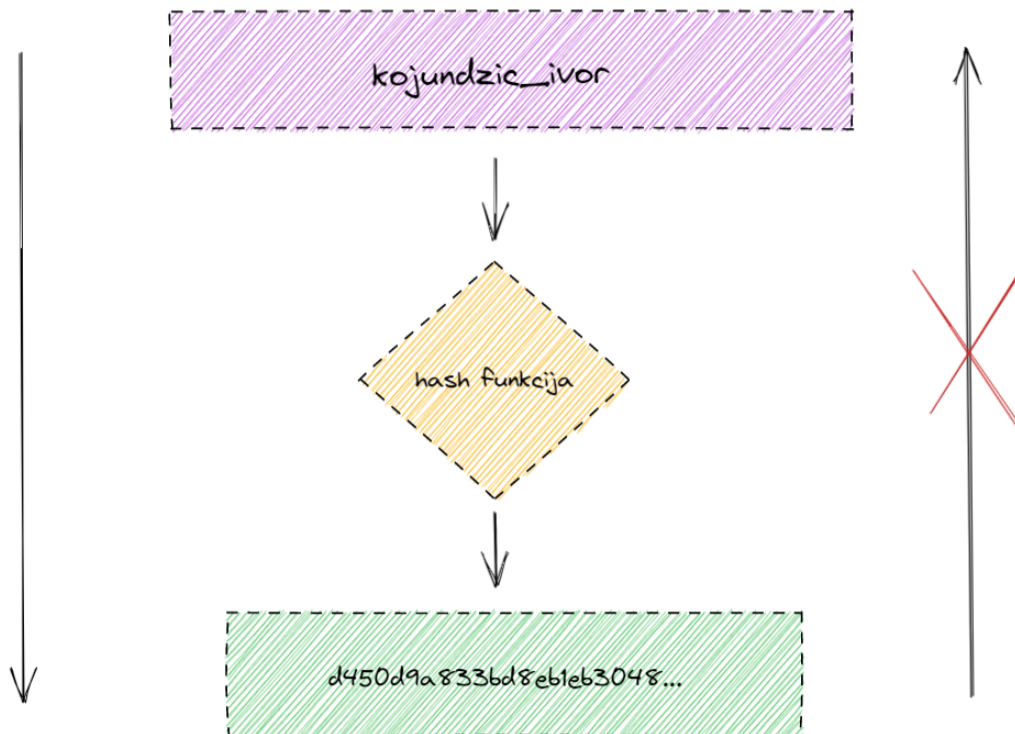
Vježba 3.

| | |
|-----------|---|
| Class | SRP |
| Type | Lecture |
| Materials | https://github.com/mcagalj/SRP-2022-23 |


U ovoj vježbi smo dešifrirali ciphertext pomoću *brute force* napada.

Prvi izazov nam se pojavio u vidu traženja željenog dokumenta. Za uspješnost *brute force* napada, napadač mora znati o čemu žrtva piše i neke bitne pojmove njegove informacije. Mi kao napadači smo znali da je u naslovu teksta dešifrirano naše ime i prezime.

Razlog zašto nismo samo dešifrirali naslov je svojstvo *one-way*. *One-way* nam govori da je nemoguće naći iz hash value poruku.



Drugi izazov nam je bio dešifrirati samu poruku. Primjenjujemo istu logiku. Kako bi izveli *brute force* napad, moramo znati nekakvu informaciju. Znamo da poruka nije tekstualna, već slika (*png*). Ispitali smo je li dokument počinje s formatom za *png* te kod svakog generiranog ključa koji je dešifrirao ciphertext provjeravali.



Congratulations Kojundzic Ivor!
You made it!