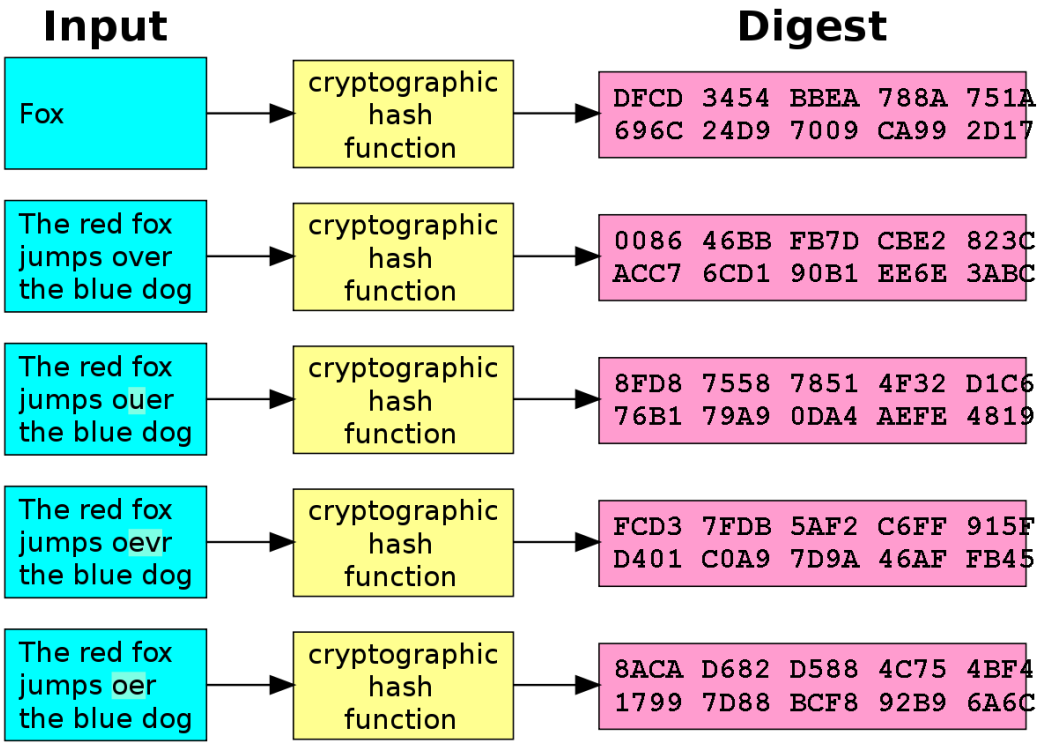
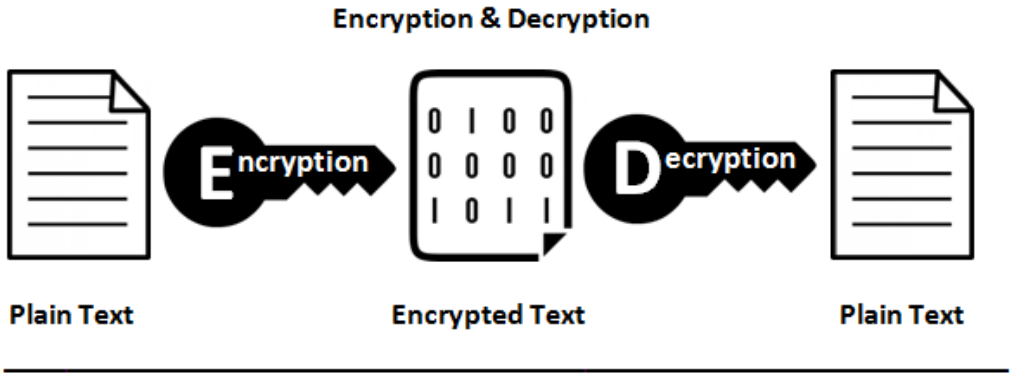
Laborator 8

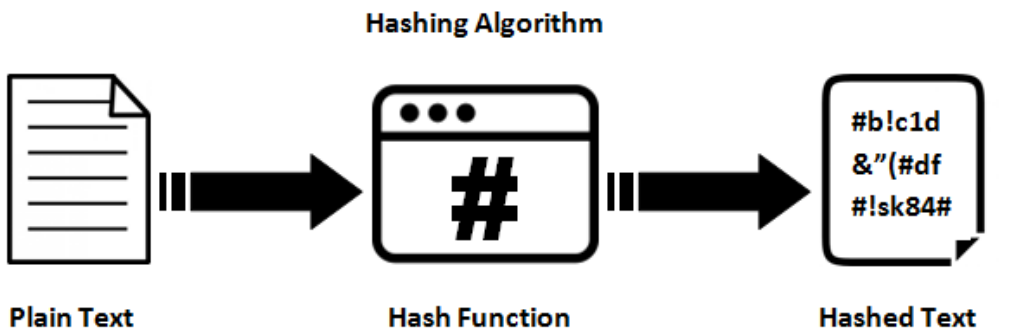
Functii Hash



Encryption VS Hashing

Encryption is reversible while hashing is not





Exercitii

▼ Exercitiul 1

a) Amestecarea ingredientelor pentru realizarea unei prăjituri poate fi considerată one-way function. **(A)**

b) Funcția hash MD5 este considerată sigură la coliziuni. **(F)**

c) SHA256 este o funcție hash cu output pe 256 biți. **(A)**

d) Valoarea hash SHA-1 pentru cuvantul „laborator” este 0x4bcc6eab9c4ecb9d12dcb0595e2aa5fbc27231f3. **(A)**

e) Este corect să afirmăm că „o funcție hash criptează”. **(F)**

f) O funcție hash folosită pentru stocarea parolelor trebuie să fie rapidă (i.e., să se calculeze rapid H(x) pentru x dat) **(F)** - sa nu apara coliziuni

g) Hash-ul (fără salt) - 095b2626c9b6bad0eb89019ea6091bd9 – corespunde unei parole sigure, care nu ar fi susceptibilă spre exemplu la un atac de tip dicționar **(F)** https://crackstation.net/

▼ Exercitiul 3

1. Parolele sunt stocare intr-o lista fara a fi asociate cu user-ul corespunzator
2. Hashuirea username-ului nu este necesara

3. Nu se foloseste un salt pentru hashuirea parolei
4. Se foloseste acelasi salt de fiecare data
5. MD5 nu este un algoritm sigur de criptare