1.

a. Amestecarea ingredientelor pentru realizarea unei prăjituri poate fi considerată one-way function. => **ADEVARAT**

b. Funcția hash MD5 este considerată sigură la coliziuni. => **FALS**

c. SHA256 este o funcție hash cu output pe 256 biți. => **ADEVARAT**

d. Valoarea hash SHA-1 pentru cuvantul „laborator” este 0x4bcc6eab9c4ecb9d12dcb0595e2aa5fbc27231f3. => **ADEVARAT**

e. Este corect să afirmăm că „o funcție hash criptează”. => **FALS**

f. O funcție hash folosită pentru stocarea parolelor trebuie să fie rapidă (i.e., să se calculeze rapid H(x) pentru x dat). => **FALS**

g. Hash-ul (fără salt) - 095b2626c9b6bad0eb89019ea6091bd9 – corespunde unei parole sigure, care nu ar fi susceptibilă spre exemplu la un atac de tip dicționar. => **FALS**

2. Nu s-au gasit coliziuni. Functia photon are 12 runde de procesare a datelor si datorita acestui numar mare de computatii ce au loc asupra datelor, exista sanse foarte mici sa se aloce aceeasi valoare hash pentru 2 string-uri diferite

3.

Exemplul 1: cheia secreta nu se schimba

Exemplul 2: este folosita o lista normala in loc de un hash table. Cu toate acestea, datele sunt procesate folosind o functie hash si viteza de executie a programului este astfel afectata

Exemplul 3: o singura iteratie SHA

Exemplul 4: security password salt e salvat in cod

Exemplul 5: md5 nu e sigura la coliziuni