

Criptografie și securitate CTI

Laborator 1

1. Adevărat sau fals:
 - (a) Algoritmul de cifrare ar trebui să fie ascuns lui Eve/Oscar;
 - (b) Scopul principal al lui Eve/Oscar este să determine cheia secretă.

2. Stabiliți la care proprietate CIA (Confidentiality, Integrity, Availability) face referire fiecare dintre următoarele situații:
 - (a) Dosarul medical al unui pacient nu trebuie făcut public;
 - (b) Un client nu poate modifica suma pe care o deține în contul de economii fără să facă o tranzacție autorizată (plată, încasare, transfer, etc.);
 - (c) Un student nu își poate modifica nota de la examen în catalog;
 - (d) Medicul de gardă trebuie să aibă acces la dosarele pacienților;
 - (e) În unele state, notele studenților trebuie să fie accesibile doar acestora, părinților/tutorilor și personalului administrativ;
 - (f) Sistemul bancar trebuie să permită plata cu cardul;
 - (g) Doctorul trebuie să fie sigur că informația din dosarul electronic al pacientului este corectă.