Autor: Ruxandra F. Olimid
Departamentul de Informatică, Universitatea din București

- Laboratorul 13 -
CrypTool

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători**!

1. CrypTool

CrypTool Portal oferă o suită de tool-uri și resurse educaționale în domeniul criptografiei și criptanalizei [1].

Instalați *CrypTool* [1] și experimentați cu primitive criptografice sau tipuri de atacuri posibile asupra acestora. Folosiți de asemenea *CrypTool* pentru vizualizarea algoritmilor studiați.

Notă 1: Alegeți singuri ce doriți să experimentați folosind *CrypTool* și prezentați rezultatele profesorului de laborator. **Atenție!** Experimentarea trebuie să fie potrivită ca nivel de dificultate. Spre exemplu, criptarea/decriptarea simetrică folosind AES în diverse moduri de operare cu observarea proprietăților amintite la curs **este acceptată**. Simpla criptare RSA folosind *RSA (step-by-step)* disponibil online [2] **nu este acceptată**.

Notă 2: Nu se acceptă pentru prezentare probleme legate de sistemele de criptare istorice.

Nota 3: Puteți experimenta și cu implementări/primitive/protocoale pe care nu le-am studiat la curs.

Nota 4: La acest laborator pot fi prezentate maxim 5 probleme.

Referințe bibliografice

1. *CrypTool Portal.* Cryptography for everybody. Accesibil la: https://www.cryptool.org/en/ Ultima accesare: ianuarie 2022.
2. CrypTool-Online. *RSA (step-by-step).* Accesibil la: https://www.cryptool.org/en/cto/rsa-step-by-step Ultima accesare: ianuarie 2022.