
LABORATORIJSKA VEŽBA BR. 1

Upoznavanje sa programskim paketom Cryptool

CILJ VEŽBE

- Instaliranje programskog paketa Cryptool
- Upoznavanje sa mogućnostima programskog paketa Cryptool
- Testiranje rada programskog paketa Cryptool

POTREBNA OPREMA

- Računar sa instaliranim Windows operativnim sistemom
- Programski paket koji download-ujete sa adrese Microsoft .NET Framework 4.7.2
- Programski paket Cryptool koji download-ujete sa adrese https://www.cryptool.org/en/ct2-downloads

TEORIJSKE OSNOVE

CrypTool predstavlja slobodni softver (freeware) koji ilustruje kriptografske koncepte i algoritme, uključujući i principe kriptoanalize. Ovaj programski paket prvenstveno je namenjen da upozna korisnika o mogućnostima i načinu rada različitih klasičnih kao i modernih simetričnih, asimetričnih i heš kriptografskih algoritama. To je jedan od najraširenijih i najkorišćenijih programa u svetu za e-učenje u oblasti kriptologije, koji sadrži veliki broj efikasno implementiranih algoritama i alata za analizu. Grafičko okruženje i obimna mrežna dokumentacija dopušta korisniku, čak i početniku, da se upozna sa tajnama kriptografske tehnologije. Aplikacija CrypTool je besplatna aplikacija koja može da se izvršava kako na Windows tako i na Linux operativnim sistemima. Podržava i savremene nastavne metode u školama i univerzitetima, a pogodna je i za obuku državnih službenika i zaposlenih kao i za podizanje svesti o čuvanju tajnosti i privatnosti podataka. Može da se koristi za primenu i analizu različitih kriptografskih algoritama. Većina klasičnih mehanizama, kao i nesimetrična kriptografija RSA, kriptografija eliptičnih kriva, digitalni potpis ili Difie-Hellman razmena ključeva objašnjeni su pomoću vizuelnih animacija što posebno pomaže u shvatanju i prihvatanju principa kriptovanja. Softver sadrži i tutorijale o prostim brojevima i osnovnoj teoriji brojeva.

Ovaj projekat je razvijan kao softver otvorenog koda. Prvobitno su ga razvile nemačke firme i univerziteti a kasnije prihvatili mnogi univerziteti širom sveta. Među njima i Singidunum Univerzitet ćiji su profesori i studenti izvršili prevod ovog programa, tako da imamo i našu srpsku verziju. Njegova osnova uloga je da korisnici postanu svesni sigurnosnih pretnji, odnosno za objašnjenje osnovnih koncepata kripotologije. Koristi se prvenstveno kao alatka za e-učenje a ne kao komercijalni program koji će vršiti kriptovanje i zaštitu podataka. Paket je dostupan na više svetskih jezika među kojima se nalazi i naš srpski jezik.

Mogućnosti i opcije programa Cryptool

Program Cryptool nam nudi veoma širok raspon mogućnosti i različitih prikaza kako klasičnih tako i modernih kriptografskih algoritama koji obuhvataju šifrovanje i dešifrovanje, generisanje ključeva, generisanje sigurnih lozinki, autentikaciju, sigurnosne protokole, i td. Među njima se ističu:

- klasične metode: npr Cezarova, Vižnerova, Hilova šifra, ADFGVX šifra, dupla transpozicija kolone (permutacija) i Enigma algoritam za šifrovanje

- moderne metode: npr. DES, Triple DES, AES, RSA algoritmi, hibridno šifrovanje i algoritmi za šifrovanje zasnovani na smanjenju rešetke i eliptičnim krivama
- Vizualizaciju nekoliko metoda (npr. Caesar, Enigma, RSA, Diffie-Hellman, digitalne potpise, AES)
- Kriptoanalizu određenih algoritama (npr. Vigenère, RSA, AES)
- Kriptoanalitičke metode merenja (npr. entropiju, n-grame, autokorelaciju)
- Pomoćne metode (npr. testovi na proste brojeve, rastavljanje na proste činioce, base64 kodiranje)
- Tutorijal o prostim brojevima
- Sveobuhvatnu online pomoć u okviru samog programa

Navešćemo još neke od specifičnih funkcija ovog programa da bi prikazali samo neki deo njegovih mogućnosti:

Pregled svih algoritama za kriptovanje nalazi se u online pomoći do koje dolazimo preko menija "Crypt".

Za klasične algoritme na raspolaganju su nam automatske analize, pomoću kojih se može doći do ključa kojim je tekst kriptovan (eventualno uz pomoć daljnjih informacija o izvornom tekstu i jeziku u kojem je pisan). Više informacija o automatskoj analizi možemo pronaći u meniju "Analysis" preko koga možemo da izaberemo algoritam koji želimo da analiziramo.

Kao podrška za analizu pojedinog dokumenta, CrypTool Vam omogućava izradu histograma, statistiku željenog N-grama ili izračun entropije za taj dokument.

U meniju "Indiv. Procedures" na raspolaganju su nam različiti pojedini algoritmi i protokoli kao:

- izračunavanje HASH vrednosti
- kompresovanje i dekompresovanje dokumenata. (tako možemo analizirati posledice kompresovanja podataka pre kriptovanja istih).
- generisanje pseudoslučajnih brojeva i njihova analiza.
- generisanje jakih ključeva po PKCS#5-Standardu.
- RSA kriptosastav (pod "Indiv. Procedures \ RSA demonstration") je detaljno predstavljen za različita kriptovanja. RSA ključevi su generisani pomoću prim brojeva koje stvara CrypTool. Pravljenje ključeva kao i enkripcija ili dekripcija može se pratiti korak po korak.
- Fakotorizacija brojeva je jako važna za kriptografiju. Sa ugrađenim algoritmima za faktoriziranje mogu se sa lakoćom razbiti jednostavni ili loše postavljeni RSA kripto sistemi. Tako možete stvoriti osećaj kolika je minimalna potrebna dužina ključa koju ćete upotrebljavati u vašem kriptosistemu da bi on bio siguran.
- U CrypToolu su ugrađeni aktuelni algoritmi koji zadovoljavaju usvojene internacionalne standarde.

Meniji i podmeniji u CrypToolu se dinamički menjaju u zavisnosti od tipa datoteke učitane u glavnom prozoru: tekst ili binarna datoteka. Na primer: podmeni "XOR" će se naći u meniju "Analysis \ Ciphertext-Only" samo onda kada je odabrana binarna datoteka. Sa druge strane možete naći podmeni "Hash \ Hash demo" pod menijem "Individual Procedures", samo kada je učitana tekst daoteka.

Pregled svih menija koje možete naći u CrypToolu možete pronaći u dodatku A skipte.

Treba naglasiti da cilj autorima CrypToola nije bilo izgraditi kriptografsku funkcionalnost već prvenstveno napraviti edukativni program koji treba da pogone u savladavanju osnovnih principa kriptologije.

Online pomoć i pristup dokumentaciji

U CrypToolu se mislilo na to da se može na bilo kom mestu jednostavnim pritiskom na taster F1 pozvati kontekstualno senzitivna pomoć. To znači da kada se nalazite u nekom od dijaloga treba pritisnuti taster F1 i CrypTool će vam prikazati tekst koji se odnosi za taj dijalog. Opširna pomoć sadži između ostalog objašnjenja svih osnovnih pojmova iz kriptografije, kratak popis preporuka za literaturu iz područja kriptografije i jedan pregled istorijskog razvoja iz tog područja.

Sa scenarijima (tutorijalima) u Online pomoći lako ćete se upoznati sa mogućnostima CrypToola. Za dobro razumevanje tema su Vam sledeće Demonstracije (vizualizacije) na raspolaganju:

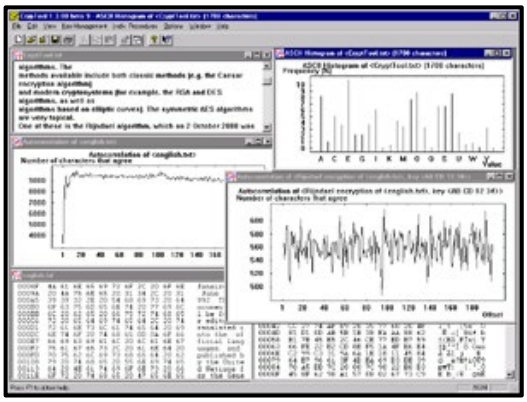
- stvaranje digitalnog potpisa,
- hiridno zaključavanje,

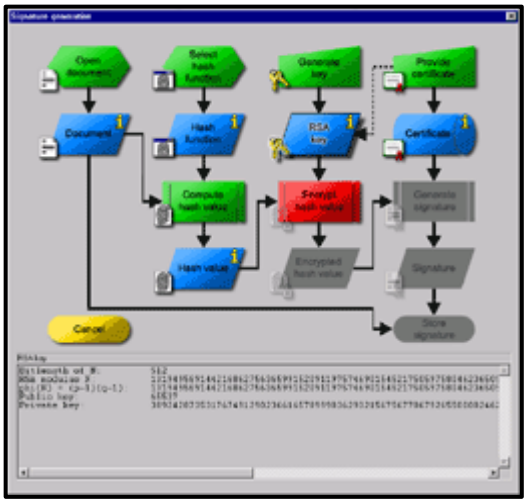
- kako promena teksta utiče na formiranje hash vrednosti
- osetljivost hash algoritma,
- stvaranje kolizija hash vrednosti (primena paradoksa dana rođenja) i
- tok izvođenja Diffie-Hellman izmene ključeva.

Snimci ekrana programa

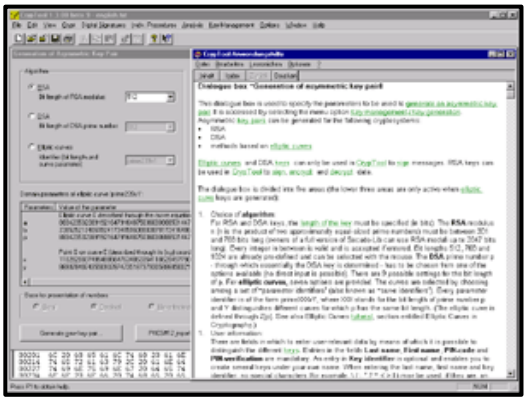
Prikazaćemo nekoliko snimka ekrana ovog programa:

U CrypTool-u su na raspolaganju brojne različite procedure za analizu teksta. One će otkriti slabosti jednostavnih enkripcijskih algoritama, dok će neki algoritmi biti automatski razbijeni.

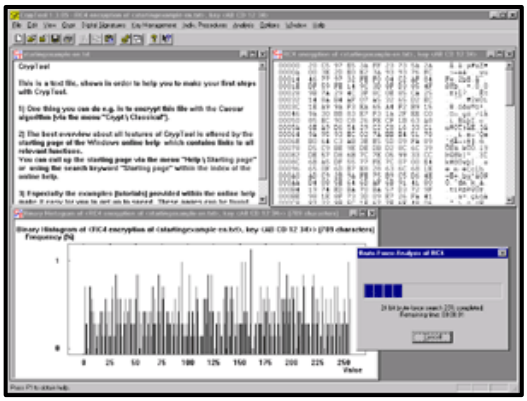




CrypTool otrkiva unutrašnji mehanizam rada digitalnih potpisa i hibridne enkripcije sa interaktivnim dijagramima toka podataka.



Mogućnosti CrypTool-a su aktivno pomognute kroz opsežan sistem pomoći (taster F1).



Zahvaljujući Secure biblioteci, CrypTool nudi mogućnost upoznavanja i testiranja modernih enkripcijskih algoritama. Analiza "Grube-sile" za ove metode Vam je takođe na raspolaganju.

Dokumentacija

Kratki uvod u program CrypTool 2: https://www.youtube.com/watch?v=dELT2-Vgsr8

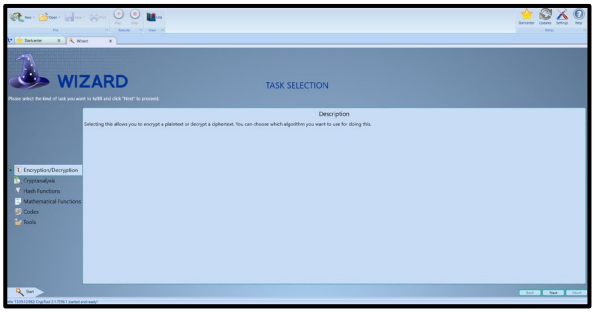
Službeni YouTube kanal za CrypTool 2:
https://www.youtube.com/channel/UC8_FqvQWJfZYxcSoEJ5ob-Q

YouTube lista za razvoj CrypTool 2 plugin-ova:
https://www.youtube.com/watch?v=YaSd_4t19nk&list=PLMuvAbyIl0PTTfPE2VhJ9PZ6qlOG0MMaX

Wiki za CrypTool 2 programere: https://www.cryptool.org/trac/CrypTool2/wiki/WikiStart

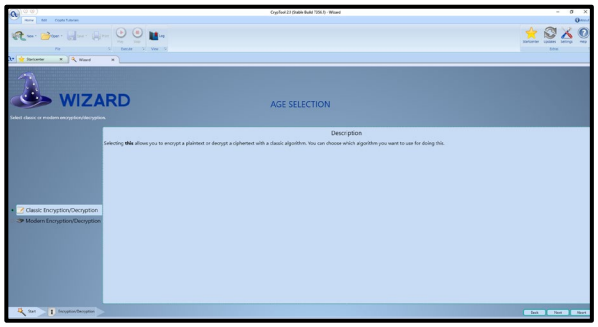
Diskusione grupe za CrypTool 2 programere:
https://www.cryptool.org/trac/CrypTool2/wiki/DiscussionGroups

Zadatak



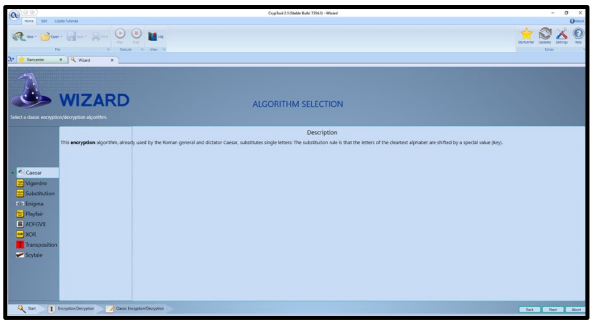
Instalirati alat za kriptovanje CrypTool2 (u daljem tekstu CP2). Proučiti osnovne funkcionalnosti alata i odraditi primer kriptovanja poruke: ***Zaštita podataka u komunikacionim mrežama.***

1. Sa web strane: *https://www.cryptool.org/en/ct2-downloads* preuzmite instalaciju CP2 alata

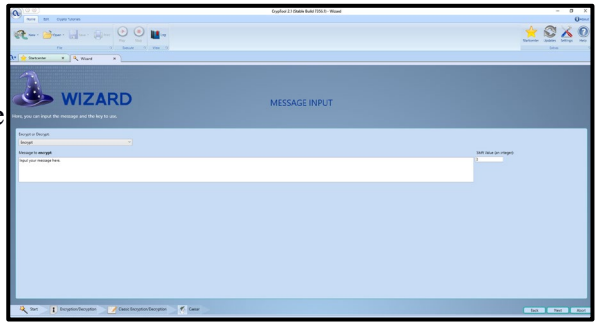


2. Nakon instalacije preuzetog softvera otvara se početna forma na kojoj birate jednu od velikog broja mogućnosti koje CP2 alat nudi:

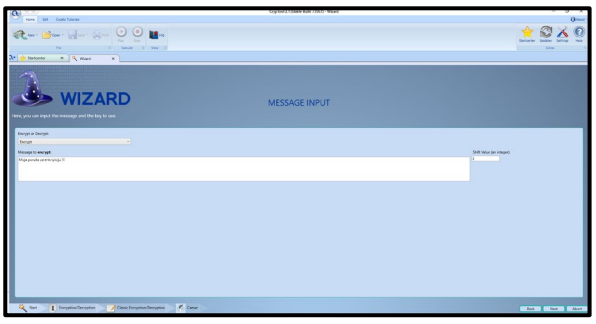
3. Izborom prve opcije i klikom na ***Next*** otvara se naredna stranica. Postoji **Klasičan** i **Moderni** način kriptovanja i dekriptovanja.



4. Izborom prvog modela otvara se naredna forma:

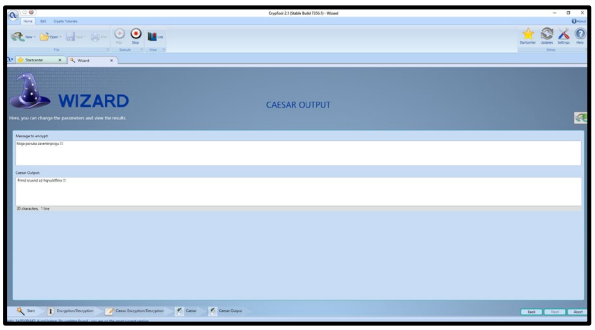


5. U klasičnom modelu nude se različiti algoritmi, čijom zamenom se menja i izlazni rezultat kriptovanja poruke. Izbrom prve opcije, ***Caesar***, otvara se forma za unos poruke koju želimo da kriptujemo, kao na sledećoj slici:



6. U polju predviđenom za poruku unosi se željeni niz karaktera koji se kriptuje kao na narednom primeru. Takođe, treba postaviti opciju za koliko karaktera se shift-uje vrednost, kao na sledećem primeru:

7. Klikom na Next dobijamo narednu formu koja prikazuje izvornu i izlaznu poruku korišćenjem već izabranih opcija za enkripciju.



Predmetni nastavnik i predmetni asistent