LABORATORIJSKA VEŽBA BR. 5

Simetrična enkripcija

CILJ VEŽBE

- Upoznavanje sa savremenim algoritmima kriptovanja
- Testiranje rada simetričnog algoritma DES
- Testiranje rada algoritma šifrovanja trostruki DES
- Testiranje rada simetričnog algoritma AES
- Testiranje rada simetričnog algoritma IDEA
- Testiranje rada simetričnog algoritma RC4
- Testiranje rada simetričnog algoritma RC6
- Testiranje rada simetričnog algoritma TWOFISH
- Upoznavanje sa programom za čuvanje podataka Truecrypt

POTREBNA OPREMA

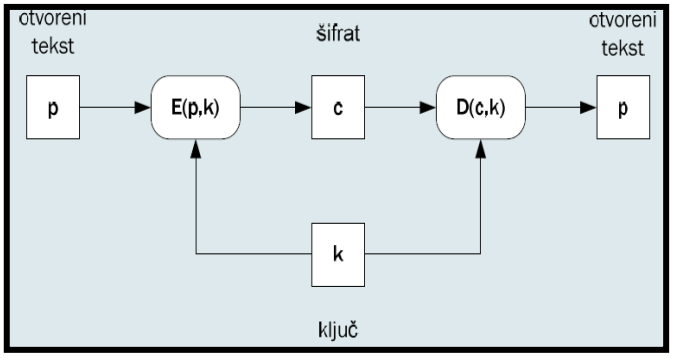
- Računar sa instaliranim Windows operativnim sistemom
- Istalirani programski paket Cryptool

TEORIJSKE OSNOVE

Savremeni kriptografski algoritmi

Pojava računara uslovila je razvoj novih algoritama kriptografije koji su svoje principe kriptovanja podataka zasnivali na snažnim računarskim karakteristikama računara. Metode klasične kriptografije zasnivale su se na tajnom pisanju, odnosno različitim matematičkim metodama koje su po nekom algoritmu primenjivane na otvorenom tekstu i na taj način ga činili nečitljivim trećim licima. Za razliku od njih metode moderne kriptografije svoj rad zasnivaju na tajnosti ključa preko koga se poruka može šifrovati i dešifrovati. U modernoj kriptografiji dakle važnija je **tajnost ključa** od tajnosti metode kriptovanja. U zavisnosti kako funkcionišu ključevi u kriptosistemu sve moderne sisteme kriptovanja tj. algoritme šifriranja možemo podeliti na:

1. **Simetrične algoritme** – koriste jedan odnosno privatni ključ
2. **Asimetrične algoritme** - koriste dva različita (javni i privatni) ključ.



Slika 1. *Blok šema principa rada simetričnog algoritma*

Simetrični algoritmi (vidi sliku 1.) za šifrovanje poruke **p** koriste ključ "**k**" kako bi dobili šifrat **c**. Dešifrovanje je obrnuto od prethodnog procesa, šifrat **c** se pomoću istog ključa "**k**" pretvara u originalnu poruku **p**. Osnovna osobina ovih algoritama je njihova brzina šifriranja pa su zato oni jako primenjivi za šifrovanje velikih datoteka. Ovi algoritmi se još nazivaju algoritmi sa jednim ključem (s*ingle key algorithms, one key algorithms*). Snaga ovih algoritama leži u tajnosti ključa. Dok god imamo potrebu da podatke šaljemo u šifrovanom obliku (što obično znači da treba da ostanu tajna za ostatak sveta), ključ za šifrovanje moramo držati u strogoj tajnosti (jer u suprotnom šifrovanje je totalno besmisleno). Šifrovanje i dešifrovanje se obavlja sledećim jednačinama:

$$E(K,P)=C$$
$$D(K,C)=P.$$

Simetrične algoritme možemo podeliti u dve grupe:

• **sekvencijalni algoritmi** (**protočni algoritmi** ili **algoritmi toka)** – šifruju poruku bajt po bajt.
• **blokovski algoritmi** ili **blokovske šifre** – šifruju delove teksta koji se nazivaju blokovi (npr, jedan blok je deo poruke dužine 64 ili 128 bita).

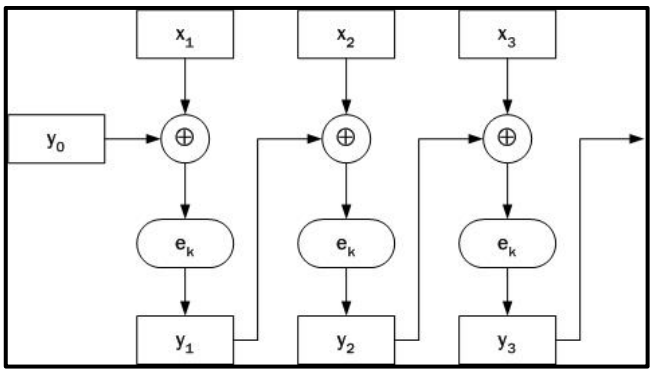
Režimi rada ECB i CBC

Pre nego što počnemo da testiramo rad simetričnih algoritama trebalo bi da napomenemo da postoje nekoliko režima rada ovih algoritama. Kao što je rečeno, blokovski algoritmi šifruju blok otvorenog teksta. To znači da DES šifruje blok dužine 64 bita. U realnim situacijama većina poruka je duža od 64 bita što znači da treba primeniti algoritam na više takvih blokova. Ovi režimi rada određuju način na koji se obavlja šifrovanje poruka dužih od jednog bloka.

Najjednostavniji režim rada je **ECB** (*electronic codebook mode*) – takozvani elektronski šifrarnik. Poruka se podeli na blokove dužine 64 bita (zadnji blok se dopuni do 64 bita slučajno generisanim nizom, ako je potrebno), a šifrovanje se obavlja blok po blok pomoću istog ključa. Identičnim blokovima otvorenog teksta odgovaraju identični blokovi šifrata. Jedan blok šifata zavisi samo od jednog bloka otvorenog teksta.

Prilikom šifrovanja u režimu **CBC** (režim ulančavanja blokova, *cipher block chaining*), najpre se računa rezultat XOR operacije izvršene nad trenutnim blokom otvorenog teksta i šifratom prethodnog bloka, a zatim se rezultat šifruje ključem K (videti sliku br.2). Povratna sprega postoji, blok šifrata zavisi od tekućeg i svih prethodnih blokova otvorenog teksta tako da identičnim blokovima otvorenog teksta u opštem slučaju odgovaraju različiti šifrati. Vrednost *y0* je inicijalna vrednost (inicijalizujući vektor, IV) koja mora biti poznata i primaocu i pošiljaocu.Za šifrovanje i dešifrovanje koriste se sledeće relacije:

$$y_i = ek\ (y_{i-1}\ \mathbf{XOR}\ x_i)\ \text{za}\ i \geq 1.$$
$$x_i = y_{i-1}\ \mathbf{XOR}\ dk\ (y_i).$$

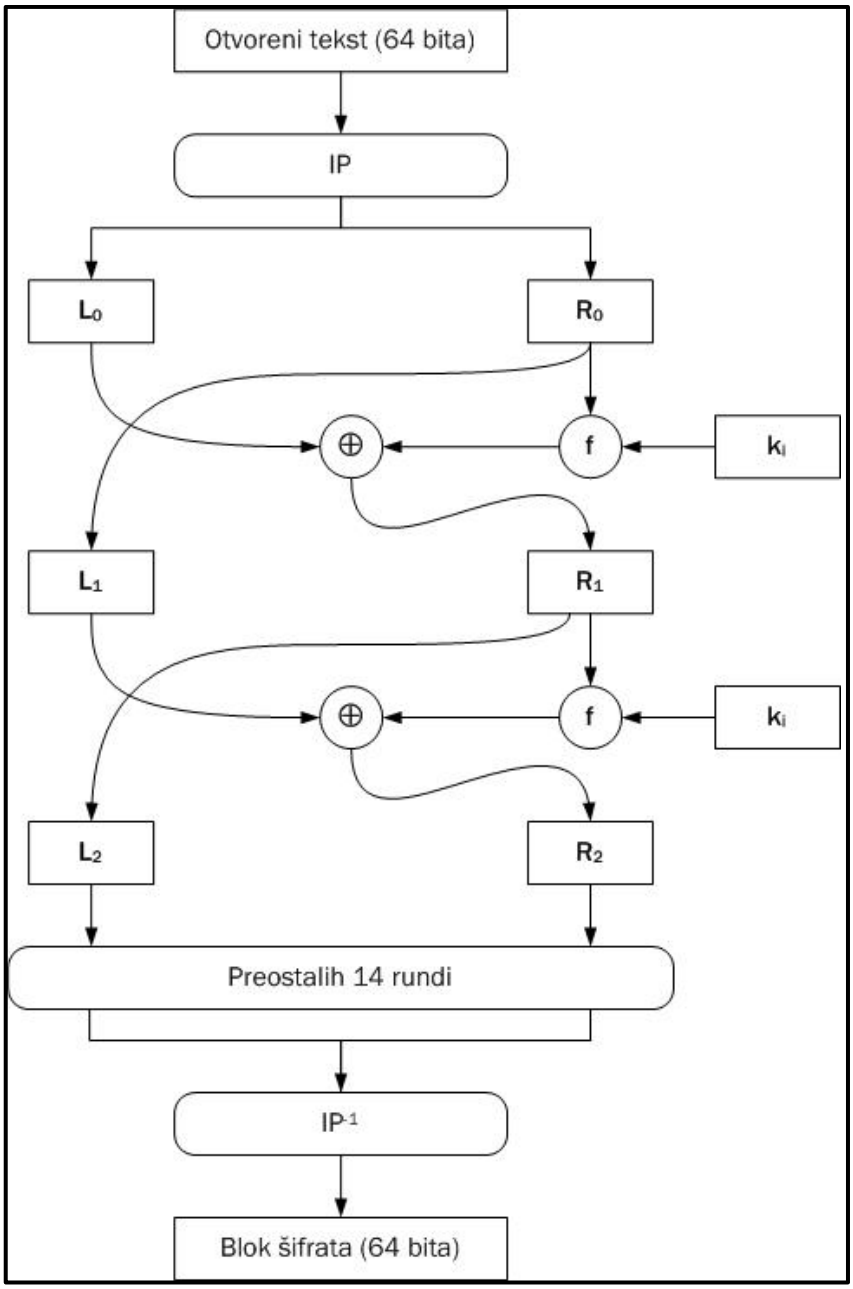


***Slika 2**. CBC*

Feistelova mreža

Feistelova mreža (*Feistel network*) je simetričan blokovski algoritam koji u i-toj rundi obavlja operacije:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \text{ XOR } f(R_{i-1}, k_i)$$



Slika 3. *Feistelova mreža*

Na slici br.3 prikazana je blok šema funkcionisanja *Feistelovog* algoritma. Parametar ***ki*** je takozvani podključ (vrednost koja se za svaku sledeću rundu nekim matematičkim postupkom generiše na osnovu ključa). Funkcija ***f*** je funkcija runde tj neki matematički postupak koji pomoću podključa transformiše ulaz u izlaz. To znači da se blok podatka deli na dva dela, od kojih se jedan propusti kroz određenu funkciju, a drugi se dalje prenosi neizmenjen. Blokovi zatim zamene mesta, pa se obavi sledeća runda (broj rundi zavisi od algoritma).

1. IDEA

Algoritam IDEA (*International Data Encryption Algorithm*) je patentiran algoritam i za komercijalnu upotrebu je potrebna odgovarajuća licenca. IDEA koristi ključ dužine 128 bitova za šifrovanje blokova otvorenog teksta dužine 64 bita. Prilikom šifrovanja, blok otvorenog teksta p dužine 64 bita najpre se deli na četiri podbloka dužine 16 bitova: p_1, p_2, p_3, p_4. Šifrovanje se obavlja pomoću 8 rundi i završne transformacije. U njima se koriste 52 potključa dužine 16 bitova (po šest u svakoj rundi i četiri u završnoj transformaciji), generisanih na osnovu polaznog ključa. Nad podblokovima dužine 16 bitova obavljaju se sledeće tri operacije:

- ekskluzivno ILI,
- sabiranje po modulu 2^{16},
- množenje po modulu $2^{16}+1$ (može se posmatrati kao S-box).

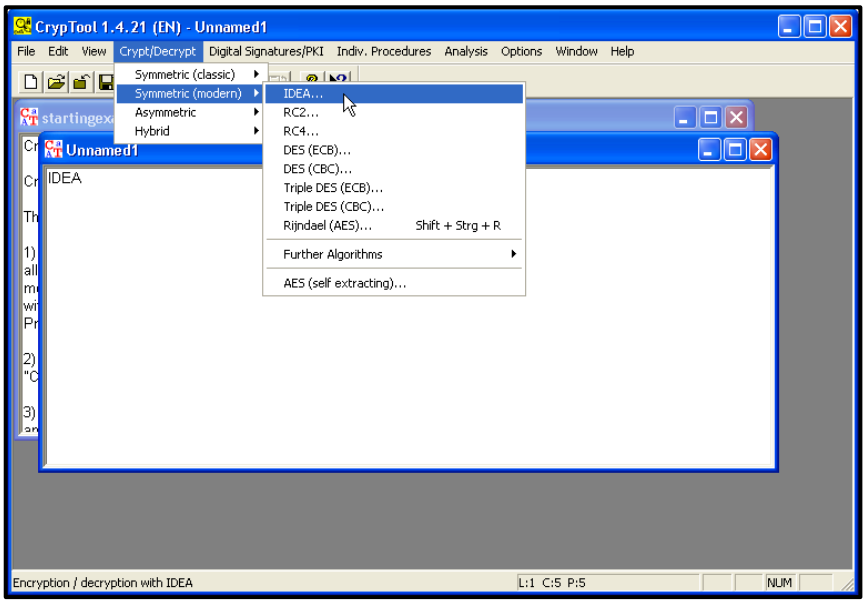
Ove operacije ne zadovoljavaju zakone asocijativnosti i distributivnosti i mogu se jednostavno softverski implementirati. Na kraju svake runde, zamenjuju se vrednosti u drugom i trećem podbloku. Posle osme runde dobijeni podblokovi prolaze kroz završnu transformaciju; šifrat se dobija konkatenacijom dobijenih podblokova C_1, C_2, C_3 i C_4.
Podključevi za runde se dobijaju podelom ključa na 8 16-bitnih vrednosti i iterativnim cikličkim pomeranjem vrednosti ulevo.
Moguća je implementacija algoritma sa nezavisnim potključevima. Pošto IDEA koristi 52 potključa dužine 16 bitova, ukupna dužina ključa bila bi 832 bita.

ZADATAK

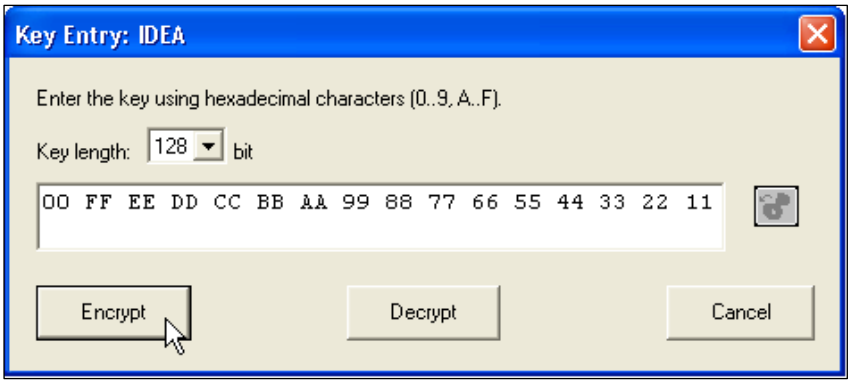
Pomoću Cryptool-a šifrovati i dešifrovati reč “IDEA” koristeći algoritam IDEA i sledeći ključ: 00 FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11.

Postupak:

Otvoriti novi prozor za unos poruka: FILE → NEW.
Otkucati “OVO JE MOJ NOVI OTVORENI TEKST” u prozor za upis teksta.
Iz menija Crypt / Decrypt izabrati Symmetric (Moden) → IDEA.



U polje za unos ključa kucate ključ iz teksta primera. Klik na Encrypt.



Dobijate šifrat:

2. RC4

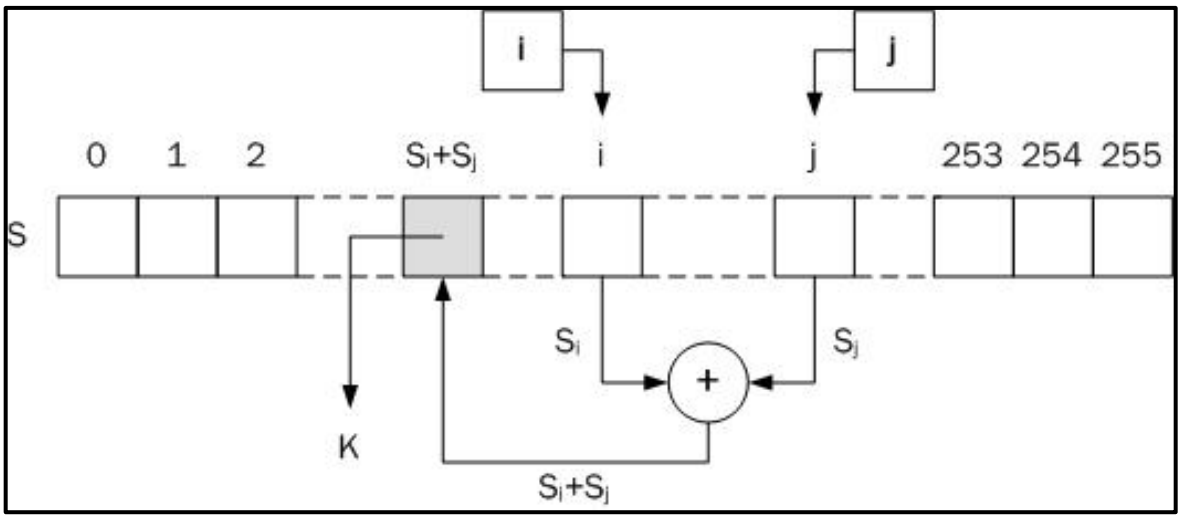
RC4 je simetrični stream algoritam sa ključem promenljive veličine. Algoritam pretvara slučajno generisani ključ (obično veličine od 40 do 256 bitova) u početnu permutaciju S koju koristi generator pseudoslučajnih brojeva kako bi proizveo pseudoslučajan niz bitova na izlazu. Generator pseudoslučajnih brojeva u petlji izvršava četiri jednostavne operacije u kojima je *i* brojač, dok se *j* povećava pseudoslučajno; posle toga se u polju permutacija S zamenjuju dve vrednosti na koje pokazuju *i* i *j*, i kao izlaz daje vrednost S na koju pokazuje S_i+S_j. Svaki član niza *S* menja se najmanje jednom, što znači da se cela permutacija S menja vrlo brzo.
Slučajni bajt se generiše na sledeći način:

$$\mathbf{i = (i + 1) \bmod 256}$$
$$\mathbf{j = (j + S_i) \bmod 256}$$

Si i Sj zamenjuju vrednosti:

$$\mathbf{t = (S_i + S_j) \bmod 256}$$
$$\mathbf{K = S_t}$$

Jedan bajt šifrata se dobija kao rezultat ekskluzivno ILI operacije primenjene nad bajtom ključne sekvence K i bajtom otvorenog teksta. Slično se dobija i otvoreni tekst – operacija ekskluzivno ILI se primeni nad šifratom i ključnom sekvencom.



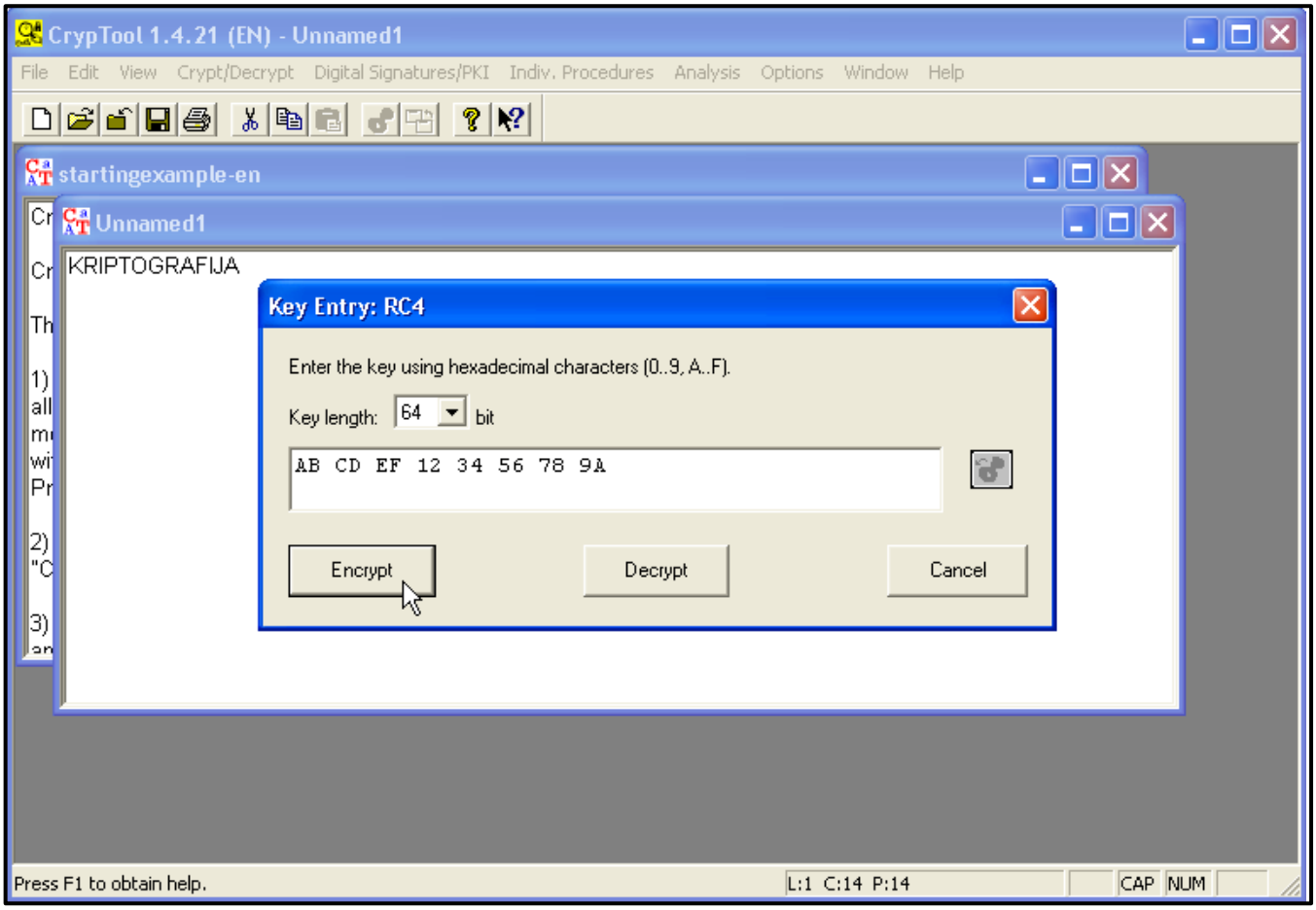
Slika 4. *RC4*

ZADATAK

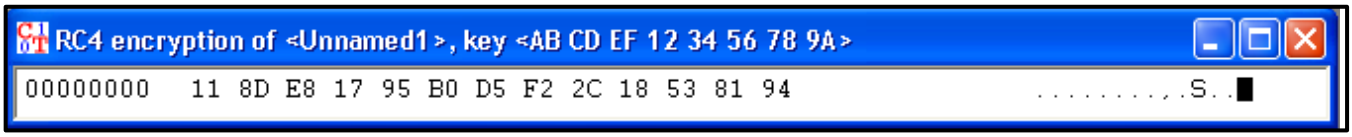
Pomoću Cryptool-a šifrovati reč KRIPTOGRAFIJA koristeći algoritam RC4 i 64-bitni ključ AB CD EF 12 34 56 78 9A.

Postupak:

Otvoriti novi prozor za unos poruka: FILE → NEW.
Otkucati "KRIPTOGRAFIJA" u prozor za upis teksta.
Iz menija Crypt / Decrypt izabrati Symmetric (Moden) → RC4.
Podesite dužinu ključa na 64 bita i u polje za unos ključa kucate ključ iz teksta primera. Klik na Encrypt



Dobijate sledeći šifrat:



3. RC6

RC6 je kao skup algoritama. Konkretna varijanta algoritma specificira se sa tri promenljive: dužina reči (w), broj rundi (r), i dužina ključa u bajtovima (b) i zapisuje se u obliku RC6-w/r/b.
Na konkurs za AES poslata je varijanta RC6-32/20/b (sa ključevima dužine 16, 24 i 32 reči).
Sve varijante RC6 algoritma obavljaju transformacije nad četiri reči dužine w bita i pri tome koriste sledećih šest osnovnih operacija:

- a + b (sabiranje reči a i b po modulu 2w)
- a – b (oduzimanje reči a i b po modulu 2w)
- a XOR b (eksluzivno ILI dve reči dužine w bita)
- a x b (množenje reči a i b po modulu 2w)

- a <<< b (rotacija reči a dužine w bita b mesta ulevo)
- a >>> b (rotacija reči a dužine w bita b mesta udesno)

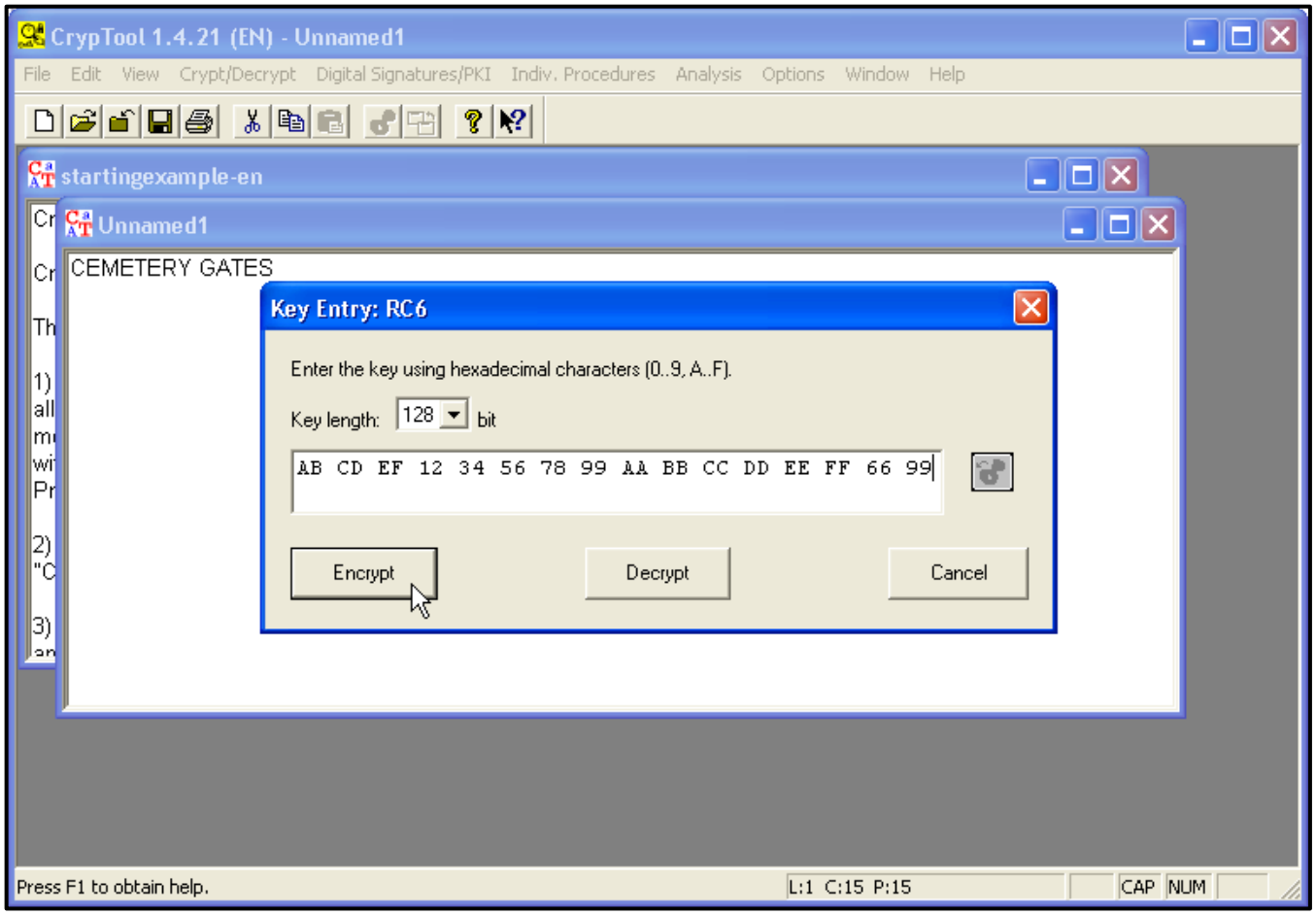
Ako je broj mesta b veći od dužine reči w, tada se reč rotira za log2w najmanje značajnih bitova od b.

ZADATAK

Pomoću Cryptool-a šifrovati tekst "CEMETERY GATES" koristeći algoritam RC6 i 128-bitni ključ AB CD EF 12 34 56 78 99 AA BB CC DD EE FF 66 99.

Postupak:

Otvoriti novi prozor za unos poruka: FILE → NEW.
Otkucati "CEMETERY GATES" u prozor za upis teksta.
Iz menija Crypt / Decrypt izabrati Symmetric (Moden) → RC6.
Podesite dužinu ključa na 128 bita, u polje za unos ključa kucate ključ iz teksta primera.Klik na Encrypt



Dobija se sledeći šifrat.

4. TWOFISH

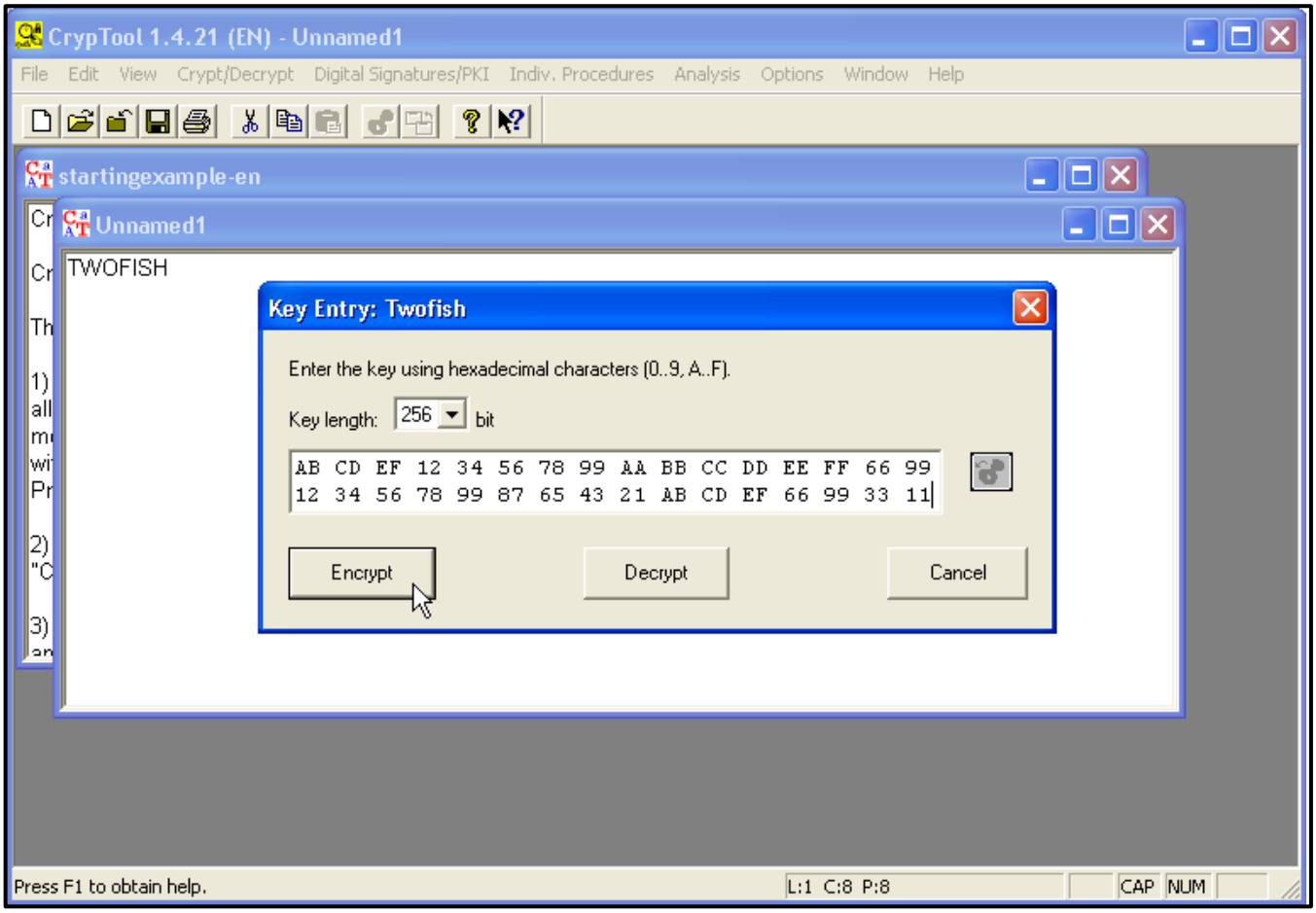
Algoritam Twofish šifruje 128-bitne blokove otvorenog teksta ključem dužine do 256 bitova. Šifrovanje se obavlja Feistelovom mrežom sa 16 rundi u kojoj je bijektivna funkcija F realizovana pomoću: četiri supstitucijske kutije zavisne od ključa runde, MDS matrice, pseudo Hadamard transformacije i operacije pomeranja bitova ulevo.

ZADATAK

Pomoću Cryptool-a šifrovati reč TWOFISH koristeći algoritam Twofish i 256-bitni ključ AB CD EF 12 34 56 78 99 AA BB CC DD EE FF 66 99 12 34 56 78 99 87 65 43 21 66 99 33 11.

Postupak:

Otvoriti novi prozor za unos poruka: FILE → NEW.
Otkucati "TWOFISH" u prozor za upis teksta.
Iz menija Crypt / Decrypt izabrati Symmetric (Moden) → Twofish.
Podesite dužinu ključa na 256 bita, a u polje za unos ključa kucate ključ iz teksta primera. Klik na Encrypt.



Dobićete prozor sa šifratom kao na slici:

Zadatak. Svaki student je dužan da pomoću gore objašnjenih algoritama šifruje **imena i prezimena** svojih članova porodice (Po četiri primera za svaki algoritam, ukoliko je broj članova porodice manji od četiri, studenti uzimaju **ime i prezime svog najboljeg prijatelja** kao četvrti primer).

Predmetni nastavnik i predmetni asistent