



## LABORATORIJSKA VEŽBA BR. 3

### Klasični kriptografski algoritmi

#### CILJ VEŽBE

- Testiranje rada *Monoalphabetic substitution*
- Testiranje rada Playfairvog algoritma
- Testiranje rada *ByteAddition*
- Testiranje rada XOR algoritma
- Testiranje rada Vernamovog algoritma

#### POTREBNA OPREMA

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

#### TEORIJSKE OSNOVE

##### Uvod

Kriptografija je zaštita informacija sifriranjem. Pod sifriranjem se podrazumeva transformacija iz jednog oblika u drugi, odnosno preslikavanje iz skupa u kriptodomen. Kriptografski sistem je skup srodnih šifarskih algoritama. Osnovna podela kriptografije je zasnovana na vremenskoj distanci kako su nastajali i na kompleksnosti primenjenih tehnika.

1. **Klasični kriptografski sistemi** koriste transformacije koje vrše:
  - ✓ šifre premeštanja - permutuju slova otvorenog teksta
  - ✓ šifre zamenjivanja - menjaju delove otvorenog teksta određenim šifarskim zamenama
  - ✓ kompozicione šifre - vrše dvostruku transformaciju kombinujući šifre ova dva sistema.
2. **Savremeni kriptografski sistemi** - realizuju se pomoću računara.
  - ✓ Koriste različite transformacije klasičnih šifara, specijalne matematičke i fiksne slučajne funkcije ili višestruka šifrovanja različitim ključevima
  - ✓ Razlika između **simetričnih** i **asimetričnih** algoritama (pored samog oblika i mogućnosti algoritama) je u tome što simetrični algoritmi koriste isti ključ za šifrovanje i dešifrovanje a asimetrični različite, javni i tajni, koji svoju snagu baziraju na tome da se bez dodatne informacije ne mogu dobiti jedan iz drugog.
  - ✓ kriptografija bazirana na simetričnim ključevima - isti ključ se koristi za sifriranje i desifriranje i on je tajni (cak i da napadac presretne ključ, on mora da zna koji algoritam je koriscen za kriptovanje)
  - ✓ kriptografija bazirana na javnim ključevima - ključevi su različiti (key1 i key2)-jedan je najcesce javni a drugi tajni; ključevi nisu isti
  - ✓ hash funkcija

## Klasični kriptografski algoritmi



- **Šifarski sistemi premeštanja - transpozicije** obuhvataju:
  1. obično premeštanje
  2. premeštanje ključem
  3. premeštanje rešetkama
  4. dvostruko premeštanje
- **Šifarski sistemi zamenjivanja** se deli na:
  - I. **Šifre proste zamene (MONOALFABETSKE)** se dele na:
    - a) alfabetske šifre
    - b) bigramske, Trigramske i poligamske šifre
    - c) kodne tablice
    - d) Kodovi
    - e) šifre raščlanjivanjem slova
  - II. **Šifre složene zamene (POLIALFABETSKE)**
    - a) šifre sa sređenim alfabetom
    - b) šifre sa nesređenim alfabetom

## 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. Cryptool je kriptografski softver koji pruža uvid u način funkcionisanja algoritama za šifrovanje, od najstarijih (Cezar) do savremenih (DES, 3DES...). Ugrađeni grafički prikazi toka šifrovanja pomažu da se pojedinačno razume svaki algoritam. Koristeći Cryptool na ovim vežbama predstavice najznačajnije algoritme za šifrovanje i usput objasniti kako svaki od njih funkcioniše. U lab.vežbi 1 već smo se upoznali sa nekim osobinama ovog kriptografskog programa.

## ZADACI:

### Monoalphabetic substitution / Atbash

**Zadatak:** koristeći cryptool-a šifrovati reč "EMPTYSHELL" šifrom Substitution gde je ključ:

**K=QWERTYUIOPLKJHGFDSA ZXCVBNM.**

Najpre, kako radi ova šifra? Ovo je monoalfabetska substitucionna šifra gde se svako slovo menja u neko drugo s tim da se ne može promeniti u dva različita već uvek u jedno! Slično Cezaru (Cezarovoj šifri), sa tom razlikom što kod Substitution cipher ne mora postojati fiksna zamena mesta za određeni broj već se svako slovo menja sa bilo kojim DRUGIM!

Kod Atbash šifre, stvar je slična sa jednom razlikom. Prvo slovo abecede se menja poslednjim, drugo slovo se menja pretposlednjim, etc:

(ABCDEFGHIJKLMNOPQRSTUVWXYZ → ZYXWVUTSRQPONMLKJIHGFEDCBA).

Slovni poredak sa obeleženim slovima otvorenog teksta:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ključ sa odgovarajućim slovima zamenjenim sa slovima iz otvorenog teksta:

Q W E R T Y U I O P L K J H G F D S A Z X C V B N M

**Rezultat:** EMPTYSHELL → TJFZNAITKK.

### **Postupak**

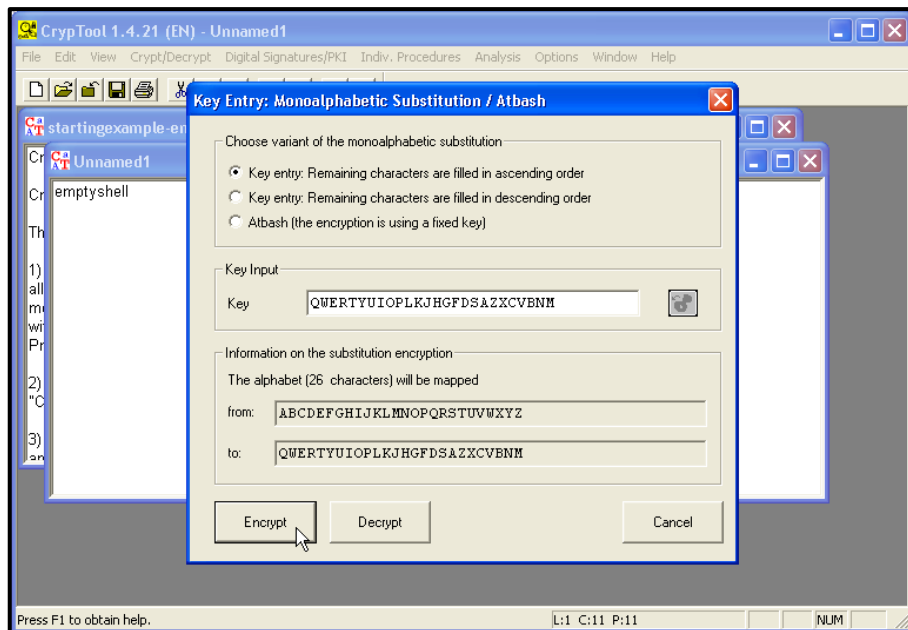
Sada probajte ovo na Cryptool-u, FILE → NEW, ukucamo EMPTYSHELL.

Encrypt / Decrypt → Symmetric (classic) → Substitution.

Dobićete prozor "Key Entry: Monoalphabetic substitution / Atbash".

U polje za ključ kucate QWERTYUIOPLKJHGFDSA ZXCVBNM.

Čekirate prvo polje za varijantu substitucije (slova poređana po redu: ABCD...).



Kliknete na Encrypt.

Dobija se šifrat.



### **Playfair-ova šifra**

**Zadatak:** šifrovati reč “EPITAPH” pomoću Cryptool-a koristeći Playfair-ovu šifru I ključ “ABSYNTH”. Playfair-ova šifra je polialfabetaska, šifruje pomoću jednog para slova tako da rezultat šifrovanja zavisi od oba slova. Ključna reč proizvodi matricu kojom se šifruje dati tekst. Pošto koristimo u primerima englesku abecedu koja ima 26 karaktera, pravi se matrica 5 x 5 (25 + ostatak 1). Opšti dogovor je da se slova I i J poistovete tako da se stavljaju u isto polje. U matricu se upisuju slova ključne reči, u ovom slučaju to je reč ABSYNTH. Upisuju se tako da nema ponavljanja, tj. upisuju se samo različita slova ključne reči a ostala slova u matrici su preostali karakteri engleske abecede. Matrica za reč ABSYNTH:

**A B S Y N  
T H C D E  
F G I J K L  
M O P Q R  
U V W X Z**

Od otvorenog teksta se prave blokovi od po dva slova (obavezno različita) – pri tome, dužina teksta mora biti parna, u slučaju da je tekst neparne dužine ubacuje se slovo po dogovoru, npr. X. Označimo slova jednog bloka u matrici. Moguće su tri situacije i shodno tome postoje tri načina za dobijanje dva slova šifrata:

- Ako su oba slova u istoj koloni, zamenjuju se slovom koje se nalazi za jedno mesto ispod
- Ako su oba slova u istom redu zamenjuju se slovom koje se nalazi za jedno mesto u desno
- Ako se ne nalaze u istoj koloni ni u istom redu, pravi se pravougaonik čija su ta dva slova tačke dijagonale.

Prvo slovo šifrata se dobija čitajući slovo koje se nalazi u istom redu prvog slova para slova otvorenog teksta, drugo slovo šifrata se dobija čitajući slovo koje se nalazi u istom redu drugog slova para slova otvorenog teksta.

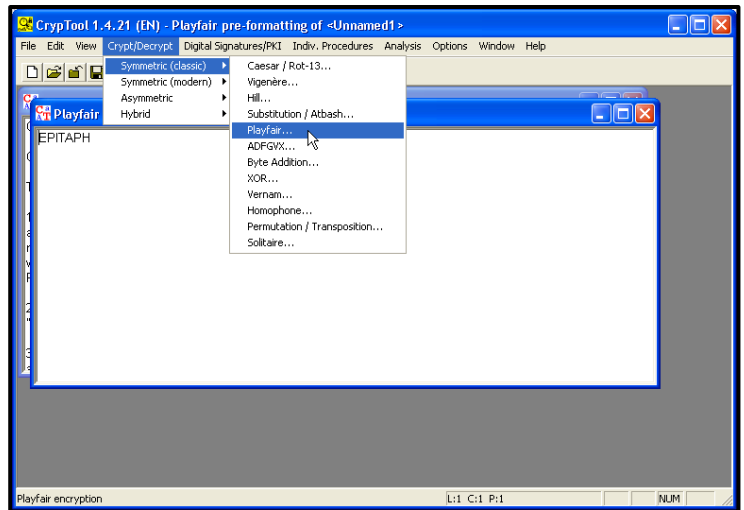
Objasnićemo ovo na primeru od nekoliko slova čiji parovi demonstriraju primenu prethodnih pravila. Pretpostavimo da šifrujemo reč GITARA. Delimo je u blokove od po dva slova: GI, TA, RA. Koristeći pravila iz prethodne tri tačke dobijemo šifrate za svaki par:

GI → IK  
 TA → FT  
 RA → MN

Ovaj postupak se ponavlja za sve ostale blokove. Naš primer je reč EPITAPH. Delimo je na blokove: EP, IT, AP, HX. U ovom slučaju dodali smo slovo X jer broj slova u reči neparan.

**Rezultat je:**

EP → CR  
 IT → FC  
 AP → SM  
 HX → DV



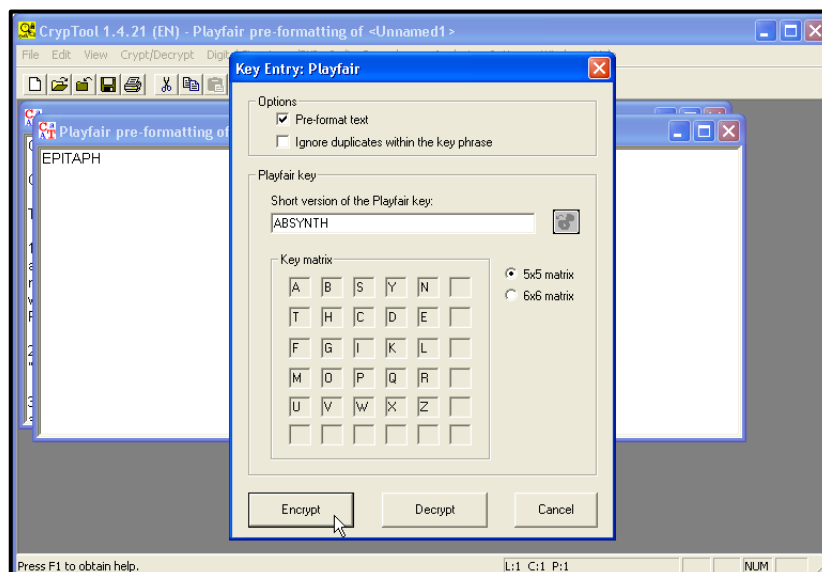
A B S Y N	A B S Y N	A B S Y N	A B S Y N
T H C D E	T H C D E	T H C D E	T H C D E
F G I J K L	F G I J K L	F G I J K L	F G I J K L
M O P Q R	M O P Q R	M O P Q R	M O P Q R
U V W X Z	U V W X Z	U V W X Z	U V W X Z

**Postupak**

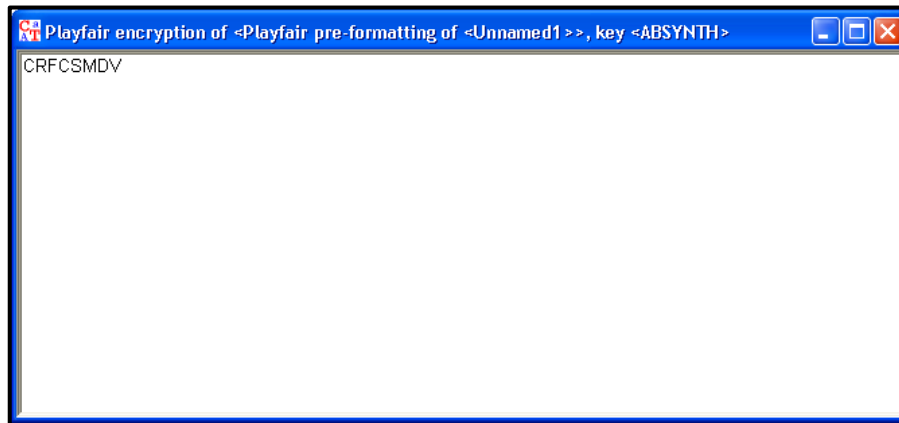
Na Cryptool-u:  
 FILE → NEW, ukucamo EPITAPH  
 Encrypt / Decrypt → Symmetric (classic) → Playfair.

Dobićete prozor “Key Entry: Playfair”. Na tom dijalogu:

- Označite checkbox Preformat text.
- Unesite ABSYNTH u polje Short version of Playfair key.
- Označite 5x5 matrix.



Dobijeni šifrat:



## ByteAddition

**Zadatak:** šifrovati "WINDOFHOURS" pomoću Cryptool-a algoritmom ByteAddition, ključem: 00 12 34 56 78 9A. ByteAddition algoritam radi tako što na otvoreni tekst dodaje karakter po karakter (bajt po bajt) ključa. Ako je dužina ključa veća od dužine otvorenog teksta onda se po svakom upotrebljenom karakteru (bajtu) iz ključa ciklički pomeramo na prvi karakter ključa i šifrujemo (dodajemo) dalje dok se ceo tekst ne šifrjuje. Svako prenošenje "carry" se ignoriše. Znači, posle svakog prenošenja Carry bit se NE setuje.

## *Postupak*

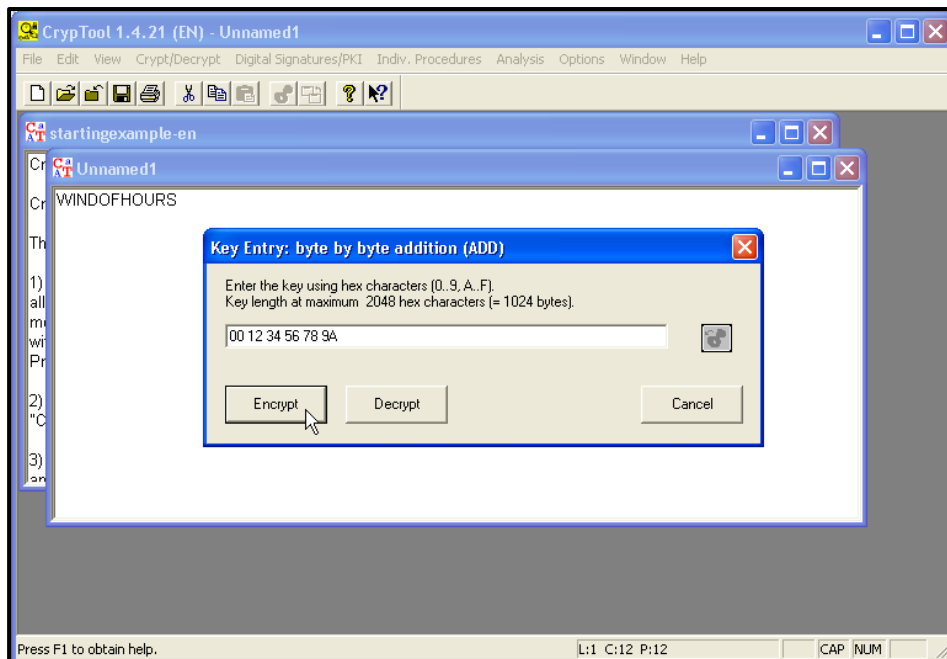
Sada ćemo demonstrirati ovaj proves šifrovanja na Cryptool-u:

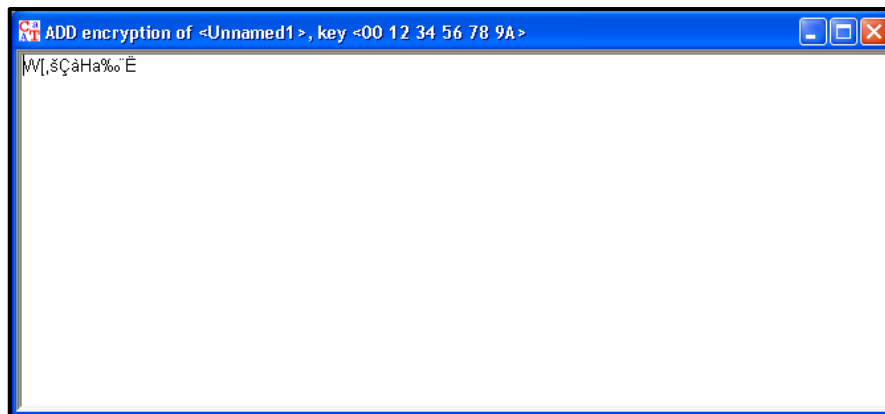
FILE → NEW, ukucamo WINDOFHOURS

Encrypt / Decrypt → Symmetric (classic) → ByteAddition.

Otvora se prozor u koji treba da unesemo ključ; popunite ga kao na slici:

Kliknite na Encrypt i dobijate sledeće:





Sada ćete sa istim ključem odraditi dešifrovanje dobijenog šifrata.

### XOR algoritam

**Zadatak:** šifrovati reč “PURITANIA” pomoću Cryptool-a algoritmom XOR (Exclusive OR), ključem: 66 69 99 96. Algoritam XOR se oslanja na jednu jako lepu osobinu istoimene logičke operacije:

$$((A \text{ XOR } B) \text{ XOR } B) = A$$

Dakle ako dva puta primenimo XOR sa istim operandom na neku vrednost, kao konačni rezultat dobijamo istu vrednost. XOR algoritam funkcioniše tako što šifrjuje otvoreni tekst bit po bit tako što XORuje bit otvorenog teksta sa bitom ključa. Ovo je tabela XOR-ovanja:

#### **A B A XOR B**

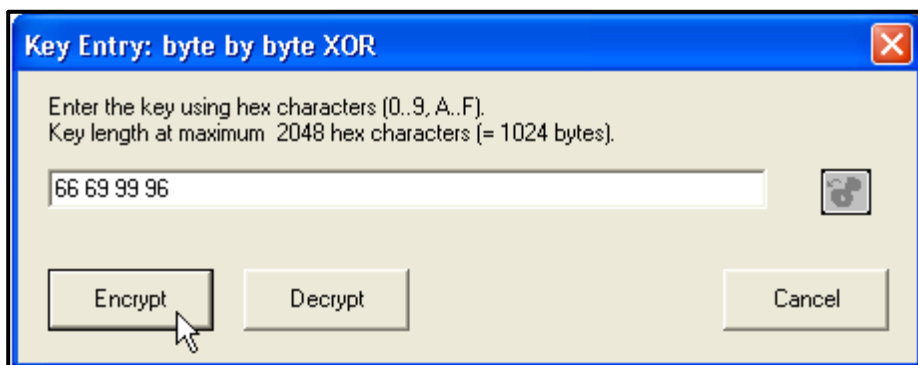
0 0	0
0 1	1
1 0	1
1 1	0

Operacija dešifrovanja je identična šifrovanju.

#### **Postupak**

Sada isto to radimo u Cryptool-u: FILE → NEW  
Crypt / Decrypt →  
Symmetric (classic) → XOR  
Popunite prozor kao na slici i odradite Encrypt.

#### **Rezultat:**



## Vernam

**Zadatak:** šifrovati tekst "I DID MY TIME AND I WANT OUT" pomoću Cryptool-a algoritmom Vernam koristeći tekstualni dokument *VernamKey.txt* (nalazi se u direktorijumu C:/Documents and Settings/Admin/My Documents/Vernam) kao ključ. Vernam-ov algoritam je zapravo XOR algoritam koji koristi dokument kao ključ za šifrovanje jer je mogućnost razbijanja ključa dosta manja nego kada se za ključ postavi niz karaktera ili binarnih vrednosti. Ovaj ključ se još naziva I jednokratna beležnica (*one time pad*).

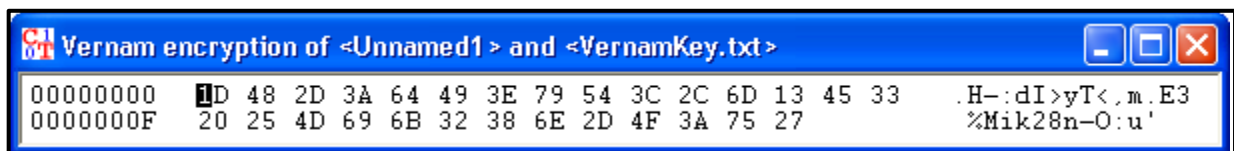
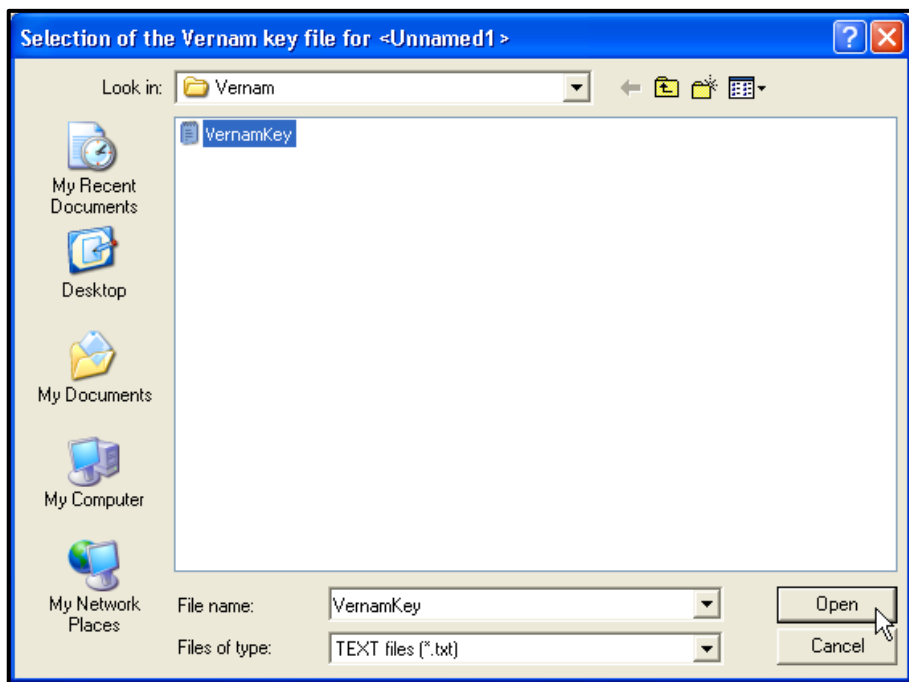
**PRIMEDBA: TEORIJSKI JE DOKAZIVO DA JE OVO SIGURNA ŠIFRA – NE MOŽE SE RAZBITI AKO SE PRIDRŽAVA DEFINISANIH PRAVILA. POSTOJI MOGUĆNOST DA SE POTPUNOM PRETRAGOM DOĐE DO NEKIH SMISLENIH REŠENJA ALI SU ONA JEDNAKO VEROVATNA I DOBIJENI REZULTAT U PRAKSI NE MOŽE DA SE ISKORISTI.**

### *Postupak*

Isprobajte na Cryptool-u Vernam-ovu šifru.

FILE → NEW, upišite "I DID MY TIME AND I WANT OUT" Crypt / Decrypt → Symmetric (classic) → Vernam

Zatim nađete tekstualnu datoteku u: C:/Documents and Settings/Admin/My Documents/Vernam i selektujete je za otvaranje. Kada kliknete na Open, Cryptool će obaviti šifrovanje i dobićete izlaz, tj. šifrat. U slučaju da je ključ kraći od otvorenog teksta, Cryptool će vam izbaciti poruku ali će sve jedno šifrovati ciklično. Poruka samo znači da je ključ nedovoljno siguran ali operacija šifrovanja može da se izvrši.



Dobijamo šifrat iz kog pomoću ponovnog kriptovanja samog šifrata istim dokumentom možemo uvek dobiti originalnu poruku, tj. otvoreni tekst. Ovo odradite sami.

**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**