Vežbe 01

Za potrebe prve vežbe ćemo razviti sistem koji koristi Skital za šifrovanje poruke (podataka).
Pre nego što nastavite dalje, kako biste se upoznali sa ovim šifarskim sistemom, potrebno je da znate šta je Skital. Potreba za zaštitom poruka je nastala još od davnih vremena, stari Grci i Egipćani su koristili ovaj vid sakrivanja podataka.

Skital funkcioniše po principu namotavanja kože na štap određene veličine. Veličina štapa je definisana između strana koje razmenjuju informacije, tako da u slučaju da neko presretne poruku ne može da je pročita ukoliko ne poseduje odgovarajuću veličinu štapa. Napdač u tom slučaju može da vidi samo razmeštena slova po dužini štapa.

S obzirom na to da ćemo mi razvijati šifarske sisteme u softveru "CrypTool", moći ćemo samo da izvršimo simulaciju ovog sistema zaštite.

Pre nego što započnemo simulaciju, potrebno je da poznajete sledeće pojmove:

- Poruka – Otvoren tekst – **M**
- Ključ – **K**
- Šifrovanje – **E** (eng. "Encryption")
- Dešifrovanje – **D** (eng. "Decryption")
- Šifrat – **C**

Za ovu vežbu će postojati 3 strane u našoj komunikaciji. Pošiljalac će se u nastavku ovog kursa obeležavati kao "Alisa", primalac poruke će biti "Bob", dok će napadač biti "Trudi". Ovi alijasi su preuzeti iz bajke "Alisa u zemlji čuda".

Takođe, **ključ** po kom se dešifruju poslate poruke, **NE SME da se deli ni sa kim**, kako ne bi došlo do kompromitovanja poverljivih informacija. To je isto kao kada biste PIN za vašu kreditnu karticu podelili sa nekim. U tom slučaju, bilo ko, ko dođe u posed broja Vaše kreditne kartice može da raspolaže sredstvima koje imate na računu.

Kada ste savladali ove osnovne pojmove, možemo preći na sam zadatak.

Tekst zadatka:

Alisa želi da pošalje poruku Bobu "*Ovo je prva vežba iz predmeta Kriptologija 1. Na vežbama je korišćen Skital za šifrovanje ove poruke.*" Dogovorili su se unapred da će koristiti ključ za šifrovanje veličine "7". Trudi presreće komunikacioni kanal, ali može da pročita samo šifrat koji je Alisa poslala Bobu. Bob poseduje isti ključ kao i Alisa, jer su ga prethodno razmenili. Da bismo se uverili da je dešifrovana poruka ista kao i ona koja je poslala Alisa, moramo da uporedimo heš (eng. "hash") vrednosti obe poruke.

Napomena:
Danas je ovaj vid šifrovanja lako probiti, jer računari poseduju ogromnu snagu resursa. Iz tog razloga nije preporučljivo da je koristite u privatne svrhe i zaštitu vaših podataka.