Аутор: Данијел Јовановић

Криптографија

Основни појмови и терминологија у криптографији „Чист текст“ или **clear text** односе се на изворну поруку или изворни текст који је могуће прочитати и разумети без примене било каквих посебних метода.

Уколико се такав текст треба пренети са места А до места Б, он се назива порука.

Порука се може слати путем рачунарске мреже као изворни текст (свима разумљива) или као неразумљив садржај који се назива шифрован или криптован текст.

Поступак помоћу кога се изворни текст трансформише у шифрован текст се назива **криптовање**. Криптовање се користи да би се обезбедило да ниједан корисник, осим корисника коме је порука намењена, не може да сазна садржај поруке.

Ако неовлашћени корисници дођу у посед криптованог текста и виде његов садржај не могу прочитати изворни текст. Криптовање изворног текста се обавља помоћу одређеног правила за криптовање односно криптографског алгоритма.

Сваки криптографски алгоритам као улазне податке има изворни текст и кључ а као излаз даје криптовани текст. Поступак који омогућава да се од криптованог текста добије оригинални изворни текст назива се **декриптовање**.

Декриптовање односно дешифровање представља инверзни поступак од криптовања. Криптовани текст за који није познат кључ зове се **криптограм**. Наука која проучава криптовања и декриптовања података се назива Криптографија.

Криптографија се ослања на математику и омогућава чување важних података као и њихов пренос преко рачунарске или телекомуникационе мреже а да при томе нико не може да их прочита осим корисника коме су намењени.

Док се криптографија бави заштитом података, **криптоанализа** је наука о откривању односно "разбијању" криптованих порука.

Обједињене криптографија и криптоанализа се називају **криптологија**.

Протокол представља скуп правила и конвенција који дефинише комуникациони оквир између два или више учесника у комуникацији.

Ту спадају:

- успостављање везе,
- одржавање везе,
- раскид везе
- и обнављање везе у случају прекида.

Криптографски протоколи се употребљавају за успостављање сигурне комуникације преко непоузданих глобалних мрежа и дистрибуираних система.

Ослањају се на криптографске методе заштите како би корисницима обезбедили основне сигурносне услуге поверљивости, интегритета и непорицљивости.

Треба напоменути разлике између термина кодирање и шифровање. Појам кодирање се односи на трансформацију изворног текста које се врши на основу обимне „књиге“ кодова, у којој се речи и фразе замењују случајним низом знакова. На пример, "JSZP" може бити код за "Ја се зовем Петар".

Насупрот томе, шифра ради на нижем нивоу: на нивоу појединачних слова, малих група слова, или у модерним шемама над појединачним битовима.

Уз то се уместо “књиге” кодова користе алгоритми који су утемељени неком математичком формулом.