Същност на криптографията

Науката **Криптография** или както са я наричали през изминалите векове Тайнопис, е средство за преобразуване на информация и данни с цел прикриването на оригиналната същност и прекратяване на нежелан достъп до криптираната информация. Представката „**крипто**“ („crypto“) идва от гръцката дума „krypto“, която означава „скрит“. Думата „криптология“ („**cryptology**“) идва от „кгуро“ и „logos“ и следователно означава „скрит свят“. Криптографията е изкуство дадена информация да се запази конфиденциална, в такава форма, в която не може да се прочете от човек, който не притежава необходимия ключ. Криптоанализите са изкуството да се използват алгоритмите разработени в криптографията.

Криптоанализите са изкуството да се използват алгоритмите разработени в криптографията. Криптирането може да се използва за нещо повече от конфиденциална комуникация. Посредством криптиране могат да се трансформират данни във форма, от която те не могат да се четат без четящия ги да има подходящо „познание“ за схемата на криптиране. Това „познание“ се нарича ключ. Ключът се използва за разрешаване на контролиран достъп до информацията на определени хора. При това положение информацията може да се изпрати до всеки, но само тези, които имат правилния ключ могат да я видят. Често се приема, че криптирането е компонент на сигурността, но в действителност то е механизъм за постигане на сигурност.

- **Открит (изходен) текст** – данни (не задължително текстови), предавани без използване на криптография.
- **Шифрован (закрит) текст** – данни, получени след използване на криптосистема с указан ключ.
- **Криптосистема** – семейство обратими преобразувания на откритият текст в шифрован.
- **Ключ** – параметър на шифъра, определящ избора на конкретно преобразуване на даденият текст. В съвременните шифри алгоритъма на шифриране е известен и криптографичната устойчивост на шифъра изцяло се определя от секретността на ключа.
- **Частен ключ** - частен ключ или секретен ключ е кодиращ/декодиращ ключ, известен само на едната страна от тези, които разменят кодирани съобщения. Традиционно в криптографията трябва да има ключ, който да е достъпен и за двете страни така, че всеки да може да кодира и декодира съобщения. Рискът при такава система е, че ако ключът бъде разбит или откраднат, системата спира да бъде защитена (на практика тя е разбита). В такива ситуации частния ключ се използва заедно с публичен ключ.