1. **OTÁZKA**

***KRYPTOGRAFIA:***

Ľudí už od nepamäti priťahovali tajomstvá a utajené informácie. Deti sa rady hrajú na hľadanie pokladu, hľadajú vianočné darčeky, vymýšľajú si rôzne tajné abecedy. Niekde hlboko v nás je zakorenená potreba niečo skrývať, ale na druhú stranu aj objavovať nové, nepoznané a hlavne zakázané alebo skôr pred nami ukryté predmety a informácie. Rôzne vojenské tajomstvá, tajné dokumenty, ktoré sa nesmeli za žiadnu cenu dostať do rúk neoprávneným osobám a už vôbec nie nepriateľom dali podnety na vznik kryptografie, čiže utajovania, šifrovania. Súčasne s kryptografiou musela vzniknúť aj kryptoanalýza, čiže dešifrovanie zašifrovanej správy bez akýchkoľvek bližších alebo len s malým množstvom informácií o spôsobe šifrovania. Obe tieto vedné disciplíny zahŕňa kryptológia. Slovo kryptografia sa skladá z dvoch gréckych slov kryptos - skrytý a graphein - písať. Niekedy ale zašifrovať správu nestačí a treba ju aj patrične ukryť. Touto oblasťou utajovania sa zaoberá steganografia, steganos - schovaný. Teda **Kryptografia** = veda o utajení obsahov správ.

Skytála (Antické Grécko), enigma (2.svetová vojna)

**Šifry poznáme:**

* ***Symetrická šifra***, niekedy nazývaná aj konvenčná, je taký šifrovací algoritmus, ktorý používa k šifrovaniu a dešifrovaniu jediný kľúč. Podstatnou výhodou symetrických šifier je ich nízka výpočtová náročnosť.

* ***Asymetrická šifra*** používa verejný kľúč pre šifrovanie a súkromný kľúč pre dešifrovanie. To znamená, že asymetrická kryptografia je skupina kryptografických metód, v ktorých sa pre šifrovanie a dešifrovanie používajú odlišné kľúče. To je základný rozdiel oproti symetrickej kryptografii, ktorá používa na šifrovanie a dešifrovanie jediný kľúč.

Symetrické šifry sa často používajú spoločne s asymetrickými. Obvyklé použitie je také, že otvorený text sa zašifruje symetrickou šifrou s náhodne vygenerovaným kľúčom. Tento symetrický kľúč sa zašifruje verejným kľúčom asymetrickej šifry, takže dešifrovať dáta môže len majiteľ tajného kľúča danej asymetrickej šifry.

