

Šifriranje je postopek **zakrivanja podatkov v tako obliko**, da ni lahko berljiv oz. uporaben, če ne vemo s čem je bil šifriran.

![[Pasted image 20230111180817.png]]

Poznamo: - Asimetrično (*za dešifriranje in šifriranje se ne uporablja isti ključ*) - Simetrično šifriranje (*za dešifriranje in šifriranje se uporablja isti ključ*), simetrično je hitrejše

Kljub temu, da lahko paket šifriramo, smo še zmeraj ranljivi sledečim napadom: Napadalec paket lahko zavrže Lahko ga spremeni Lahko ga podvoji, napad z ponovitvijo