Iz Islovarja

Islovar je spletni terminološki slovar informatike, ki ga objavlja jezikovna sekcija Slovenskega društva INFORMATIKA in ga najdete na naslovu http://www.islovar.org. Vabimo vas, da tudi vi prispevate svoje pripombe, predloge ali nove izraze.

blokóvni algorítem -ega -tma m *(angl. block algorithm)* simetrični šifrirni algoritem, s katerim se naenkrat šifrira celoten blok; prim. pretočni algoritem

blokóvno šifríranje -ega -a s *(angl. block encryption, block cipher mode)* simetrično šifriranje, pri katerem se uporablja blokovni algoritem; prim. pretočno šifriranje

dekodíranje -a s *(angl. decoding)* pretvarjanje kodiranega sporočila z uporabo dogovorjene kode v prvotno obliko; prim. kodiranje

dešifríranje -a s (angl. *decryption, decypherment, decrypting, decipherment*) postopek, pri katerem se tajnopis z uporabo šifrirnega algoritma in šifrirnega ključa spremeni v čistopis; prim. šifrirati

kóda -e ž *(angl. code)* sistem pravil za pretvorbo podatkov v drugo obliko, včasih skrajšano ali tajno, za komunikacijo ali shranjevanje; prim. šifra, psevdokoda, strojna koda

kodíranje -a s *(angl. encoding)* pretvarjanje sporočila v drugačno zaporedje znakov z uporabo dogovorjene kode; prim. dekodiranje

kodíranje signála -a -- s *(angl. scrambling)* spreminjanje signala s podatki tako, da ga prejemnik prepozna samo s podobno napravo

oznáka -e ž *(angl. identifier, label, ID)* kar je mogoče uporabiti za enolično označevanje česa; sin. identifikator, šifra[1]

pretočni algoritem -ega -tma m *(angl. stream algorithm)* simetrični šifrirni algoritem, s katerim se šifrira tok podatkov; prim. blokovni algoritem

pretóčno šifríranje -ega -a s *(angl. stream encryption)* simetrično šifriranje, pri katerem se uporablja pretočni algoritem; prim. blokovno šifriranje

prográmska kóda -e -e ž *(angl. program code)* zapis računalniškega programa ali dela računalniškega programa v enem od programskih jezikov; sin. koda

simétrični šifrírni algorítem -ega -ega -tma m *(angl. symmetric encryption algorithm)* šifrirni algoritem, ki za šifriranje in dešifriranje uporablja isti tajni ključ; prim. asimetrični šifrirni algoritem

šífra[1] -e ž (angl. *identifier, label*) kar je mogoče uporabiti za enolično označevanje česa; sin. oznaka, identifikator

šífra[2] -e ž *(angl. code, cipher)* pravilo za pretvorbo sporočila v neprepoznavno obliko; prim. koda, šifrirni ključ

šífra[3] -e ž *(angl. password)* gl. geslo

šifránt -a m *(angl. code list)*
1. urejen seznam šifer[1] z razlago pomena
2. nabor kriptografskih kod

šifríranje -a s *(angl. encryption, encipherment)* postopek, pri katerem se z uporabo šifrirnega algoritma in šifrirnega ključa čistopis spremeni v tajnopis; prim. dešifriranje

šifrírni ključ -ega -a m *(angl. key, encryption key)* niz znakov, ki služi za kodiranje in dekodiranje podatkov; prim. šifra