→ Objasnite substitúciu ako metódu šifrovania, dešifrujte text šifrovaný Caesarovou šifrou kľúčom 3: OLVW CQLFLW.

Cieľom šifrovania je utajiť správu tak, aby bol čas a náklady na rozlúštenie informácie cudzou osobou dostatočne veľký v porovnaní s dôležitosťou šifrovanej správy.

SUBSTITÚCIA je nahradenie jedného alebo viacerých znakov jedným alebo viacerými znakmi (v prípade počítačov môže ísť i o náhradu binárne kódovanej správy - teda náhradu bitov).

CAESAROVA ŠIFRA je najjednoduchšou substitúciou, ktorá sa dá považovať za šifru. Posunie každý znak o tri písmená v abecede. Kľúčom je v tomto prípade číslo 3. Túto šifru používal Július Caesar (100 - 44 p.n.l.). Táto šifra, pri ktorej sa každé z písmen posúva o rovnakú hodnotu, sa tiež nazýva **monoalfabetická šifra.**
Riešenie: LIST ZNICIT.

→ Vysvetlite zmysel kontroly disku, defragmentácie disku a zálohovania súborov. Ukážte na vašom počítači spôsoby spustenia týchto systémových nástrojov.

Kontrola chýb
Nástroj Kontrola disku vám môže pomôcť i v prípade, keď budete potrebovať získať dáta z disku, avšak operačný systém pri ich otváraní alebo kopírovaní hlási chybu z dôvodu poškodenia disku. Pri správnom použití tohto nástroja existuje reálna šanca, že sa požadované dáta podarí získať. Aspoň sa o to môžete pokúsiť.

Defragmentácia disku
Fragmentácia disku znamená rozptýlenie častí jedného diskového súboru na rôznych miestach disku. Fragmentácia vzniká pri odstraňovaní súborov z disku a pridávaní nových súborov. Prejavuje sa spomalením prístupu na disk a znížením celkového výkonu diskových operácií.
Program Defragmentácia disku analyzuje lokálne zväzky a konsoliduje fragmentované súbory a priečinky, takže každý obsadí vo zväzku len jedno súvislé miesto.

Zálohovanie
Súbory v počítači je potrebné pravidelne zálohovať, aby ste neprišli o vytvorené, upravené a uložené súbory. Súbory je možné kedykoľvek zálohovať manuálne, alebo je možné nastaviť automatické zálohovanie.
(Štart, položka Ovládací panel, položka Systém a údržba, položka Centrum zálohovania a obnovy.

→ Rozdeľte vírusy podľa spôsobu deštruktívnosti a odolnosti voči antivírusovým programom.

Podľa spôsobu deštruktívnosti:

- Nedeštruktívne – vizuálne a akustické prejavy
- Napádajúce programy – prepisujú programy (väčšinou stačí súbor vymazať)
- Ničiace údaje – prekódovanim, naformátovaním alebo vymazaním)
- Modifikujúce údaje – „sedia“ v počítači a občas zmenia údaj
- Odosielajúce údaje – prostredníctvom e-mailu alebo siete
- Ničiace hardvér – zapisujú sa do BIOSu počítača (modifikácia štartovacej sekvencie základnej dosky).

Podľa odolnosti voči antivírusovým programom:

- **S rovnakým kódom** – ľahko identifikovateľné
- **Polymorfné** – pri rozmnožovaní menia svoj kód
- **Stealth vírusy** – rezidentne umiestnené v pamäti (pri otváraní infikovaného súboru vírus preberie riadenie, deinfikuje súbor, po uzavretí ho znovu infikuje)