Dům dětí a mládeže
Ostrava-Poruba
příspěvková organizace

středisko DDM Polská
Polská 1624/4, Ostrava – Poruba 708 00
www.ddmporuba.cz

Pracovní list číslo 1: Jednoduchá substituce

Substituce nahrazuje jednotlivá písmena jinými písmeny či znaky. Pokud chceme změnit písmena na různé roztodivné znaky, přidá to šifře na exotičnosti., ale principy zůstávají stejné. Zde budeme zobrazovat písmena na písmena a budeme se držet konvence, že originální text bude psán malými písmeny a šifry velkými.
Nejzákladnějším a dlouhou dobu také nejpoužívanějším šifrovacím mechanismem je jednoduchá monoalfabetická substituce. Při ní se každé písmeno zobrazuje fixně na určitý znak, například:

a b c d e f g h i j k l m n o p q r s t u v w x y z
L Z Y C N O P S I R M J K V T U A E F G H B X D Q W

S pomocí této substituce zašifrujeme větu „Dočkej času jako husa klasu“ následovně:

dockej casu jako husa klasu
CTYMNR YLFH RLMT SHFL MJLFH

V uvedeném příkladu je způsob zobrazení písmen na šifrovací abecedu nesystematicky. V takovém případě je nutné mít k dispozici tabulku, která toto zobrazení udává. Tato tabulka je klíčem, a to nepříliš snadno zapamatovatelným. Takový klíč není vhodný, protože je nutné si ho zapsat, a existence psaného klíče je slabým místem jakéhokoli šifrovacího systému. Existuje však mnoho způsobů, jak toto zobrazení provést systematičtější, a tudíž bez nutnosti zápisu tabulky.

- pevný posun abecedy (posun o 3 písmena je známá *Caeserová šifra*, posun o 13 je znám jako *ROT13*);

a b c d e f g h i j k l m n o p q r s t u v w x y z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- převrácená abeceda (tzv. *ATBASH šifra*, používaná ve starý hebrejských textech);

a b c d e f g h i j k l m n o p q r s t u v w x y z
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

- lineární transformace $ax + c \ mod$ 26, kde x je číslo písmena, $a, b \in$ N, a nesoudělné s 26 (též zváno affinní šifra);
  příklad: 3x + 5

a b c d e f g h i j k l m n o p q r s t u v w x y z
F I L O R U X A D G J L P S V Y B E H K N Q T W Z C

- převod dle klíčového slova: slovo, ze kterého vynecháme opakující se písmena, tvoří začátek šifrovací abecedy, zbylá písmena doplníme v abecedním pořadí;

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz

OSTRAVA!!!

klíč: Petrklíč

a b c d e f g h i j k l m n o p q r s t u v w x y z
P E T R K L I C A B D F G H J M N O Q S U V W X Y Z

ŠIFRY – řešením rčení/citáty slavných

Příklad 1 Posun

EXILB AKLMI KTOWR GXSIR MXEGT WXCX

Příklad 2 Posun

CVGJQ UZDWV SNSVN SCJSL VSNS

Příklad 3 Jednoduchá substituce (ATBASH)

QHGV OR MZ KLXSBYZXS IRPVQGV KIZEWF

Přezdívka	**Jméno**	**Příjmení**	**Věk** (např. 10 let)	**Kontakt**
Název	**Řešení šifry**			**Počet bodů**
Příklad 1				
Příklad 2				
Příklad 3				

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz