Zadání úlohy – ADFG(V)X

Vytvořte aplikaci pro šifru ADFG(V)X, používanou během 1. světové války. Tato šifra funguje na následujícím principu:

1. Vygenerujete si náhodnou abecedu A-Z a uspořádáte ji do matice 5x5. Všechna písmena se vám do matice nevejdou, z tohoto důvodu budete nahrazovat J -> I nebo W -> V.
2. Jednotlivým řádkům a sloupcům přiřadíme indexy pomocí znaků A,D,F,G,X
3. Každý znak otevřeného textu nahradíme řádkovým a sloupcovým indexem vybraného znaku z vygenerované šifrovací tabulky, tzn. každý znak bude v šifrovaném textu představovat dvojici znaků.

V dalším kroku použijete zadané klíčové slovo, pomocí kterého bude probíhat transformace sloupců v matici.

1. Zjistíte si délku klíčového slova a podle toho rozdělíte šifrovaný text do řádků.
2. Klíčové slovo seřadíte dle abecedy spolu s příslušnými sloupci šifrovaného textu.
3. Po sloupcích přepíšeme zašifrovaný text.

Dešifrování probíhá inverzním způsobem. Tabulku jste generovali náhodně, proto musíte použít stejnou tabulku na dešifrování.

Implementujte obě varianty tj. ADFGX a ADFGVX. Rozdíl spočívá pouze ve velikosti matice, tzn. že u varianty ADFGVX použijete matici 6x6.

Popis šifry si můžete najít např. na https://en.wikipedia.org/wiki/ADFGVX_cipher.

Tento úkol je hodnocený a jeho správné, včasné a samostatné vypracování je podmínkou pro získání zápočtu.

Celkově je možno získat 10 bodů. 6 je potřeba a bude hodnoceno známkou „Prošel“

- 0,5b za správnou filtraci vstupních dat (Jak jsme zvyklí z předchozích šífer, **zachování mezer a čísel**)
- 0,5b za funkci pro vygenerování náhodné abecedy pro ADFG(V)X
- 0,5b za funkci pro ADFGX šifrování
- 0,5b za funkci pro ADFGVX šifrování
- 0,5b za funkci pro ADFGX dešifrování
- 0,5b za funkci pro ADFGVX dešifrování

- 6b za uživatelské rozhraní, které bude obsahovat pole pro zadání textu pro šifrování a dešifrování, pro zadání klíče, pro zadání šifrovací matice ručně (spolu s vyřazováním nebo znázorněních zbývajících znaků pro vyplnění), výpis zašifrovaného textu (mezeru dle sloupců), výpis aktuální šifrovací tabulky, tlačítko pro volbu šifrování dešifrování v rámci stejného GUI, přepínač pro volbu verze ADFGX (CZ/EN verze u 5x5) a ADFGVX šifry, přepínač pro volbu zadání matice a náhodného generování.
- 1b za umělecký dojem

Tento úkol odevzdejte 14 dní od zadání na cvičení. (viz podmínky k zápočtu a deadline v MOODLE)

Máte na vypracování čas 14 dní, tj do přespříštího cvičení. Je to tak schválně, abyste během příštího cvičení mohli konzultovat s vyučujícím případné problémy, co se týče naprogramování úkolu.

V případě dotazů se ptejte.