KRY - Kryptografie 2020

Projekt č. 1 - One time pad

Zadání:

Vaším úkolem je nastudovat jak funguje šifra One Time Pad. Tato šifra je považována za neprolomitelnou při splnění určité podmínky. Podmínkou je pravidlo, že klíč, který je generován náhodně, je použit pouze na jednu zprávu a dále nikdy není použit znovu. V tomto projektu byla tato podmínka porušena. Cílem Vaší práce je získat část klíče, kterým bylo zašifrováno několik zpráv.

Každému studentovi byl vygenerován klíč o délce zhruba 300 znaků. Studentovi je umožněno vygenerovat si téměř neomezený počet vět, které budou šifrovány jemu přiděleným klíčem. Jedinou informaci, kterou o dané zprávě víte je, že se jedná o text v českém jazyce bez diakritiky.

Server pro generování zpráv je dostupný na adrese pcocenas.fit.vutbr.cz. Úkolem každého studenta je prolomit danou šifru a získat co nejdelší část svého šifrovacího klíče.

Formát odezvdání

Do wisu se odvevzdává archiv xlogin00.zip a v něm soubor xlogin00.txt, který bude obsahovat šifrovací klíč. Klíč do souboru uložte v binárním formátu. Příklad odevzdaní je zde.

Dotazy k projektu směřujte primárně na fórum. Konzultace poskytuje: iocenas@fit.vutbr.cz
Datum odevzdání: 3.5.2020