Jméno a příjmení: Jan Kubiš
Login: xkubis13

Dokumentace k 1. projektu KRY 17/18

(Zjišťování klíče)

- **Ruční řešení**

V zipu se vstupními soubory se nachází soubory „bis.txt“ a jeho zašifrovaná verze „bis.txt.enc“. Funkcí XOR obsahů těchto souborů získáme keystream o délce 512B. Jelikož se jedná o synchronní šifru, keystream se v závislosti na vstupních datech pro šifrování nemění. Za (správného) předpokladu, že byl při šifrování ostatních souborů použit stejný klíč, můžeme funkcí XOR získaného keystreamu a obsahu souboru „super_cipher.py.enc“ získat prvních 512B plaintextu tohoto souboru. Uvnitř lze najít algoritmus, jakým je keystream generován.

Klíčová je funkce step, která přijímá vstup x a z něj vypočítá výstup y (vždy o velikosti 32B). Nejprve určitým způsobem transformuje x, a to tak, že jej zleva rozšíří o LSb(x) a zprava o MSb(x). Tento tvar nazvěme x'={LSb(x)|x|MSb(x)}. Poté v cyklu provádí nad x' bitový posun doprava, pomocí spodních tří bitů takto posunutého x' vybere prvek z předem daného pole SUB a v každé iteraci jej napojí k výstupnímu y zleva. Tento proces je proveden několikrát za sebou, což ale nehraje velkou roli (inverzní step provedeme stejný počet krát).

Získaný keystream je tedy výsledek v proměnné y, my se budeme snažit získat x. Víme, že se do proměnné y přidávaly bity zprava doleva, my tedy půjdeme opačným směrem. Vezmeme nejlevější bit, a zjistíme, jak mohl vzniknout - vznikl na základě určitého indexu do pole SUB (celkem 4 možnosti pro 0 i pro 1). Uložíme si všechny 4 možnosti, které budeme sledovat i dále. Další bit vznikl opět na základě určitého indexu do pole SUB, ale víme, že tento index sdílí s předchozím indexem minimálně 2 bity (x se ve funkci step při každé iteraci posune o jeden bit, nicméně indexace probíhá na základě tří bitů). Uložíme si tedy tyto indexy k odpovídajícím možnostem. Po odpovídajícím počtu kroků (N) máme 4 různá pole indexů o délce N. Jelikož se funkce step volá v cyklu, před spuštením dalšího cyklu musíme zjistit, která z těchto možností je správná, jinak by došlo k exponenciálnímu růstu počtu možností. To uděláme tak, že jednotlivá pole indexů převedeme na řetězec bitů (z prvního prvku pole bereme všechny 3 bity, z dalších už po jednom), čímž dostaneme potenciální x'. Po adekvátní uprávě (odseknutí MSb a LSB) získáme potenciální vstup x (celkem 4 různé možnosti). Správné x lze zjistit zavoláním funkce step nad každou z možností a porovnání výstupu s naším původním výstupem (v první iteraci porovnání s keystream). Tím získáme správný vstup x.

Tento postup (inverze funkce step) se poté zavolá tolikrát, kolikrát byla zavolána funkce step. Po doběhnutí všech iterací získáme původní klíč, ze kterého byl výsledný keystream vytvořen.

- **SAT řešení**

Zjištění klíče pomocí SAT solveru není implementováno.