KRY - Projekt 1
Synchrónna prúdová šifra

Patrik Segedy, xseged00

Získanie keystreamu a algoritmu

Najprv je potrebné získať keystream a pomocou neho rozšifrovať `*.enc` súbory. Keystream získame útokom `Known plaintext attack`, použití operácie `XOR` na súbory bis.txt a bis.txt.enc.Získavame `512B` dlhý keystream na základe ktorého môžeme dešifrovať prvých `512B` zašifrovaného algoritmu `super_cipher.py.enc`. Prvých `512B` algoritmu je dostatočných na zistenie spôsobu vytvorenia keystreamu. Pomocou funkcie `step()` aplikovanou na keystream vieme tento keystream predĺžiť a následne dešifrovať celé súbory `super_cipher.py.enc` a `hint.gif.enc`.

Ručné riešenie

Riešenie pozostáva z reverzácie funkcie `step()`, ktorou bol z kľúča inicializovaný keystream. Šifrovanie pomocou funkcie `step()` pozostáva z dvoch krokov. Prvým je rotácia vstupu a druhým je substitúcia podľa 3 bitov vstupu, ktoré indexujú pole SUB.
Z poľa `SUB` si všimneme, že výstup 0 vznikol z trojice bitov `[000, 011, 101, 111]` a výstup 1 z `[001, 010, 100, 110]`. Ak vezmeme prvý bit zľava z keystreamu, získavame teda 4 možnosti ako mohol vzniknúť. Uložíme si 4 možnosti trojíc bitov z ktorých mohol prvý bit vzniknúť. Tri bity z ktorých vznikol ďalší bit keystreamu zľava zdieľa 2 bity s predchádzajúcim riešením. Na základe hodnoty aktuálneho bitu keystreamu teda doplníme každé z potenciálnych 4 riešení o jeden bit, tak aby sme zo spodných 3 bitov dokázali vytvoriť aktuálny bit keystreamu.
Po prejdení všetkých bitov a získaniu 4 možných riešení, tieto riešenia rotujeme inverzne voči rotácii z funkcie `step()` a nad každým z riešení zavoláme funckiu `step()`, čím zistíme ktoré riešenie je správne.
Celý postup opakujeme toľkokrát, koľkokrát bola zavolaná funkcia `step()` pri inicializácii keystreamu.
Výsledkom je kľúč, ktorým bol algoritmus inicializovaný.

Riešenie pomocou SAT solveru

Pri riešení pomocou SAT solveru bola využitá knižnica `satispy` pre jazyk `Python`. Riešenie spočíva vo vytvorení formuly v konjunktívnej normálnej forme, ktorá popisuje každý bit kesytreamu, kde každý bit je reprezentovaný jednou premennou.

Formulu získame spojením formúl pomocou operátoru `AND` každého bitu keystreamu. Kde formulu v KNF pre bit 1 získame pomocou Karnaughovej mapy pre pole SUB kde hodnoty nadobúdajú 1. Výsledkom je MNKF $(A + B + C) * (\overline{B} + \overline{C}) * (\overline{A} + \overline{C})$, formulu pre bit 0 z keystreamu získame negáciou formuly pre 1.
Minisat pre takto zadanú formulu nájde ohodnotenie premenných, ktoré vyhovuje riešeniu. Z ohodnotenia premenných následne poskladáme hľadaný kľúč tak, že pre ohodnotenie premennej `True` dáme na výstup bit 1 a pre ohodnotenie `False` dáme na výstup bit 0. Následne doriešime rotáciu ako pri ručnom riešení, reverzáciu opäť opakujeme (`N // 2`) krát a získavame kľúč, ktorým bola šifra inicializovaná.