Návrh a kryptoanalýza šifier

Zadanie 1

Peter Čuřík

Výsledok

PT: `In October, 1805, a Russian army was occupying the villages and towns of the Archduchy of Austria, and yet other regiments freshly arriving from Russia were settling near the fortress of Braunau  and burdening the inhabitants on whom they were quartered.`

Key: `6237AD5C00000000000000000000000`

Použitý HW a SW na výpočty

HW

SW

Naprogramovanie riešenia v jazyku Python s pomocou knižnice pycryptodome
Rozdelenie problému medzi všetky virtuálne jadrá CPU (8)

Riešenie a analýza

-- jadrá si keyspace rozkrájajú na 8 častí a každé rieši svoju časť od najväčšieho kľúča po najmenší (v zmysle integer hodnoty hexa kľúča) v danom intervale
-- okolo 30 000 000 pokusov na jadro za hodinu
-- správny PT je ten, ktorý sa podarí dekódovať pomocou UTF-8
-- prehľadaný priestor kľúčov: 87.5% (cca 3 760 000 000 kľúčov)
-- čas: 13,7h (104h po sčítaní času všetkých jadier (jedno ukončilo svoju činnosť skôr))

Overhead

Výsledok príkazu `openssl speed aes-128-cbc` na mojom HW:

```
Doing aes-128 cbc for 3s on 256 size blocks: 1363594 aes-128 cbc's in 3.00s
```

Uvažujeme, že CT má veľkosť približne 256 bajtov.
Z uvedeného vyplýva, že za 1s stíha openssl dešifrovať CT 454 531 krát.
openssl by trvalo 2,2h aby prešlo toľko blokov, čo moje riešenie (vyše 47x rýchlejšie)

Podľa vzorca pre Overhead = T/Tref * 100 - 100, kde

- T je čas môjho riešenia,
- Tref je čas, koľko by to trvalo openssl

by sa Overhead v tomto prípade rovnalo 4 627,27%.