Návrh a kryptoanalýza šifier

Zadanie 1

Pavol Sobota

1. Teoretické informácie

1.1 Operačný systém a softvér

Pracujeme s CPU procesorom Mac M1:

```
Model Name: MacBook Air
Model Identifier: MacBookAir10,1
Chip: Apple M1
Total Number of Cores: 8 (4 performance and 4 efficiency)
Memory: 8 GB
System Firmware Version: 6723.140.2
OS Loader Version: 6723.140.2
Serial Number (system): C02GF2PZQ6L7
Hardware UUID: 9A343954-E30D-531C-AE75-0CFBC3F54D53
Provisioning UDID: 00008103-001439603A60801E
Activation Lock Status: Disabled
```

Dodatočné informácie:

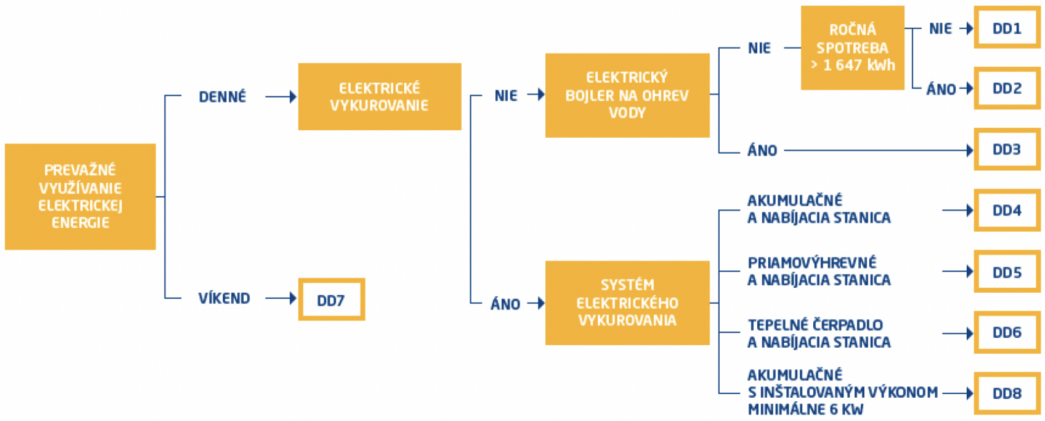
```
machdep.cpu.brand_string: Apple M1
machdep.cpu.core_count: 8
machdep.cpu.cores_per_package: 8
machdep.cpu.logical_per_package: 8
machdep.cpu.thread_count: 8
machdep.user_idle_level: 0
machdep.deferred_ipi_timeout: 64000
machdep.lck_mtx_adaptive_spin_mode: 1
machdep.time_since_reset: 101760778597
machdep.virtual_address_size: 47
machdep.wake_abstime: 102980618481
machdep.wake_conttime: 4246899719445
```

Verzia openssl protokolu:

```
pavolskumaprospektykapitalizmu@ghuztc ~ % openssl version
LibreSSL 2.8.3
```

1.2 Sadzba za elektrinu

Najprv treba zistiť v akej sadzbovej skupine sa nachádzame. Riadime sa podľa grafu uvedeného na stránke SSE. https://www.sse.sk/domacnosti/elektrina/sadzby?page_id=5521



Tým pádom vieme vyvodiť že sme v skupine DD2 a dokážeme dohľadať potrebné informácie o tom aká je sadzba za spotrebu 1 kWh. Informácie o cene spotreby sme získali zo zdroja pre ZSE.
https://www.zse.sk/documents/13897953/Cennik_domacnosti_EE_01012019.pdf

2. DomovKlasik - DD2

DomovKlasik - DD2		
Sadzba je zložená z:	bez DPH [€]	s DPH [€]
a) mesačnej platby za jedno odberné miesto [€/mes.]	0,7500	0,9000
b) ceny za elektrinu [€/kWh]	0,0568	0,0682

DomovKlasik - DD2 - jednopásmová sadzba s vyššou spotrebou elektriny.

Sadzba dodávky elektriny DomovKlasik - DD2 môže byť dohodnutá, len ak pre distribúciu elektriny do odberného miesta bude dohodnutá zodpovedajúca distribučná sadzba pre odberateľov elektriny v domácnosti s charakteristikou najbližšie zodpovedajúcou sadzbe dodávky elektriny DomovKlasik - DD2.

2. Výpočet

2.1 OpenSSL

Po zbehnutí príkazu openssl speed pre dekrypciu šifry aes s veľkosťou kľúča 128 bitov sme dostali nasledujúce výsledky.

```
pavolskumaprospektykapitalizmu@ghuztc NKS-2022 % openssl speed -decrypt -elapsed aes-128-cbc
You have chosen to measure elapsed time instead of user CPU time.
Doing aes-128 cbc for 3s on 16 size blocks: 56385979 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 64 size blocks: 14753288 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 256 size blocks: 3737077 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 1024 size blocks: 928816 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 8192 size blocks: 117259 aes-128 cbc's in 3.00s
LibreSSL 2.8.3
built on: date not available
options:bn(64,64) rc4(ptr,int) des(idx,cisc,16,int) aes(partial) blowfish(idx)
compiler: information not available
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
aes-128 cbc     300640.24k   314218.77k   318797.56k   317039.88k   319690.88k
```

Z pozorovania `56 385 979 aes-128 cbc in 3.00s` sme prepočítali že náš stroj vie za sekundu dešifrovať 18 987 917 aes blokov o veľkosti 16 bajtov. Na prepočítanie priestoru kľúčov s počtom 2^{64} (priestor všetkých permutácii kľúča s veľkosťou 64 bitov *) budeme potrebovať 971,499,089,326 sekúnd čo je v prepočte 269,860,858 hodín, 11,244,202 dní a 30,784 rokov.

*Za predpokladu, že pre kľúč s veľkosťou 64 bitov je rovnaká algoritmická zložitosť, ako pre klúč s 128 bitmi. A nie je potrebné pozmeniť dešiforvací algoritmus, ktorí využíva openssl speed.

2.2 Elektrická spotreba

Túto sme vypočítali pomocou vzorca kde P je výkon počítača pri najväčšom zaťažení a t je čas dešifrovania.

$$E_{(\mathrm{kWh})} = P_{(\mathrm{W})} \times t_{(\mathrm{hr})} / 1000$$

A následne prenásobili súčasnou spotrebou energie za 1 kWh. A pripočítali mesačný poplatok za elektrické pripojenie v domácnosti. To nám spolu vychádzalo 39W * 269,860,858 * 0,0682€/kWh / 1000. Čo nám dokopy dáva 717,775.87 € k čomu keď pripočítame mesačný poplatok za pripojenie do siete, dostaneme sumu 717,775.87 € + 332,467 € = 1,050,242 €

3 Záver

Pre náš osobný počítač sme zistili, ako časovo aj finančne náročné bude možné prehladať priesor kľúčov s veľkosťou 64 bitov. V práci nie je uvedená alternatíva pomocou GPU ani Cloudového nástroja.