

Skr3k4j n4gr4d0: izziv št. 4

Končno je na vrsti zahtevnejši izziv, za katerega upam, da boste porabili več kot le nekaj uric programiranja.

Glavni kriptogram je šifriran z algoritmom Blowfish v bločnem načinu CBC in je objavljen tukaj: <http://www.nevarnost.org/store/competition/kriptogram4.enc> .

Za dešifriranje kriptograma potrebujete geslo, katerega kriptogram pa ste uspeli prestreči med poslušanjem šifrirane povezave med nekim odjemalcem ter strežnikom. Ta pomožni kriptogram je šifriran z neznanim simetričnim šifrirnim algoritmom v bločnem načinu CBC v pomožnem kriptogramu, ki se v heksadecimalni obliki glasi:

```
0802 0401 2010 8040 00dc df76 8143 aea3 6d40 8cb7 2730 fde3
```

K sreči ste si zapomnili tudi IP naslov ter vrata strežnika, kamor je bil pomožni kriptogram poslan, to je **89.212.6.198**, vrata pa so **9002 TCP**. Poleg tega ste na internetu našli celo specifikacijo za ta posebni protokol, ki sta ga odjemalec ter strežnik uporabljala.

Definicija protokola sledi:

Odjemalec	Smer	Strežnik
<i>Vzpostavitev TCP seje na vratih 9002</i>		
	←	1 bajt z vrednostjo 0x01 (potrditev povezave)
1 bajt z vrednostjo 0x01 (napoved para blokov)	→	
2 bloka kriptograma velikosti 8 bajtov (skupaj 16 bajtov)	→	
	←	1 bajt z vrednostjo 0x01, če je bilo dešifriranje uspešno, oziroma 0x00, če dešifriranje ni bilo uspešno
1 bajt z vrednostjo 0x01 (napoved še enega para blokov)	→	
2 bloka kriptograma velikosti 8 bajtov (skupaj 16 bajtov)	→	
	←	1 bajt z vrednostjo 0x01, če je bilo dešifriranje uspešno, oziroma 0x00, če dešifriranje ni bilo uspešno
...
1 bajt z vrednostjo 0x00 (prekinitev povezave)	→	

Torej strežnik (ki šifrirni ključ pozna) ima celo to lastnost, da vam, če mu pošljete dva bloka kriptograma (blok je dolg 8 bajtov), pove, ali je bilo dešifriranje uspešno ali ne.

Čistopis glavnega kriptograma je glasbena datoteka v formatu *.ogg* znanega slovenskega kantavtorja. Rešitev izziva so prve tri besede, ki jih avtor v skladbi zapoje.

Ko boste mnenja, da ste rešitev (torej iskane tri besede) našli, jo pošljite na elektronski naslov skr3k4j@nevarnost.org, zadeva pa naj bo "Skr3k4j n4gr4d0: izziv št. 4". V primeru, da bo rešitev pravilna, vas bomo povprašali po naslovu, kamor naj nagrado pošljemo. Prosimo, da poleg rešitve same, na kratko opišete še postopek reševanja ter podate (ne)dovoljenje za objavo vašega imena v primeru pravilne rešitve.

Izziv pripravil: Nejc Škoberne