Megoldások – sztegano-hacking 2010

Bevezetés

Ezen dokumentum a szteganográfiai feladat megoldását tartalmazza. A feladat 6 különböző rejtési módszert tartalmaz.

1. Vesszős rejtés

A módszer kihasználja a bizonyos szavak esetén tapasztalható helyesírási bizonytalanságokat – jelen esetben az „and”, „or”, „which” és „that” szavak előtti vessző meglétét. Szándékosan olyan szavakat választottunk, amelyeknél a helyesírás még az angol anyanyelvűek körében is ingadozni szokott.
A rejtés során 0 bitet jelent az előbb felsorolt szavak előtti vessző hiánya, 1 bitet jelent a vessző megléte.
Megfejtéséhez a helyesírási ismeretekből, valamint a szavak előtti vesszők gyakoriságának eltéréséből lehet következtetni, majd a dekódolt bitek az ASCII-kódtáblából már könnyen megfejthetőek.

2. UTF karakteres rejtés

A módszer a hasonló karakterek módszerén alapul. A karakter kódtáblákban több, egymástól csak néhány pixelben eltérő karakter van. Ezek cserélgetésével rejtettünk információt. 0 bitet jelent a megszokott ASCII-karakter, 1 bitet jelent az UTF-8-as helyettesítő társa.
A rejtés során használt karakterek: ('O', 'K', 'M', 'H', 'P', 'C', 'T', 'X', 'a', 'I', 'J', 'B');
Megfejtéshez a karakterek kódjait érdemes megnézni pl. hexaszerkesztővel, valamint könnyen szemet szúrhat a rejtés, ha a böngészőben karakterkódolást váltunk.

3. HTML attribútumok cseréje

A rejtés során azt használtuk ki, hogy a HTML attribútumoknak nincs megkötött helyük a „kacsacsőrök” közt, tehát sorrendezésükkel információt lehet rejteni, méghozzá a következőképpen:

N: az attribútumok száma
k: rejthető bitek száma

$N! <= 2^k$, ahol a „!” a faktoriális művelet jelölése.

Megfejtés: A HTML-dokumentum végén azok a tagek, melyekben nem történt rejtés, abc-sorrendben vannak, így ezek szemet szúrhatnak. Ezek után már csak egy egyszerű algoritmus kell, hogy megállapítsuk, hogy a rendezett attribútumok hányadik permutációban (sorrendben) szerepelnek az adott esetben, és ezt visszaváltva bináris számmá, megkapjuk a rejtett információt.

4. HTML tagek

A módszer azt használja ki, hogy a böngésző nem törődik azzal, hogy a HTML-tageket alkotó karakterek kis- vagy nagybetűsek-e. Így az oldal megjelenítése nem változik a tagek betűnagyságainak változtatásával.
A rejtés során mind a nyitó, mind a záró taget felhasználtuk a rejtéshez. A kisbetű 0-t a nagybetű 1-et jelent.
Megfejtés során könnyen láthatóak a tagek neveiben az eltérések. Talán ez a legkönnyebben felfedezhető rejtés…

5. Szóközös rejtés

A rejtés során a sor végére helyezett szóközökkel rejtettünk információt. Szemmel nem láthatóak a szóközök, de egy egyszerű kijelöléssel könnyen detektálhatóvá válnak.

Ha a sor végén nincs szóköz: 0, ha a sor végén van szóköz: 1.

6. RLE-LSB

Az LSB-n alapuló szteganográfia a képi információrejtés állatorvosi lova – többek között az angol Wikipedia Steganography c. szócikkében is szerepel. Itt csak annyi a bonyolítás, hogy az LSB rejtés előtt konvertáljuk az elrejtendő információt futamhosszkódolással (Run-length Encoding, RLE), méghozzá bitszinten. Az eredményül kapott bájtokban az MSB jelöli a futam által hordozott bitet, a többi bit pedig a futam hosszát. Ha a versenyző LSB módszerrel kinyeri az információt a képből (amit előtte BMP formátumba konvertált a veszteségmentes tömörítést használó PNG-ből), akkor látni fogja, hogy az első nagyjából 12 bájtban az MSB szisztematikusan alternál, és ezek után egy 0 bájt következik. Ha az MSB váltakozását észreveszi, feltehetőleg már viszonylag könnyen rájön, hogy a többi bit jelöli a futamhosszt, annál is inkább, mert ezek a számok nagyon kicsik (mivel nyomtatható ASCII-karakterek sorozatát rejtettük). A weblapon három kép van elhelyezve, de abból csak az egyik tartalmaz rejtett információt, a másik kettőben nem rejtettünk semmilyen adatot.

A rejtések sorrendje és a rejtett információ

1. Vesszős rejtés: BReb
2. UTF betűs rejtés: 7W72mepafrUc
3. html attributum cserélő: decoy
4. html tag név változtató: tinyurl
5. szóközös: Decoy!
6. RLE-LSB: Asw4

A végső titok összeállítása

Ha a visszafejtés eredménye egy algoritmussal „decoy”, akkor értelemszerűen adódik, hogy ez nem része a titoknak. A maradék kinyert információmorzsák közül a „tinyurl” megmutatja, hogy egy tinyurl-lel rövidített címről van szó. A maradék három részletnek hatféle konkatenációja lehetséges, ezek végigpróbálgatásával kiadódik a „végállomást” jelentő cím: http://tinyurl.com/BReb7W72mepafrUcAsw4