Algorithms of Information Security: Steganography - exercises

Faculty of Information Technology
Czech Technical University in Prague

December 9, 2020

Skrýtá zpráva

Úloha.
Jedním z potenciálních nosičů pro skrytí zpráv na internetu je spam. Zkuste se podívat na následující text a uhodněte v něm skrytou zprávu.

Skrýtá zpráva - část 1

Dear Friend , We know you are interested in receiving cutting-edge announcement . This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 1816 , Title 4 , Section 305 . This is a ligitimate business proposal ! Why work for somebody else when you can become rich in 10 WEEKS . Have you ever noticed most everyone has a cellphone and most everyone has a cellphone . Well, now is your chance to capitalize on this ! We will help you increase customer response by 170% plus SELL MORE . You can begin at absolutely no cost to you ! But don't believe us ! Prof Ames who resides in Utah tried us and says "My only problem now is where to park all my cars" . We assure you that we operate within all applicable laws . DO NOT DELAY - order today ! Sign up a friend and you'll get a discount of 70% .

Skrýtá zpráva - část 2

Thank-you for your serious consideration of our offer ! Dear Cybercitizen ; You made the right decision when you signed up for our mailing list . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our database . This mail is being sent in compliance with Senate bill 1622 ; Title 8 , Section 309 ! THIS IS NOT A GET RICH SCHEME . Why work for somebody else when you can become rich in 86 MONTHS . Have you ever noticed most everyone has a cellphone plus most everyone has a cellphone ! Well, now is your chance to capitalize on this . We will help you SELL MORE plus SELL MORE ! You can begin at absolutely no cost to you . But don't believe us . Mrs Simpson who resides in Wyoming tried us and says "I was skeptical but it worked for me" . We assure you that we operate within all applicable laws ! If not for you then for your LOVED ONES - act now ! Sign up a friend and your friend will be rich too . Thank-you for your serious consideration of our offer .

Řešení.

- Táto zpráva vypadá jako typický spam, který obvykle ignorujeme a odstraňujeme z e-mailové schránky.
- Zpráva byla vytvořená pomocí *spam mimic*. Odkaz https://www.spammimic.com/index.cgi
- Je to webová stránka, která převádí krátkou textovou zprávu na textový blok, který vypadá jako typický spam.
- Třetí strana nezjistí nic všimaním nebo rozestupem mezer nebo gramatických chýb.
- Skrytá zpráva ve spamu výše je: Cviceni ze steganografie

Úloha.
Předpokládejme, že máme následující mřížku pro 3 pixely 24bitového obrázku:

$$(001011010001110011011100)$$

$$(101001101100010000001100)$$

$$(110100101010110101100011)$$

a chceme do ní vložit pomocí metody LSB zprávu: 200.

Řešení.

- Nejprve 200 převedeme do binární soustavy. Tedy máme 11001000.
- Dále vložíme číslo 200 za použití metody LSB s využitím posledního bitu do mřížky pixelů.
- Dostaneme následující výsledek:

$$(00101101\ 00011101\ 11011100)$$

$$(10100110\ 11000101\ 00001100)$$

$$(11010010\ 10101100\ 01100011)$$

- Tučně jsou vyznačeny bity, které tvoří tajnou zprávu a bity, které se změnily oproti originálu, jsou podtrženy.
- Z příkladu vidíme, že je poměrně pravděpodobné, že bity, které chceme zapsat, se již shodují se zapsanými, a tudíž nedochází ke změně.

Úloha

Předpokládejme, že máme 2 následující pixely 24bitového obrázku: První je binárně $(00110111\ 01010101\ 01101111)$ a druhý je $(00010011\ 00111010\ 01011011)$ a chceme do nich vložit písmeno A za použití metody LSB s využitím posledních dvou bitů.

Řešení.

- Nejprve písmeno A převedeme do binární soustavy. Víme, že znak A je dekadicky ASCII 65.
- Tedy binárně máme 01000001. Dále tučně označíme nahrazované bity a poslední 2 byty zůstanou nedotčené, jelikož nezapisujeme více než písmeno A:

$$(00110\mathbf{11}\ 01010\mathbf{01}\ 01101\mathbf{11})$$

$$(00010\mathbf{11}\ 00111010\ 01011011)$$

- Dostaneme následující výsledek:

$$(00110\mathbf{0}1\ 0101010\mathbf{0}\ 01101\mathbf{00})$$

$$(00010\mathbf{0}1\ 00111010\ 01011011)$$

- Tučně jsou vyznačeny bity, které se změnily oproti originálu.

OpenStego - https://www.openstego.com/

- OpenStego je steganografická aplikace, která poskytuje dvě funkce:
  - Skrývání dat: Může skrýt jakákoli data v krycím souboru (např. Obrázky).
  - Vodoznak: Vodoznak souborů (např. Obrázky) s neviditelným podpisem. Lze jej použít k detekci neoprávněného kopírování souborů.
- Tento nástroj je napsaný v jazyce Java a měl by běžet na všech platformách podporovaných Javou. Podporovány jsou MS Windows a Linux a neměl by mít problém ani na jiných platformách.
- Umožňuje šifrovat informace na základě algoritmů AES 128 a AES 256.
- Pro ukrývání informací využívá algoritmus RandomLSB (Randomized LSB) a pro tvorbu vodoznaku Dugadův algoritmus.
- Příkladem podporovaných vstupních souborů jsou JPEG, GIF, BMP nebo PNG.

Úloha.
Nejprve si nainstalujte software OpenStego.

- Vytvořte tajnou zprávu (.txt soubor), kterou chcete skrýt do obrázku. Zvolte obrázek do kterého skryjete zprávu. Pomocí software OpenStego do Vámi zvoleného obrázku skryjte nějaký tajný text a uložte si výsledný soubor.
- Pomocí software OpenStego získejte tajnou zprávu uloženou v novém obrázku.

Můžeme také vytvořit vodoznak, pomocí kterého je možné ověřit obrázky s naším podpisem. Nejprve musíte vygenerovat podpisový soubor a poté jej lze použít k vytvoření vodoznaku nebo jeho ověření později.

Úloha.
Pomocí software OpenStego:

1. Vygenerujte podpisový soubor, který potom použijete k vytvoření vodoznaku.
2. Vytvořte vodoznak.
3. Ověřte vodoznak.