Steganography using RSA and MP3

A Practical Implementation

John Shaver
What is Steganography?

- Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message; a form of security through obscurity.

- Wikipedia.org
Why should anyone care?

- Encrypted information attracts attention.
- Possession and use of encryption software heavily regulated/banned in: China, Iran, Russia, Singapore, Venezuela, etc.
  - EPIC.org

- Man in UK jailed for not revealing password (a few weeks ago)
Why should anyone care?

- Not just other countries
  - Carnivore
  - Laptop seizures at US borders

- Article by Bruce Schneier - *Taking your laptop into the US? Be sure to hide all your data first*
Digital Media as a Transport Vector For Other Information

- Requires unaltered original to confirm steganography
- Image files ideal
- Compressed files trickier
  - Less “extra” space
  - Data corruption magnified during decompression
MP3 File Structure

- Stored as thousands of pages, each representing approximately 26 ms
- Encoding algorithms not standardized
  - Varying page sizes
MP3 File Structure

- Some MP3 encoders include page checksum
- Feasible to detect periodic data alteration
- Non-periodic much more difficult to determine embedded data from “noise”
MP3Steg

- Goal: Embed RSA-encrypted text message into an MP3 file such that:
  - Still looks like an MP3 file
  - Behaves as expected
MP3Steg

Usage

- GUI Interface
- Supply RSA modulus, encryption/decryption keys of arbitrary length
- Supply MP3 file
  - Ideally a unique encoding
- If encrypting, input text
- Wait..
MP3Steg
Details

- Written in Java
- Uses BigInteger class
- Pseudo-random seed varies interval length between data-bytes
- Uses simple ASCIIPad representation
MP3Steg
Details

- Encrypt option creates new MP3 file
- Exactly the same number of bytes
- Original should be destroyed