Steganography

Encryption in Plain Sight

1 Types of Steganography

Pure Steganography

- Pure Steganography is the simplest form of steganography
- Involves no keys, or key exchanges
- Pure Steganography can be defined as the quadruple (C, M, E, D) where:
  - C: is the set of possible covers
  - M: is the set of possible secret messages where $|C| \geq |M|$
  - E: $C \times M \rightarrow C$ is the embedding function
  - D: $C \rightarrow M$ is the extraction function
  - With the property that $D(E(c, m)) = m$ for all $m \in M$ and $c \in C$

Secret Key Steganography

- Secret Key Steganography involves only a single key
- If the secret key is known to the receiver, he can reverse the process and extract the secret message
- Secret Key Steganography can be defined as the quintuple (C, M, K, E_k, D_k) where:
  - C: the set of possible covers
  - M: the set of possible secret messages
  - K: the set of possible secret keys
  - E_k: $C \times M \times K \rightarrow C$
  - D_k: $C \times K \rightarrow M$
  - With the property that $D_k(E_k(c, m, k), k) = m$ for all $m \in M$, $c \in C$ and $k \in K$

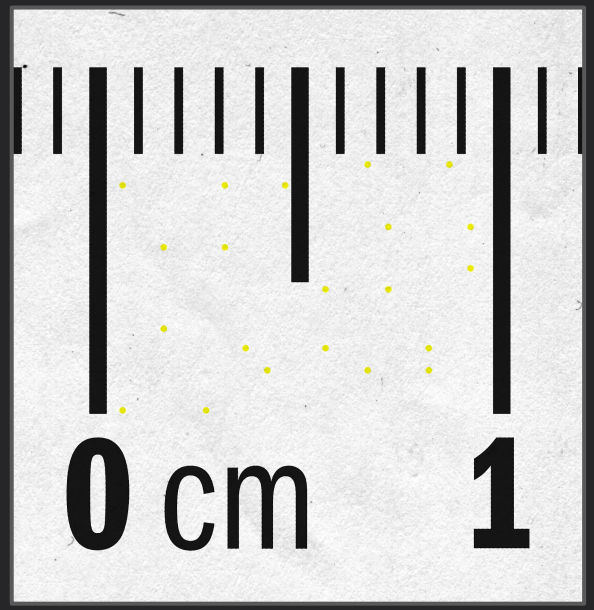
Public Key Steganography

- Public key Steganography does not depend on the exchange of a secret key. It requires two keys, one of them private and the other public:
  - The public key is used in the embedding process
  - The secret key is used to reconstruct the secret message
- Public key Steganography relies on the fact that encrypted information is random enough to hide in plain sight
- The sender encrypts the information with the receiver's public key to obtain a random-looking message and embeds it in a channel known to the receiver
- Public Key Steganography can be defined as the sextuple (C, M, KU, KR, E_{KU}, D_{KR}) where:
  - C: the set of possible covers
  - M: the set of possible secret messages
  - KU: the public key
  - KR: the private key
  - E_{KU}: $C \times M \times KU \rightarrow C$
  - D_{KR}: $C \times KR \rightarrow M$
  - With the property that $D_{KR}(E_{KU}(c, m, KU), KR) = m$ for all $m \in M$, and $c \in C$

2 Areas of Applications

Applications

- Printers
  - model, serial number, and timestamps
- Money
- Watermarking
- Malware



3 Mathematics & Methodology

Substitution Systems

- Least Significant Bit
  - Substitute the least significant bit of each cover-element with the bit of a secret message
  - Most Common Method
- Random Interval
  - A pseudorandom number generator is used to spread the secret message over the cover-elements in a random manner
  - Sender and receiver share a secret key as a seed for a random number generator
  - A random sequence is created and an interval between two embedded bits is determined
  - The secret message bits are stored according to the interval

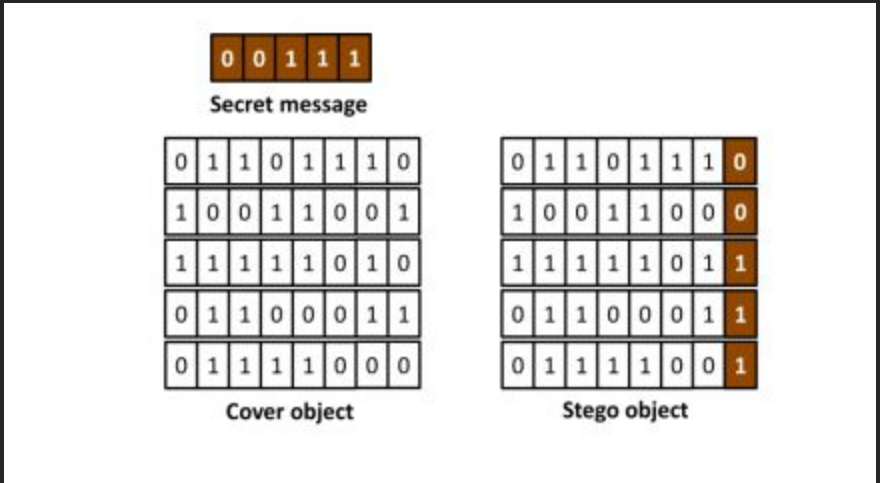
Substitution Systems (cont.)

- Pseudorandom Permutation
  - Distribution of the secret message is done in random manner over the whole cover-elements
  - Increases the complexity for an attacker because there is no guarantee that subsequent message bits are embedded in the same order
  - A sequence is generated using a pseudorandom number generator, and secret message bits are stored according to bit position of cover-elements determined by the generated sequence
- Image Downgrading
  - Given a cover-image and secret image of equal dimensions, the sender exchanges the four least significant bits of the cover's color values with the four most significant bits of the secret image

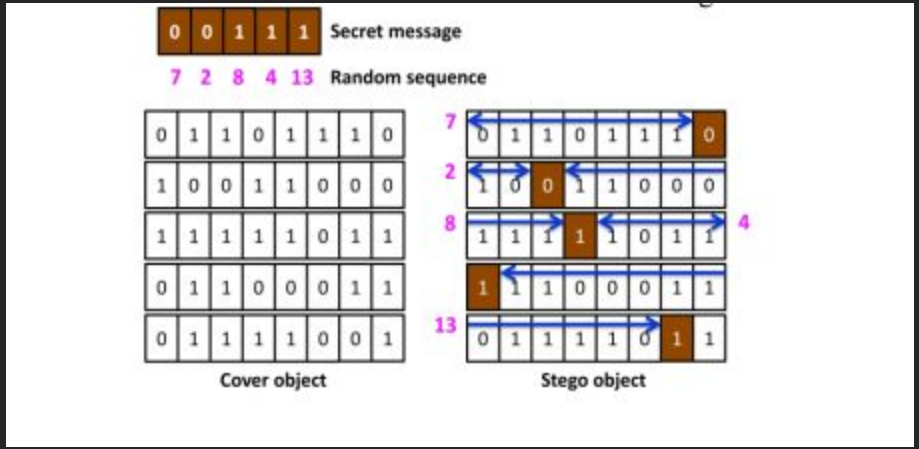
Substitution Systems (cont.)

- Cover-regions and Parity Bits
  - A stego-key is used as the seed to generate pseudorandom sequence of disjoint cover-regions
  - Cover-region length is calculated by dividing the cover image length with the message length
  - Only one bit of the secret message is stored in a whole cover-region rather than in a single element
  - In the embedding process, disjoint cover-regions are selected, each encoding one secret bit in the parity bit
  - A parity bit of a region can be calculated by the number of 1's mod 2
  - One LSB of a random chosen cover-element is flipped if the parity bit of the cover-region does not match with the secret bit to encode
  - The parity bits of all the selected cover-regions are calculated and lined up to reconstruct the message at the receiver

Least Significant Bit



Random Interval



Pseudorandom Permutation

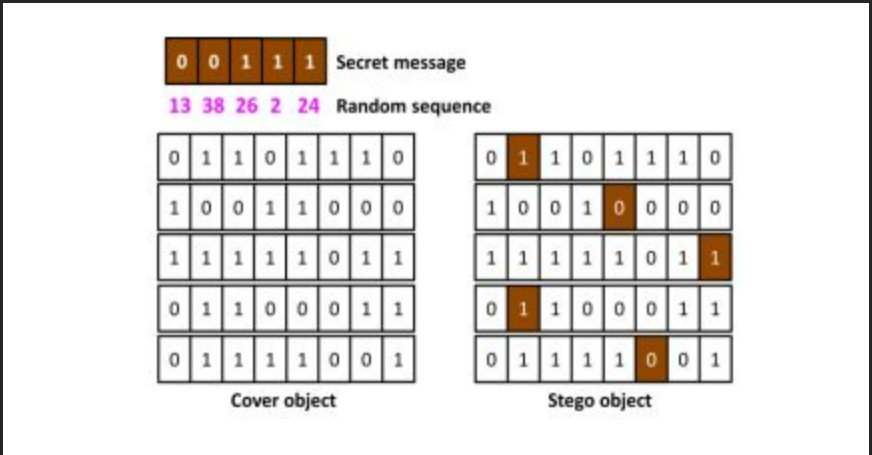
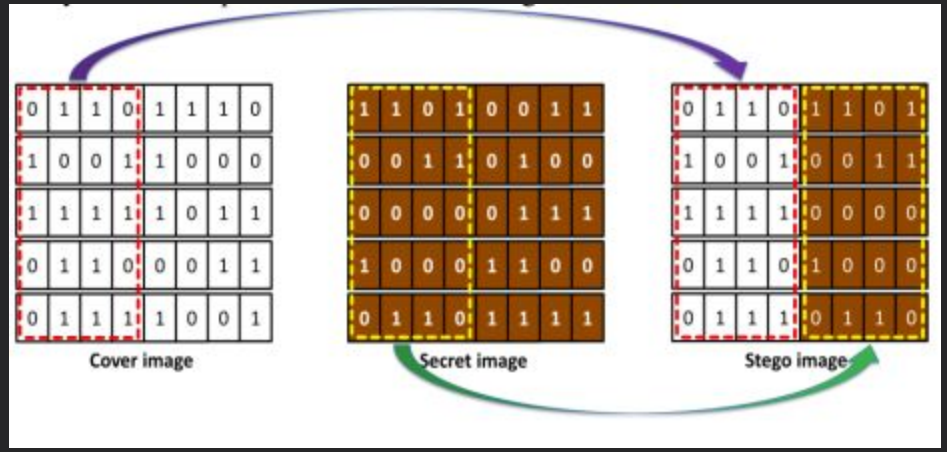
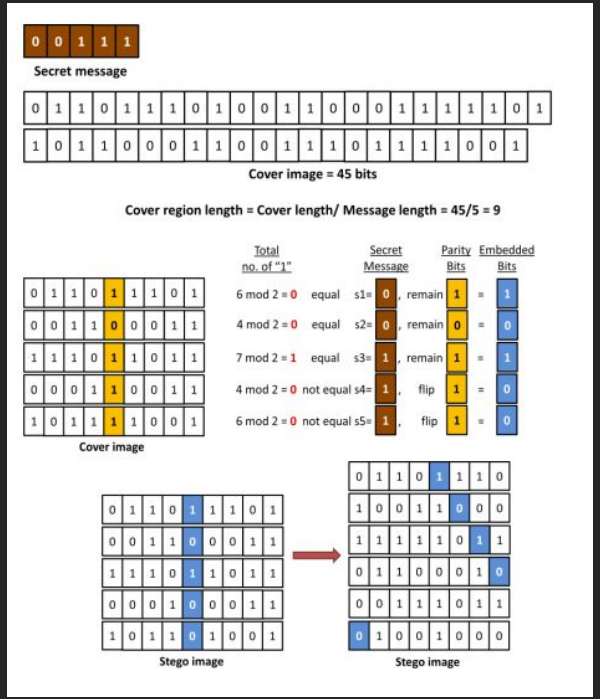


Image Downgrading



Cover-regions and Parity Bits



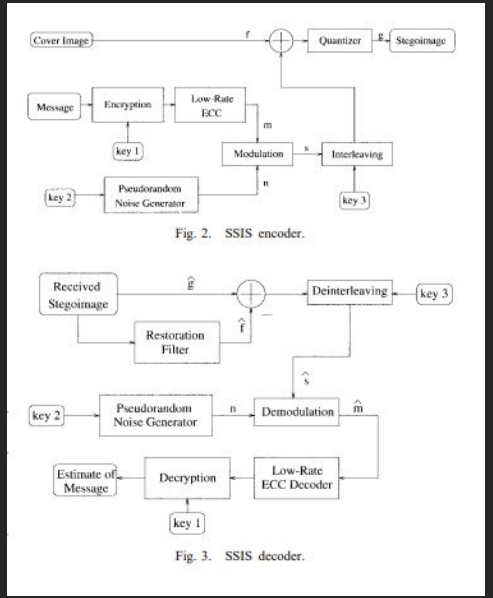
Transform Domain Technique

- DCT Image Steganography
  - Discrete Cosine Transform
- DWT Image Steganography
  - Discrete Wavelet Transform
- DWT & SVD Image Steganography
  - Discrete Wavelet Transform & Singular Value Decomposition

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Spread Spectrum Technique

- Create encoded message by adding redundancy via error-correcting code
- Add padding to make the encoded message the same size as the image
- Interleave the encoded message
- Generate a pseudorandom noise sequence
- Use encoded message to modulate the the sequence, generating noise
- Combine the noise with the original image



Distortion Technique

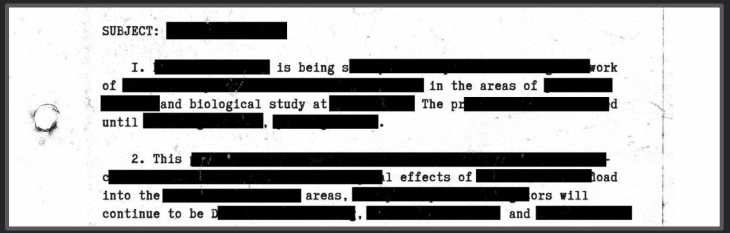
- In contrast to substitution systems, distortion requires the knowledge of the original cover in the decoding process
- The sender applies a sequence of modifications to the cover in order to get a stego-system
- The receiver measures the difference in the original cover in order to reconstruct the sequence of modification applied by the sender, which corresponds to the secret message

Cover Generating Method

- Generates a cover based on the given secret message
- Easily implemented when hide messages in text
- Much harder to implement than any other method
    - With the advent of AI this may become easier through the form of AI image creation

Cover Generating Method

- Generates a cover based on the given secret message
- Easily implemented when hide messages in text
- Much harder to implement than any other method
    - With the advent of AI this may become easier through the form of AI image creation



SUBJECT: [redacted]

I. [redacted] is being s[redacted]work of [redacted] in the areas of [redacted] and biological study at [redacted] The pr[redacted]d until [redacted].

2. This [redacted] effects of [redacted]oad into the [redacted] areas, [redacted]ors will continue to be D[redacted], [redacted] and [redacted]

Cover Generating Method (cont.)

Dear E-Commerce professional ; This letter was specially selected to be sent to you . 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 1624 ; Title 7 , Section 307 ! Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich within 46 weeks . Have you ever noticed people are much more likely to BUY with a credit card than cash and people love convenience ! Well, now is your chance to capitalize on this ! We will help you use credit cards on your website and increase customer response by 180% ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Ms Anderson who resides in Arizona tried us and says "Now I'm rich many more things are possible" . We are a BBB member in good standing ! Do not delay - order today . Sign up a friend and you get half off . Best regards ! Dear Colleague , Thank-you for your interest in our newsletter . We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1622 ; Title 1 , Section 302 ! This is not multi-level marketing . Why work for somebody else when you can become rich within 12 MONTHS ! Have you ever noticed people will do almost anything to avoid mailing their bills & nearly every commercial on television has a .com on in it ! Well, now is your chance to capitalize on this . WE will help YOU SELL MORE plus decrease perceived waiting time by 190% . You can begin at absolutely no cost to you ! But don't believe us . Mrs Anderson who resides in New Hampshire tried us and says "My only problem now is where to park all my cars" . We are licensed to operate in all states ! Don't delay - order today ! Sign up a friend and you get half off ! Thanks . Dear Cybercitizen , Your email address has been submitted to us indicating your interest in our publication ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 1621 ; Title 1 ; Section 305 . THIS IS NOT A GET RICH SCHEME ! Why work for somebody else when you can become rich as few as 53 days ! Have you ever noticed people are much more likely to BUY with a credit card than cash & nearly every commercial on television has a .com on in it . Well, now is your chance to capitalize on this . We will help you deliver goods right to the customer's doorstep and turn your business into an E-BUSINESS ! You can begin at absolutely no cost to you . But don't believe us ! Mrs Ames of Nebraska tried us and says "Now I'm rich many more things are possible" . We are licensed to operate in all states ! We beseech you - act now ! Sign up a friend and your friend will be rich too ! God Bless ! Dear Friend , Especially for you - this breath-taking intelligence ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 2416 , Title 7 ; Section 304 ! THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich inside 34 days . Have you ever noticed more people than ever are surfing the web & people love convenience ! Well, now is your chance to capitalize on this ! WE will help YOU decrease perceived waiting time by 190% and process your orders within seconds ! The best thing about our system is that it is absolutely risk free for you . But don't believe us . Ms Simpson who resides in Florida tried us and says "Now I'm rich many more things are possible" . We assure you that we operate within all applicable laws . For the sake of your family order now . Sign up a friend and you'll get a discount of 10% ! God Bless ! Dear Decision maker ; You made the right decision when you signed up for our mailing list ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1624 ; Title 4 , Section 301 ! This is different than anything else you've seen ! Why work for somebody else when you can become rich as few as 46 MONTHS . Have you ever noticed how many people you know are on the Internet and society seems to be moving faster and faster ! Well, now is your chance to capitalize on this . We will help you SELL MORE plus use credit cards on your website . You can begin at absolutely no cost to you . But don't believe us . Prof Jones who resides in Iowa tried us and says "Now I'm rich, Rich, RICH" ! We are a BBB member in good standing ! For God's sake, order now ! Sign up a friend and you get half off . God Bless .

Hidden Message: I am a message being hidden in a cover being generated.

Created using: SpamMimic

4 Comparisons

Steganography and Encryption

- Data is not always encrypted in steganography
- Random Interval Substitution and Pseudorandom Permutation very similar to a Diffie Hellman key exchange
- Data being hidden can be encrypted thus making it much harder to detect
- Steganography is more about information hiding than data encryption

5 Security

Security of Steganographic Methods

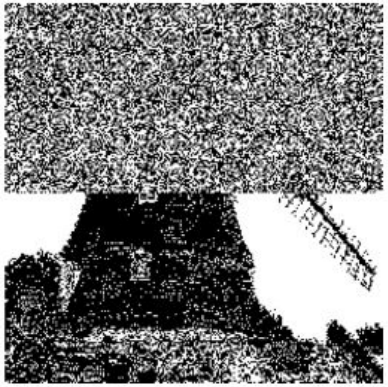
- Can be as secure as you want it to be, by first encrypting the secret message
- Encrypting data before embedding makes the data harder to detect, looks more like noisy channel than a message hidden inside
- If the cover and message are very close in size the noise will be dispersed across the whole image
    - A message smaller than the cover, embedded with certain methods, will appear as noise that abruptly cuts off making it very easy to detect
- Malware can be embedded into an image
    - Executed by the image loader

6 Examples

Message Smaller than Cover

Original

LSBs of Original



LSBs of Steganographed Version

Message the Same Size as Cover

Discrete Cosine Transform

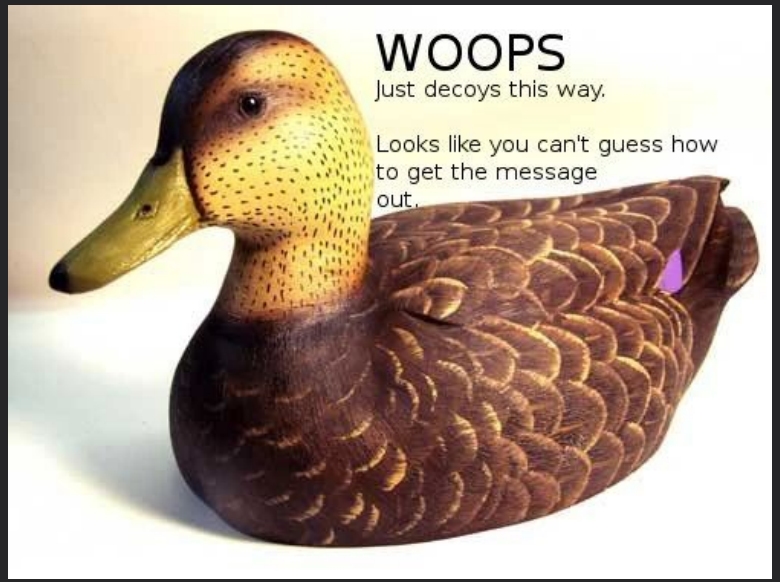
Discrete Cosine Transform (cont.)

Cicada 3301 (2012)

final.jpg

Cicada 3301 (2012)

TIBERIVS CLAVDIVS CAESAR says "lxxt>33m2mqkyv2gsq3q=w]O2ntk"
https://i.imgur.com/m9sYK.jpg



Cicada 3301 (2012)

Here is a book code. To find the book, and more information, go to http://www.reddit.com/r/a2e7j6ic78h0j/

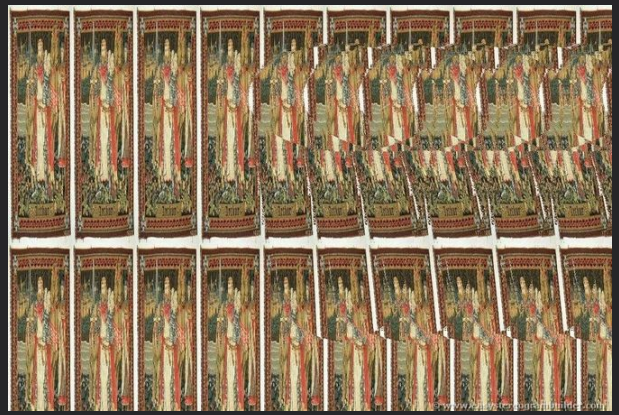
1:20, 2:3, 3:5, 4:20, 5:5, 6:53, 7:1, 8:8, 9:2, 10:4, 11:8, 12:4, 13:13, 14:4, 15:8, 16:4, 17:5, 18:14, 19:7, 20:31, 21:12, 22:36, 23:2, 24:3, 25:5, 26:65, 27:5, 28:1, 29:2, 30:18, 31:32, 32:10, 33:3, 34:25, 35:10, 36:7, 37:20, 38:10, 39:32, 40:4, 41:40, 42:11, 43:9, 44:13, 45:6, 46:3, 47:5, 48:43, 49:17, 50:13, 51:4, 52:2, 53:18, 54:4, 55:6, 56:4, 57:24, 58:64, 59:5, 60:37, 61:60, 62:12, 63:6, 64:8, 65:5, 66:18, 67:45, 68:10, 69:2, 70:17, 71:9, 72:20, 73:2, 74:34, 75:13, 76:21

Good luck.

3301

Cicada 3301 (2012)

Welcome and *Problems?*



Cicada 3301 (2012)

Welcome

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
- From here on out, we will cryptographically sign all messages with this key.

It is available on the mit keyservers. Key ID 7A35090F, as posted in a2e7j6ic78h0j.

Patience is a virtue.

Good luck.

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJPBRz7AAoJEBgfAeV6NQkP1UIQALFcO8DyZkecTK5pAIcGez7k
ewjGBoCfjfO2NlRROuQm5CteXiH3Te5G+5ebsdRmGWVcah8QzN4UjxpKcTQRPB9e
/ehVI5BiBJq8GlOnaSRZpzsYobwKH6Jy6haAr3kPFK1lOXXyHSiNnQbydGw9BFRI
fSr//DY86BUILE8sGJR6FA8Vzjiifcv6mmXkk3ICrT8z0qY7m/wFOYjgiSohvYpg
x5biG6TBwxfmXQOaITdO5rO8+4mtLnP//qN7E9zjTYj4Z4gBhdf6hPSuOqjh1s+6
/C6IehRChpx8gwpdhIlNf1coz/ZiggPiqdj75Tyqg88lEr66fVVB2d7PGObSyYSp
HJl8llrt8Gnk1UaZUS6/eCjnBniV/BLfZPVD2VFKH2Vvvty8sL+S8hCxsuLCjydh
skpshcjMVV9xPIEYzwSEaqBq0ZMdNFEPxJzC0XISlWSfxROm85r3NYvbrx9lwVbP
mUpLKFn8ZcMbf7UX18frgOtujmqqUvDQ2dQhmCUywPdtsKHFLc1xIqdrnRWUS3CD
eejUzGYDB5lSflujTjLPgGvtlCBW5ap00cfIHUZPOzmJWoEzgFgdNc9iIkcUUlke
e2WbYwCCuwSlLsdQRMA//PJN+a1h2ZMSzzMbZsr/YXQDUWvEaYI8MckmXEkZmDoA
RL0xkbHEFVGBmoMPVzeC
=fRcg
-----END PGP SIGNATURE-----

Problems?

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

The key has always been right in front of your eyes.

This isn't the quest for the Holy Grail. Stop making
it more difficult than it is.

Good luck.

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJPCBl3AAoJEBgfAeV6NQkPo6EQAKghp7ZKYxmsYM96iNQu5GZV
fbjUHsEL164ZLctGkgZx2H1HyYFEc6FGvcfzqs43vV/IzN4mK0SMy2qFPfjuG2JJ
tv3x2QfHMM3M2+dwX30bUD12UorMZNrLo8HjTpanYD9hL8WglbSIBJhnLE5CPlUS
BZRSx0yh1U+wbnlTQBxQI0xLkPIz+xCMBwSKl5BaCb006z43/HJt7NwynqWXJmVV
KScmkpFC3ISEBcYKhHHWv1IPQnFqMdW4dExXdRqWuwCshXpGXwDoOXfKVp5NW7Ix
9kCyfC7XC4iWXymGgd+/h4ccFFVm+WWOczOq/zeME+0vJhJqvj+fN2MZtvckpZbc
CMfLjn1z4w4d7mkbEpVjgVIU8/+KClNFPSf4asqjBKdrcCEMAl80vZorElG6OVIH
aLV4XwqiSu0LEF1ESCqbxkEmqp7U7CHl2VW6qv0h0Gxy+/UT0W1NoLJTzLBFiOzy
QIqqpgVg0dAFs74SlIf3oUTxt6IUpQX5+uo8kszMHTJQRP7K22/A3cc/VS/2Ydg4
o6OfN54Wcq+8IMZxEx+vxtmRJCUROVpHTTQ5unmyG9zQATxn8byD9Us070FAg6/v
jGjo1VVUxn6HX9HKxdx4wYGMP5grmD8k4jQdF1Z7GtbcqzDsxP65XCaOYmray1Jy
FG5OlgFyOflmjBXHsNad
=SqLP
-----END PGP SIGNATURE-----

Cicada 3301 (2012)

- Several more intermediate steps and puzzles were apart of the whole puzzle
- A shift cipher involving Mayan Numerals to gain a key to be used in a Vigenère cipher
- A telephone answering machine message that lead back to the original image, that then lead to a website countdown
- The website was also discovered to have a steganographic message inside it
- An RSA puzzle received by email, lead to a MIDI musical note puzzle
- Participants, were said to have been contacted
- Radio silence

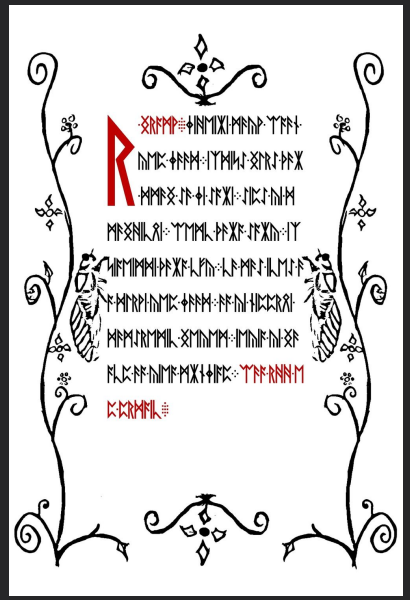
Cicada 3301 (2012)

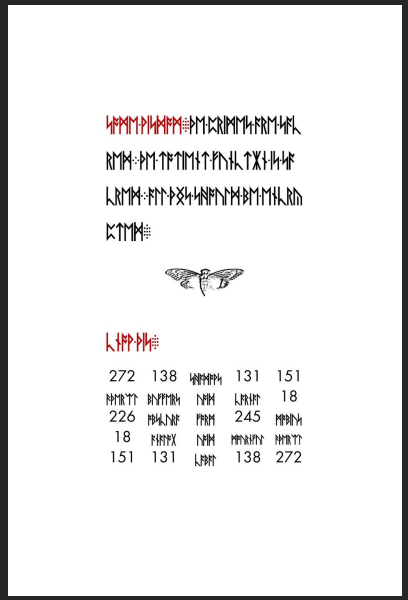
The Final Message

Cicada 3301 (Post 2012)

- 2012, 2013, 2014
- Liber Primus
  - 57 pages
  - 17 solved (2 for certain 15 still have yet to be verified)
- The Leaked Email (2012, 2013)
- 2015, 2016 Messages
- PGP Signed Message April 2017

Cicada 3301 (Liber Primus)





272	138		131	151
				18
226			245	
18				
151	131		138	272

Sources

AL-Ani, Zaidoon Kh., et al. “Overview: Main Fundamentals for Steganography .” *Journal Of Computing*, vol. 2, no. 3, Mar. 2010, pp. 158–165, https://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pdf.

Brundick, Frederick S, and Lisa M Marvel. “Implementation of Spread Spectrum Image Steganography.” *Army Research Laboratory*, Mar. 2001, apps.dtic.mil/sti/pdfs/ADA389095.pdf.

Chen, Kejiang, et al. “Cover Reproducible Steganography via Deep Generative Models.” *IEEE TRANSACTIONS ON DEPENDABLE SECURE COMPUTING* , 26 Oct. 2022, https://doi.org/https://doi.org/10.48550/arXiv.2210.14632.

Gibson, Ryan. “Steganography: Hiding Data In Plain Sight.” University of North Carolina. https://www.cs.unc.edu/~lin/COMP089H/LEC/steganography.pdf. Accessed 26 Nov. 2023.

Holub, Vojtěch, et al. “Universal distortion function for steganography in an arbitrary domain.” *EURASIP Journal on Information Security*, vol. 2014, no. 1, 3 Jan. 2014, https://doi.org/10.1186/1687-417x-2014-1.

P, Vaishali, and Pradyumna Bhat. “Transform Domain Techniques for Image Steganography.” *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*, 3`, no. 1, Apr. 2015, pp. 65–68, https://ijireeice.com/wp-content/uploads/2015/05/T1_131.pdf.

“Steganography.” *Wikipedia*, Wikimedia Foundation, 25 Oct. 2023, en.wikipedia.org/wiki/Steganography.

“Uncovering Cicada Wiki.” *Fandom*, uncovering-cicada.fandom.com/wiki/Uncovering_Cicada_Wiki. Accessed 26 Nov. 2023.

Zakaria, Abdul Alif, et al. “Analysis of Steganography Substitution System Methods Using New Testing Techniques Proposed for Strict Avalanche Criterion.” *International Journal of Cryptology Research*, vol. 1, no. 5, 2015, pp. 61–76, https://www.cybersecurity.my/data/content_files/53/1648.pdf.