Famous Unsolved Codes: *Kryptos*

Elonka Dunin

Strange Loop

September 24, 2012

Overview

- Introduction
- Plaintext and methods of parts 1-3
- Speculations about Kryptos Part 4
- Sanborn's 2010 hint
- Summary

The CIA's Kryptos Sculpture

Famous Unsolved Codes

- 1. Beale Ciphers
- 2. Voynich Manuscript
- 3. Dorabella Cipher
- 4. Zodiac Killer Ciphers
- 5. Kryptos

Kryptos

- Commissioned in 1988
- Dedicated in 1990
- Code systems designed by Ed Scheidt, Chairman of a "CIA Cryptographic Center"
- Sculptor: Jim Sanborn

CIA & Kryptos

Kryptos

- Two panels are a Vigenère table
- A keyword builds a cipher alphabet
- First keyword: Kryptos
- Solvers (of the first three parts):
  - 1998: David Stein, CIA Analyst
  - 1999: Jim Gillogly
  - 1992: Four-person team, led by Ken Miller, with Dennis McDaniels

The NSA Effort

- 1992: CIA's deputy director Admiral William O. Studeman to NSA:
  - “You guys are so hot, let's see how hot you are."
- NSA's director Vice Adm. John M. "Mike" McConnell took up the challenge
- 4-person team ran computer attacks, solved parts 1-3 by December 1992
- Couldn’t solve K4

FOIA Efforts

- **March 28, 2010**
  - Filed FOIA request for information “related to the NSA team that was formed to solve the puzzles of the Kryptos sculpture”
- **April 2010**
  - Confirmation about willingness to pay search fees
- **June 7, 2010**
  - Search completed, placed in the first-in, first-out processing queue for Non-Personal Easy cases, but since there were several cases ahead of mine, they were unable to respond within 20 days.
- **December 2010**:
  - "The referenced case is actively being worked, and, in fact, has already made it through the first level of review. There are additional review and approval stages, and there are other cases ahead of yours so it may be some time before you receive the response."
- **May 2011**:
  - “FOIA case is in the final approval stages. “
- **September 2011**:
  - “Your FOIA case is in the final approval stages. There are a number of cases ahead of yours in that queue.”

The "Untitled Kryptos Piece"

The "Untitled Kryptos Piece" – Antipodes

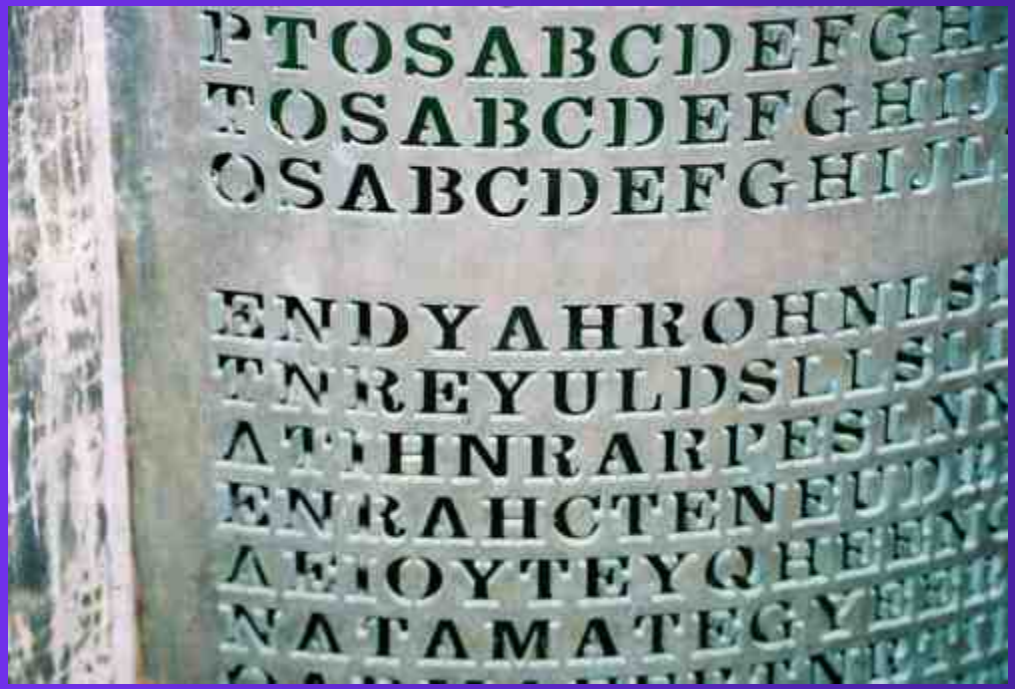
Sanborn's Cyrillic Projector

Untitled Kryptos Piece – Differences

- English Side:
  - Sections are in a different order, and aligned differently.
  - Untitled version contains two extra dots

Untitled Kryptos Piece – Differences

- English Side:
  - Sections are in a different order, and aligned differently.
  - Untitled version contains two extra dots



Untitled Kryptos Piece – Differences

- English Side:
  - Sections are in a different order, and aligned differently.
  - Untitled version contains two extra dots

Untitled Kryptos Piece – Differences

- English Side:
  - Sections are in a different order, and aligned differently.
  - Untitled version contains two extra dots

Untitled Kryptos Piece – Differences

- English Side:
  - Sections are in a different order, and aligned differently.
  - Untitled version contains two extra dots

Kryptos

Vigenère Table

Vigenère Table

- Keyword: Kryptos

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Vigenère Table

KRYPTOSABCDEFGHIJLMNQUVWXZ
RYPTOSABCDEFGHIJLMNQUVWXZK
YPTOSABCDEFGHIJLMNQUVWXZKR
PTOSABCDEFGHIJLMNQUVWXZKRY
TOSABCDEFGHIJLMNQUVWXZKRYP
OSABCDEFGHIJLMNQUVWXZKRYPT
SABCDEFGHIJLMNQUVWXZKRYPTO
ABCDEFGHIJLMNQUVWXZKRYPTOS
BCDEFGHIJLMNQUVWXZKRYPTOSA
KRYPTOSABCDEFGHIJLMNQUVWXZ

Vigenère Table

- Keywords: Kryptos and Palimpsest

Kryptos – Part 1

Kryptos – Part 1

- EMUFPHZLRF
- BETWEENSUB

KRYPTOSABCDEFGHIJLMNQUVWXZ

PTOSABCD***E***FGHIJLMNQUVWXZKRY

ABCDEFGHIJL***M***NQUVWXZKRYPTOS

LMNQ***U***VWXZKRYPTOSABCDEFGHIJ

IJLMNQUVWXZKRYPTOSABCDE***F***GH

MNQUVWXZKRY***P***TOSABCDEFGHIJL

PTOSABCDEFG*H*IJLMNQUVWXZKRY

SABCDEFGHIJLMNQUVWX*Z*KRYPTO

EFGHIJ*L*MNQUVWXZKRYPTOSABCD

SABCDEFGHIJLMNQUVWXZK*R*YPTO

TOSABCDE*F*GHIJLMNQUVWXZKRYP

Kryptos – Part 1

Kryptos – Part 1

- EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
  YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD

Kryptos – Part 1

- EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
  YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
- Keywords: KRYPTOS and PALIMPSEST

Kryptos – Part 1

- EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
  YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
- Keywords: KRYPTOS and PALIMPSEST
- "Between subtle shading and the absence of light lies the nuance of iqlusion."

Kryptos – Part 2

Kryptos – Part 2 Ciphertext

- VFPJUDEEHZWETZYVGWHKKQETGFQJNCE
  GGWHKK?DQMCPFQZDQMMIAGPFXHQRLG
  TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA
  QZGZLECGYUXUEENJTBJLBQCRTBJDFHRR
  YIZETKZEMVDUFKSJHKFWHKUWQLSZFTI
  HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE
  EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX
  FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF
  FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ
  ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE
  DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP
  DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG

Kryptos – Part 2 (corrected) Ciphertext

- VFPJUDEEHZWETZYVGWHKKQETGFQJNCE
  GGWHKK?DQMCPFQZDQMMIAGPFXHQRLG
  TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA
  QZGZLECGYUXUEENJTBJLBQCRTBJDFHRR
  YIZETKZEMVDUFKSJHKFWHKUWQLSZFTI
  HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE
  EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX
  FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF
  FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ
  ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE
  DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP
  DQUMEBEDMHDAFMJGZNUPLGESWJLLAETG

Kryptos – Part 2 Plaintext

Kryptos – Part 2 Plaintext

- Keywords: KRYPTOS and ABSCISSA

Kryptos – Part 2 Plaintext

- Keywords: KRYPTOS and ABSCISSA
- It was totally invisible. How's that possible? They used the earth's magnetic field. x The information was gathered and transmitted undergruund to an unknown location. x Does Langley know about this? They should: it's buried out there somewhere. x Who knows the exact location? Only WW. This was his last message: x Thirty-Eight degrees Fifty-Seven minutes Six Point Five seconds North, Seventy-Seven degrees Eight minutes Forty-Four seconds West. ID by rows.

Kryptos – Part 2 (corrected) Plaintext

- Keywords: KRYPTOS and ABSCISSA
- It was totally invisible. How's that possible? They used the earth's magnetic field. x The information was gathered and transmitted undergruund to an unknown location. x Does Langley know about this? They should: it's buried out there somewhere. x Who knows the exact location? Only WW. This was his last message: x Thirty-Eight degrees Fifty-Seven minutes Six Point Five seconds North, Seventy-Seven degrees Eight minutes Forty-Four seconds West. **x Layer two.**

Kryptos – Part 3

Kryptos – Part 3 Ciphertext

- ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
  CHTNREYULDSLLSLLNOHSNOSMRWXMNE
  TPRNGATIHNRARPESLNNELEBLPIIACAE
  WMTWNDITEENRAHCTENEUDRETNHAEOE
  TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
  EIFTBRSPAMHHEWENATAMATEGYEERLB
  TEEFOASFIOTUETUAEOTOARMAEERTNRTI
  BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
  AECTDDHILCEIHSITEGOEAOSDDRYDLORIT
  RKLMLEHAGTDHARDPNEOHMGFMFEUHE
  ECDMRIPFEIMEHNLSSTTRTVDOHW

Kryptos Part 3 – Rows

Kryptos Part 3 – Rows

- ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIACHTNRE**Y**ULD**S**LLS**L**L
  NOHSNOSMRWXMNETPRNGATIHNRARPESLNNELEBLPII**A**CAE**W**MT
  WNDITEENRAHCTENEUDRETNHAEOETFOLSEDTIWENH**A**EIO**Y**TEY
  QHEENCTAYCREIFTBRSPAMHHEWENATAMATEGYEER**L**BTE**E**FOA**S**
  FIOTUETUAEOTOARMAEERTNRTIBSEDDNIAAHTTMSTEW**P**IER**O**A
  GRIEWFEBAECTDDHILCEIHSITEGOEAOSDDRYDLORIT**R**KLM**L**EH
  AGTDHARDPNEOHMGFMFEUHEECDMRIPFEIMEHNLSST**T**RTV**D**OHW?

Kryptos Part 3 – Rows

- ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIACHTNRE**Y**ULD**S**LLS**L**L
  NOHSNOSMRWXMNETPRNGATIHNRARPESLNNELEBLPII**A**CAE**W**MT
  WNDITEENRAHCTENEUDRETNHAEOETFOLSEDTIWENH**A**EIO**Y**TEY
  QHEENCTAYCREIFTBRSPAMHHEWENATAMATEGYEER**L**BTE**E**FOA**S**
  FIOTUETUAEOTOARMAEERTNRTIBSEDDNIAAHTTMSTEW**P**IER**O**A
  GRIEWFEBAECTDDHILCEIHSITEGOEAOSDDRYDLORIT**R**KLM**L**EH
  AGTDHARDPNEOHMGFMFEUHEECDMRIPFEIMEHNLSST**T**RTV**D**OHW?

Kryptos Part 3 – Rows

- ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIACHTNREYULDSLLSLL
  NOHSNOSMRWXMNETPRNGATIHNRARPESLNNELEBLPIIACAEWMT
  WNDITEENRAHCTENEUDRETNHAEOETFOLSEDTIWENHAEIOYTEY
  QHEENCTAYCREIFTBRSPAMHHEWENATAMATEGYEERLBTEEFOAS
  FIOTUETUAEOTOARMAEERTNRTIBSEDDNIAAHTTMSTEWPIEROA
  GRIEWFEBAECTDDHILCEIHSITEGOEAOSDDRYDLORITRKLMLEH
  AGTDHARDPNEOHMGFMFEUHEECDMRIPFEIMEHNLSSTTRTVDOHW?

- S L O W L Y D E S P A R A T L Y

Kryptos – Part 3 Plaintext

Kryptos – Part 3 Plaintext

- Slowly, desparatly slowly, the remains of passage debris that encumbered the lower part of the doorway was removed. With trembling hands I made a tiny breach in the upper left-hand corner. And then, widening the hole a little, I inserted the candle and peered in. The hot air escaping from the chamber caused the flame to flicker, but presently details of the room within emerged from the mist. x Can you see anything q?

Kryptos – Part 4 Ciphertext

- OBKR
  UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
  TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
  VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

Other Kryptos Discoveries / Speculations

- The extra "L"
- IBCDEFGHIJLMNQUVWXZKRYPTOSABCDE
  JCDEFGHIJLMNQUVWXZKRYPTOSABCDEF
  KDEFGHIJLMNQUVWXZKRYPTOSABCDEFG
  LEFGHIJLMNQUVWXZKRYPTOSABCDEFGH
  MFGHIJLMNQUVWXZKRYPTOSABCDEFGHI
  NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
  OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL
  PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM
  QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN
  RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ
  SMNQUVWXZKRYPTOSABCDEFGHIJLMNQU
  TNQUVWXZKRYPTOSABCDEFGHIJLMNQUV
  UQUVWXZKRYPTOSABCDEFGHIJLMNQUVW

Cyrillic Projector – The extra bolt

Closeup images courtesy John Wilson, scirealm@aol.com

Cyrillic Projector – The extra bolt

Closeup images courtesy John Wilson, scirealm@aol.com

Cyrillic Projector – The extra bolt

Closeup images courtesy John Wilson, scirealm@aol.com

Cyrillic Projector – The extra bolt

Closeup images courtesy John Wilson, scirealm@aol.com

Cyrillic Projector – The extra bolt

Closeup images courtesy John Wilson, scirealm@aol.com

Cyrillic Projector – The extra bolt

Closeup images courtesy John Wilson, scirealm@aol.com

Scheidt said:

- He did things to "mask the English" in part 4
- The first 3 parts were solved “without recovering the keys first.”
- “A little bit of stego”
- “Duress ciphers”
- The last part is definitely English
- It uses “all the letters”

2010 Hint

- November 20, 2010, Sculptor Sanborn announced a hint, for characters 64-69:

```
                                        ?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```

- **NYPVTT** == **BERLIN**

Possible key pairs

- Using Vigenere with keys of SHIFTED and BINARY puts "Berlin" at proper location

OBKR

UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFB**NYP**
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

BDXK

HQNMVUHNSYHDCESDAWUVLOFGSPIGJRX
DMIFRQUQYOEDHMENTRNKTLSFTAHR**BER**
LINADECGAFLMPVNTOBUBXLBWZQOEOCJ

Other key pairs

- SHIFTED BINARY
  OVERCROWDS BULGARIAN
  INCONTINENCIES CHERRYSTONES
  MISUSE CRAFTY
  UPSWELLED CRANBERRY
  SHABBINESS DOMICILIARY
  WITCHED FILAMENTARY
  SUBCOMPACT GORKI
  ALGORITHMIC GRATEFULNESS
  CAVILER HYPERTHYROIDS
  BUSHELER INCESSANT
  ATHWART LENIN
  BULWARK MISDRAWN
  DRIFTS MOBILIZE
  DERISORY NARCOMANIA
  BRAINPAN NONDOMESTICATED
  HYDROGRAPHER OPERABILITIES
  SAPSUCKER OVERUSED

BERLIN hint

- AHRBERLINADE
- amBER LINe
- numBER of LINks
- Berlin Wall? Berliner? Berlin Tunnel?

Kryptos – Part 3 – Alignment

Part 3 – Alignment

- Sanborn: "This is important."

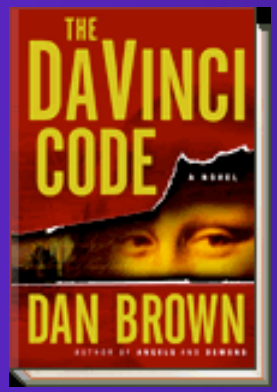
Berlin Wall and the CIA

- Kryptos was installed 1988-1990
- Berlin Wall fell in November 1989
- Berlin Wall Monument dedicated at CIA, December 1992


GlobeXplorer™
© 2003 GlobeXplorer, AirPhotoUSA

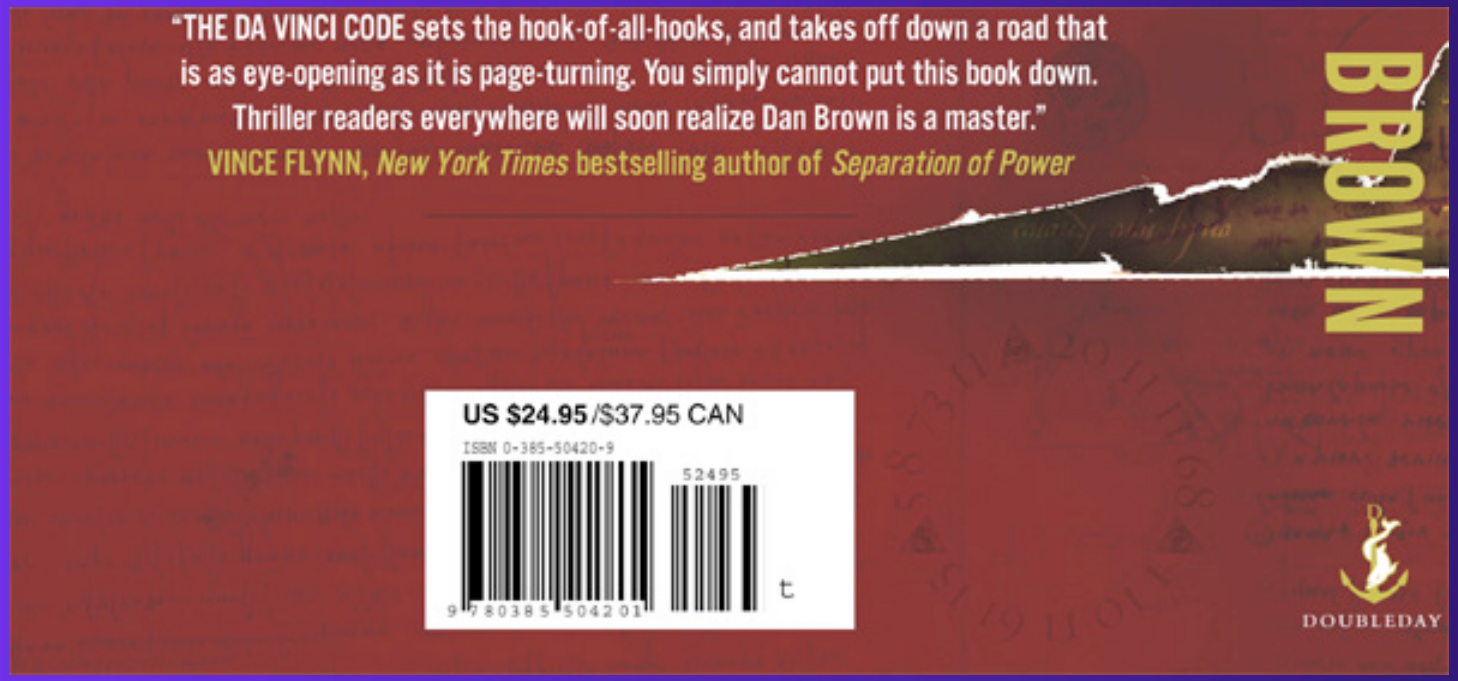
Kryptos in Pop Culture

Kryptos in Pop Culture



Kryptos in Pop Culture

Kryptos in Pop Culture

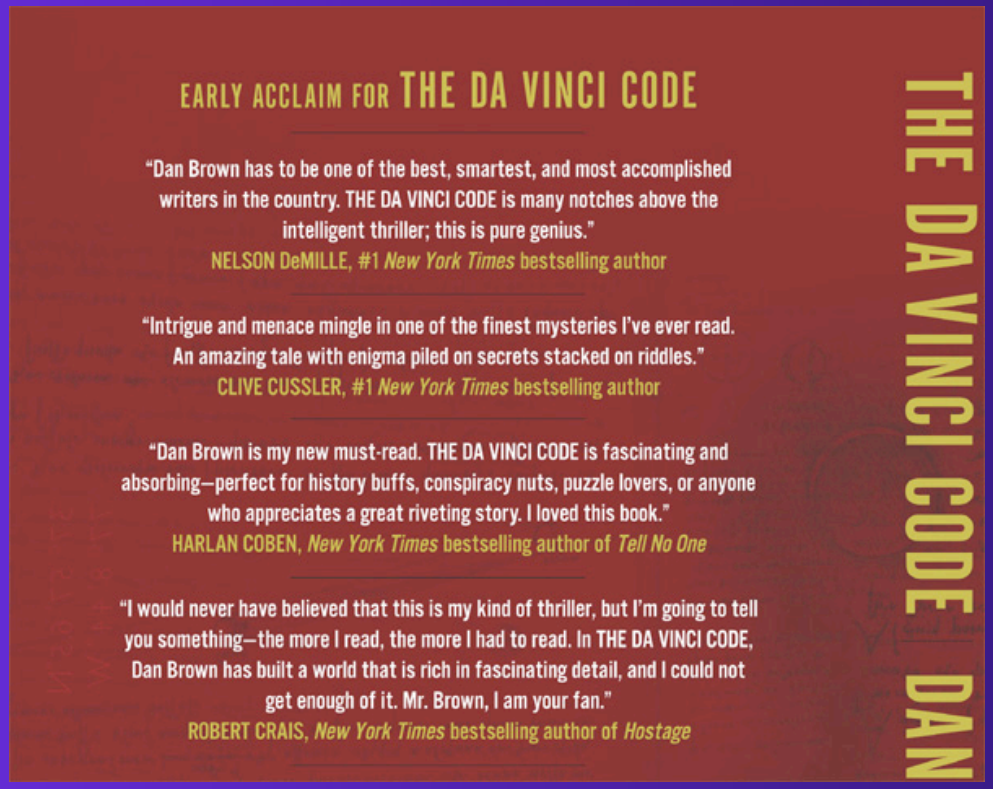


Kryptos in Pop Culture

Kryptos in Pop Culture

Kryptos and *The Da Vinci Code* Novel

Kryptos and *The Da Vinci Code* Novel

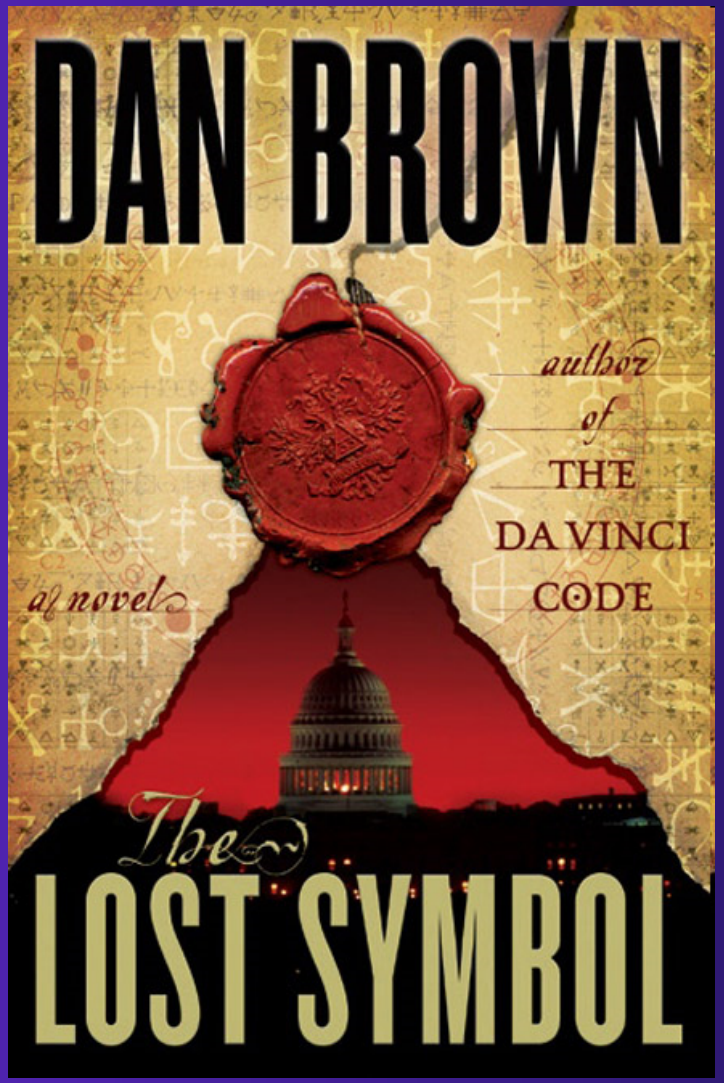


Kryptos and *The Da Vinci Code* Novel

Kryptos and *The Da Vinci Code* Novel

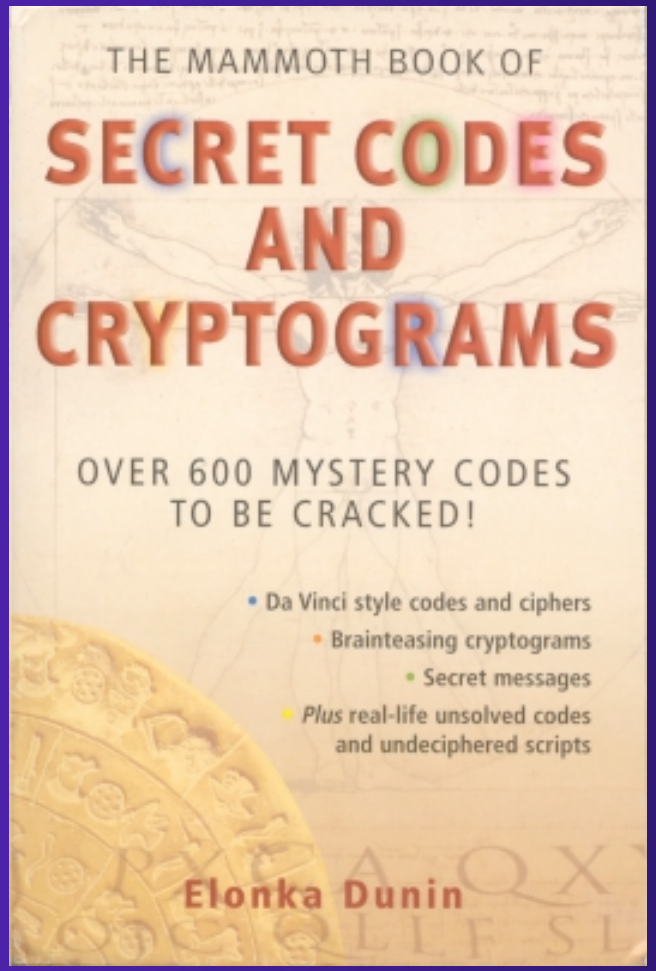
The Lost Symbol

- Takes place in Washington DC
- Features *Kryptos* as a recurring theme
- CIA analyst character "Nola Kaye" named after Elonka



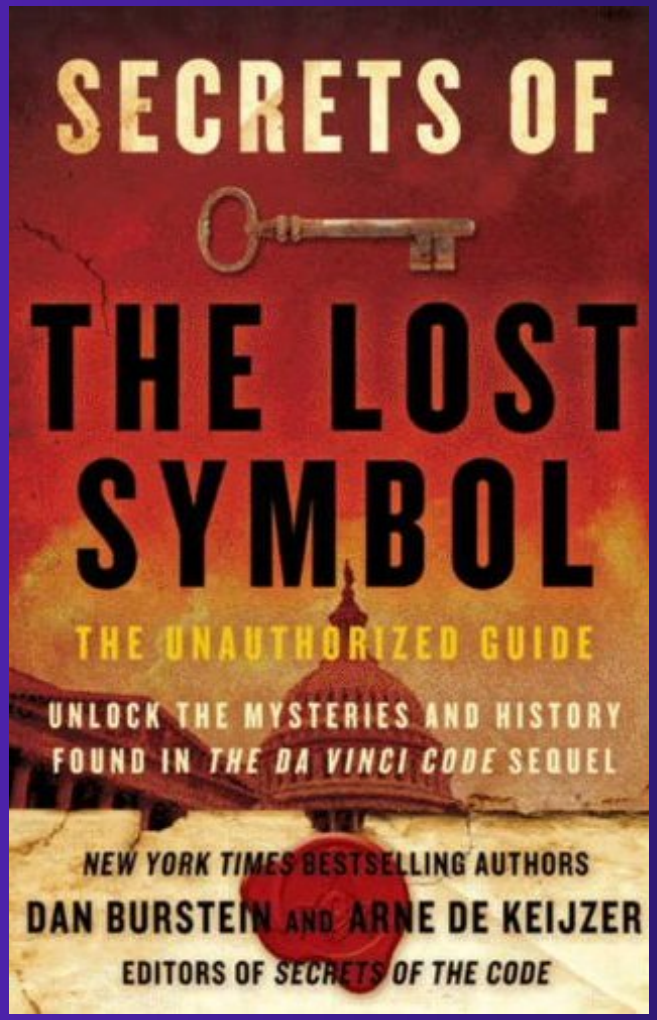
To get more information

- Kryptos YahooGroup
  - kryptos-subscribe@yahoogroups.com
- http://www.elonka.com/kryptos
  - (elonka.com has received nearly 4 million page views)
- AIM: Elonka
- Google
- http://www.pbs.org/nova
  - NOVAscienceNOW



To get more information

- Kryptos YahooGroup
  - kryptos-subscribe@yahoogroups.com
- http://www.elonka.com/kryptos
  - (elonka.com has received nearly 4 million page views)
- AIM: Elonka
- Google
- http://www.pbs.org/nova
  - NOVAscienceNOW



Why Hasn't K4 Been Solved Yet?

- It's short – Just 97 characters, so it's very difficult to find patterns
- There may be a necessary key that's only accessible on CIA grounds
- We may have missed something, or been misdirected in some way
- It might have a mistake that makes it unsolvable

Summary

- Kryptos has 4 sections of code
  - 3 of the 4 have been solved
- The reason for Part 4 being unsolved:
  - It's very short
  - It may have a mistake
  - There may be a necessary clue that's on CIA grounds
  - We may have been misdirected
- Both Sanborn and Scheidt have said that it's solvable.
- My goal is not necessarily to solve it, but to help see it solved.

Q & A