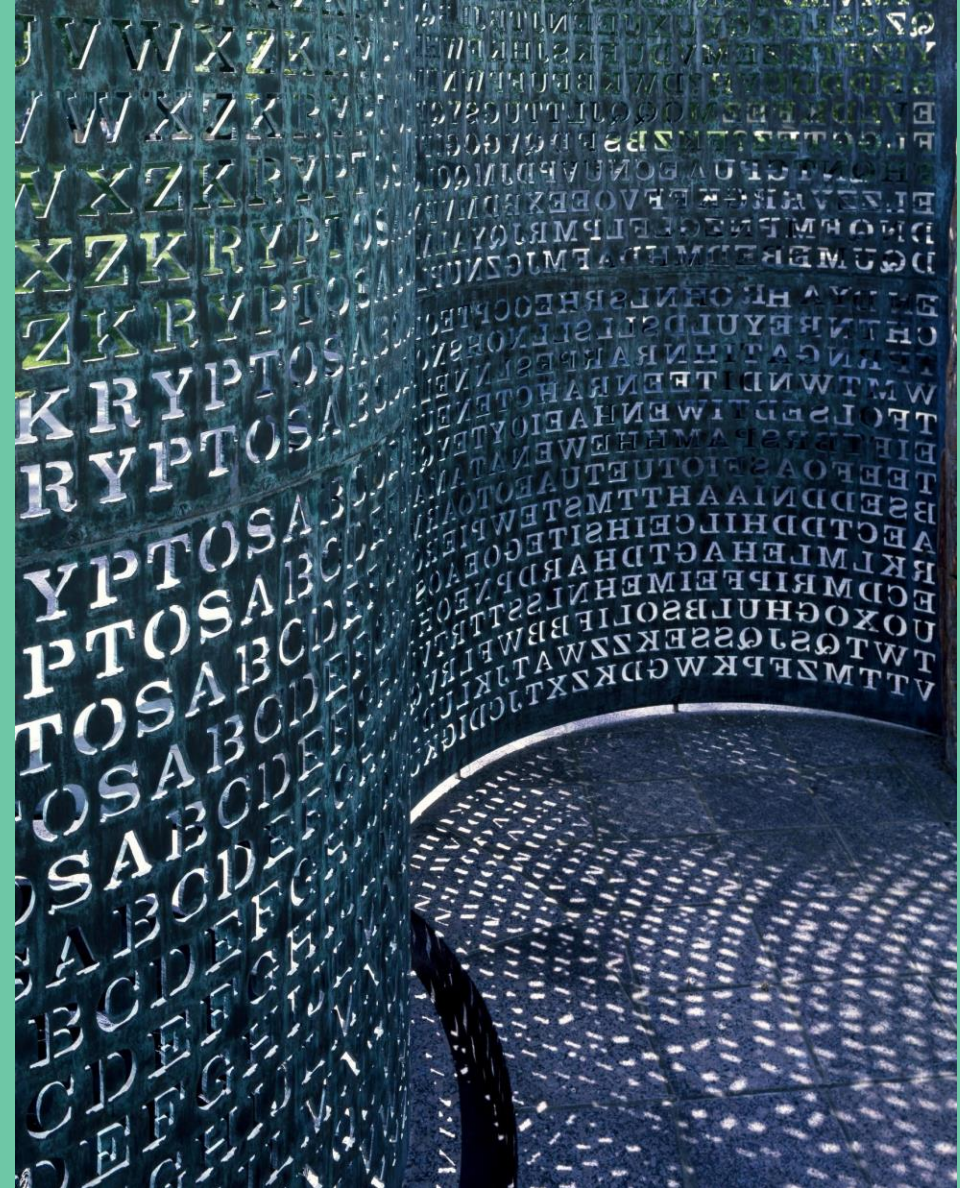
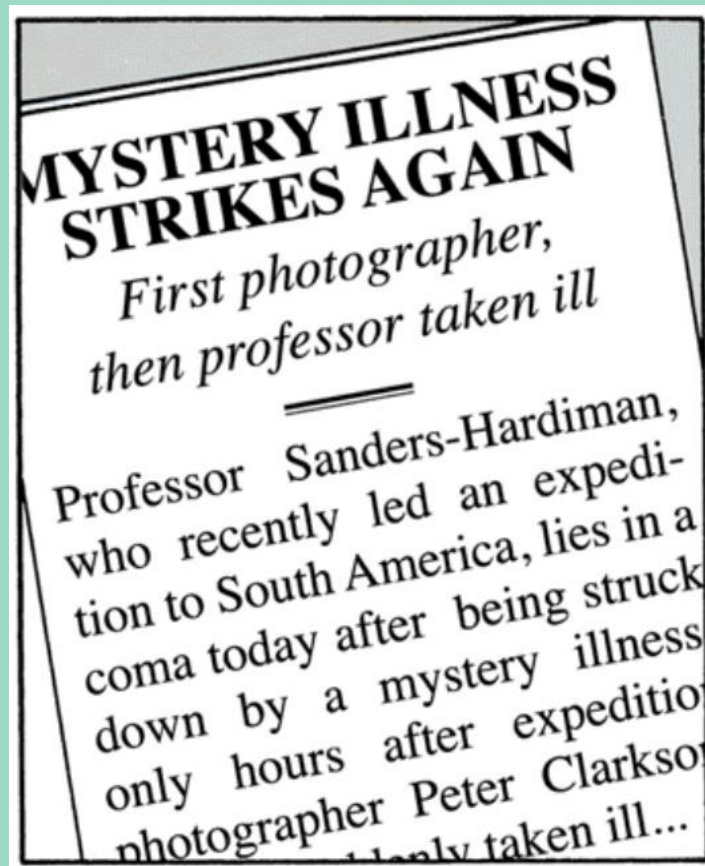


Kryptos K4 – from Gromark to Autoclave

17 November 2024



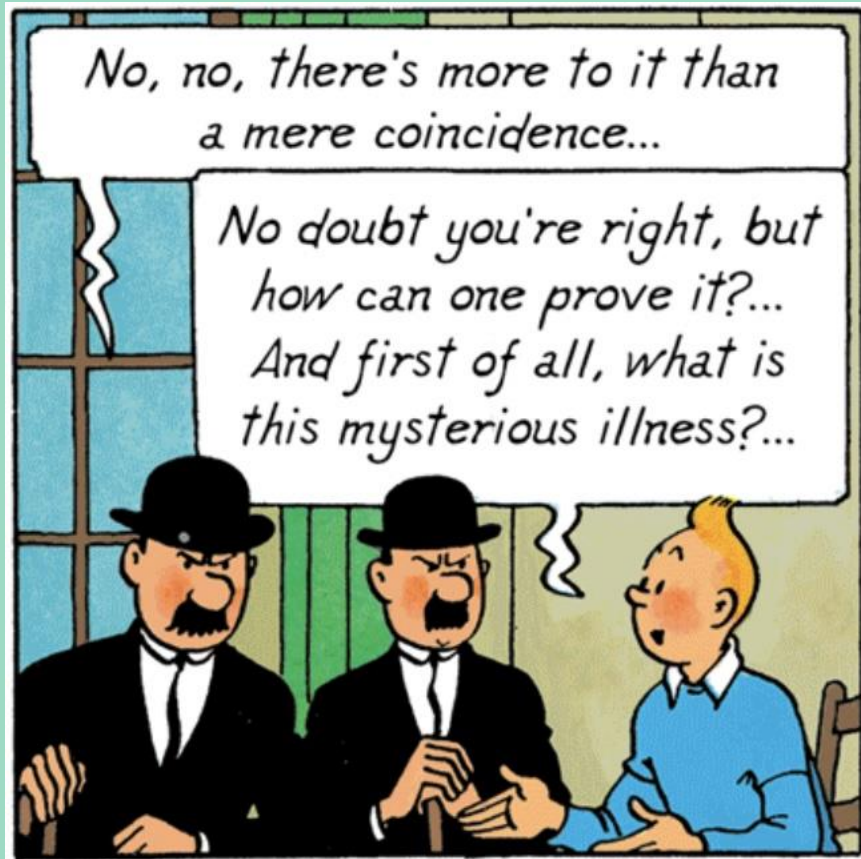
Mysterious illness! (“Seven Crystal Balls” 1943)



Pure coincidence (“Seven Crystal Balls”)



How can you prove 'more than coincidence'



2021

- 10 August 2021 – My *“Cryptodiagnosis of K4”* paper published in HistoCrypt 2021 proceedings
- 20 August 2021 – Dennis McDaniels one of 1992 NSA K1-3 solvers died at 81
- 29 August 2021 – I solved a Porta cipher published in HistoCrypt 2021 proceedings “An alchemical cipher in a shared notebook of John and Arthur Dee”
- 4 October 2021 – I published my third, most recent, K4 Vimeo/Youtube talk *“Reminiscences de K4”*



2022

- January 2022 – Frank Rubin (ACA “FIRE-O”) publishes “Secret Key Cryptography: Ciphers, from Simple to Unbreakable”
<https://www.manning.com/books/secret-key-cryptography>
- March-November 2022. Moshe Rubin (ACA “THE BRUIN”) uploads some books to archive.org. https://archive.org/details/@moshe_rubin
 - “Elementary Cryptography and Cryptanalysis” by Donald D. Millikin (1943)
 - “Cryptographers Way” by Bradford Hardie III (1967)
 - “Solving Cipher Problems” by Frank Lewis (1992)
- 2 June 2022 – I played with GPT-3 to “Create 97 letter English text with constraints”; ChatGPT 4 Dec 2022. AI now banned from r/codes; lots of Dunning-Kruger type posts <https://community.openai.com/t/create-97-letter-english-text-with-constraints/18500> ... “o1-preview” of 2024 does better but can’t solve
- 21 June 2022 – I gave my HistoCrypt talk on K4 in Amsterdam (after Covid postponed 2020 physical conference). Learned about “*prewhitening*” as K4 hint (John Tukey word 1956, Hellman DES 1979, Rivest DESX 1984 in Schneier 1995 as “whitening”).
- July 2022 and February 2023 – I visited Canberra: NKRYPT in front of Questacon, and read books in National Library of Australia e.g. David Shulman’s “An annotated bibliography of Cryptography” (1976)
- 21 September 2022 – E-book “Apprehended” by Bill Bonk published (Hantman book cipher) <https://www.amazon.com/dp/B0BG4LG8XK>

Preemphasis

Emphasis of certain frequencies (in comparison with others), before processing, as an aid to the quality of result.

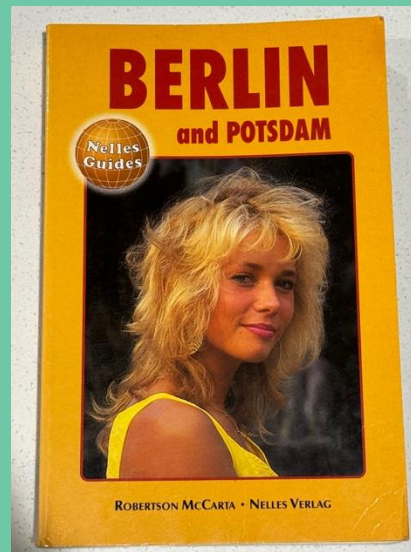
Prewhitening

Preemphasis designed to make the spectral density more nearly constant (the spectrum more nearly flat).



2023

- 6 March 2023 – NSA Dragon Seeds newsletters published by GovernmentAttic.org. “Diagnosis is presented as a 5-step iterative process.”
https://www.governmentattic.org/48docs/NSAdragonSeedsNewsletters_1972-1974.pdf
- 29 April 2023 – I bought “Berlin” guidebook from Nelles Guides (1991). Describes the main three clocks: Set Theory, World Time and Flowing Time (interesting yellow/red cover colours)
- 28 May 2023 – David Vierra solved Feynman Ciphers 2 and 3 (published in 1987) assisted by AZDecrypt
https://www.reddit.com/r/codes/comments/13txikf/solutions_to_feynman_ciphers_2_and_3/
- 24 June 2023 – After HistoCrypt 2023 in Munich, I went to Berlin for one day to visit several clocks
- August 2021 and July 2023 – I made extensive updates to Ed Scheidt English Wikipedia page
https://en.wikipedia.org/wiki/Edward_Scheidt



2024

- 5 January 2024 – David Shulman’s “Supplement to An Annotated Bibliography of Cryptography” published (1985) thanks to Rob Simpson at National Cryptologic Museum https://5099.sydneyplus.com/final/Portal/Default.aspx?lang=en-US&g_AABJ=vf+183-001
- 27 March 2024 – Oranchak, Blake, van Eycke “The Solution of the Zodiac Killer’s 340-Character Cipher” <https://arxiv.org/abs/2403.17350>
- 1 April 2024 – NSA Kryptos Society newsletters published by GovernmentAttic.org (“Principles of Diagnosis” by R. Dale Shipp; Hantman cipher) <https://www.governmentattic.org/53docs/NSAKryptosSocNwsltrs1994-2003.pdf>
- 5 May 2024 – Lemmino Kryptos video (up to 5.7 million views as of November 2024) <https://youtu.be/iVpsLMCIB0Y>
- 11 June 2024 – With Louie Helm (Beijing House), I solved Klaus Schmeh and Elonka Dunin’s 24 and 22 letter Playfair challenges (from Jan 2020 and Aug 2021) – KenLM models critical – using large language model of multi terabyte size, generated in 2014. Also used normal and positional English 8, 9 and 10-gram statistics. <https://scienceblogs.de/klausis-krypto-kolumne/2020/01/27/can-you-solve-this-playfair-cryptogram-and-set-a-new-world-record-3/>
- 20 June 2024 – Christian Schridde writes about Ed Scheidt’s driveway Mayan symbols <http://numberworld.blogspot.com/2024/06/ed-scheidts-mayan-symbols.html>
- 6 September 2024 – “YefimShifrin” solved three 26-letter cryptograms of Lambros D. Callimahos https://www.reddit.com/r/codes/comments/iezmay/three_cryptograms_of_lambros_d_callimahos/

(U) Principles of Diagnosis

(U//~~FOUO~~) These principles of cryptanalytic diagnosis were gathered by R. Dale Shipp, a Distinguished Member of the KRYPTOS Society (1999). Except for the first, they are not in order of importance. Where known, the originator or popularizer of the principle is credited.

(U//~~FOUO~~) A short bio for Dale may be found in the November 1999 issue of Tales of the KRYPT: <http://www.█.nsa/kryptos/Newsletters/1999/nov99/█.html>

1. (U) Look at the data.

(b) (3) – P.L. 86-36

Today I'm presenting a 24 letter message that has been encrypted with a Playfair cipher. Such a short Playfair cryptogram has never been solved before.

In December, I reported on [Konstantin Hamidullin's solution of a Playfair challenge](#) I had published four weeks earlier. With only 26 letters, this cryptogram is the shortest Playfair message that has ever been broken.

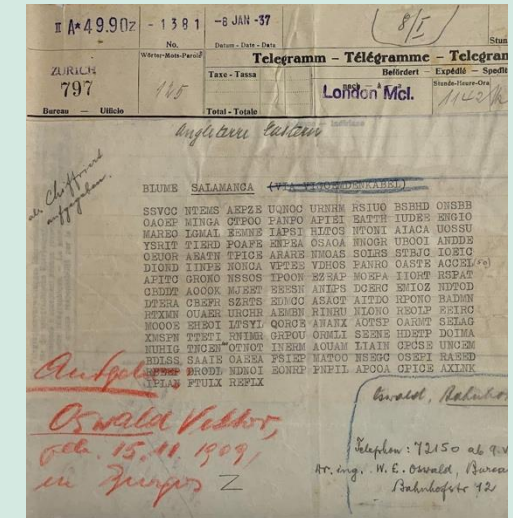
Playfair cipher records

Konstantin's deciphering success was already the fifth Playfair world record set by my blog readers. Here are the four previous ones:

- Magnus Ekhall [broke a 28-letter Playfair message](#).
- Magnus Ekhall [broke a 30-letter Playfair message](#).
- Nils Kopal [broke a 40-letter Playfair message](#).
- George Lasry [broke a 50-letter Playfair message](#).

Years of cryptanalysis failures... including K4

- Cosimo Palma's *Turbolo Chapel "Santa Maria la Nova" Naples* inscription from HistoCrypt 2023 – seems exactly like monoalphabetic substitution, should be Latin, but cannot be solved. What is going on?
<https://ecp.ep.liu.se/index.php/histocrypt/article/view/703>
- *Werner Oswald telegram (from 1937/2023)* - <https://cryptiana.blogspot.com/2023/09/a-telegram-from-switzerland-1937.html> should be transposition, Spanish
- "*Thorough Summary of All Celestial Influence*" Prinke and Zuber (2020) – Cod. Alchim. 651 -- a cipher which looks like a monoalphabetic substitution in a European language, but cannot be solved <https://doi.org/10.1163/15733823-00255P01>
<https://scienceblogs.de/klausis-krypto-kolumne/2021/01/05/ungehoeste-verschlueselungen-in-einem-300-jahre-alten-manuskript/>
- *Rudolf II handbell cipher (c. 1600, Gannon 2020)* – inscription looks just like a "keyphrase" cipher, but can't be solved in European languages; Keyphrase cipher seen in 1649 (Lasry at HistoCrypt 2023 "poly-homophonic cipher") and 1832 (Duchess of Berry). Another cipher engraved in metal.
- Hantman book ciphers – using KenLM, mountains of dictionaries
- NKRYPT, MysteryTwister Vatican (haven't looked at much)
- Perhaps I should look at alchemical ciphers when time



Seaman M.Sc. math thesis (2012)

- Noticing that “ELYOIE” implied key (using K1/K2 encryption scheme with KRYPTOS alphabets) for given plaintext BERLIN looks like English:
 - What does a chi-square test say about whether K4 could be English enciphered with a transposed English key (e.g. a transposition of the plaintext itself; or a transposed running key) with K alphabets
 - The test shows the idea cannot be ruled out.
 - The chi-squared stat for the “wrong” table as seen on the sculpture (plain alphabet = A-Z, key alphabet = A-Z, cipher alphabet = KRYPTOS alphabet) shows that the K4 letter distribution matches the expected letter distribution closely (using plain and key from English text)
 - Transposed English key would also make it easier to place the **KR/SO/T/YP** on the edges of the sculpture and add “ambiguity” to the solution. Sanborn has said “The answer will be far more ambiguous”.

ECDMRIPFEIMEHNLSTTRTVDOHW?OB**KR**
UOXOGHULBSOLIFBBWFLRVQQPRNGKS**SO**
TWTQSJQSSEKZZWATJKLUDIAWINFBN**YP**
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

- Running key papers – Griffing (2006) and Reddy and Knight (2012). 100 letter ciphertexts can be solved about 40% of the time.

Kryptos
by
Kristine Seaman, B.A.
A Thesis
In
Mathematics
Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for the Degree of
Master of Science
Approved
Mara D. Neusel
Chair of Committee
Chris Monico
Lars W. Christensen
Peggy Gordon Miller
Dean of the Graduate School
May, 2012

Diagnosis (from NSA newsletter “Dragon Seeds” 1972)

The National Cryptologic School now offers a course in the diagnosis of manual cryptosystems as part of the cryptanalysis curriculum. Designed to be taken after completion of General Cryptanalysis CA-100, which stresses cryptography and exploitation of known cryptosystems, Practical Diagnosis CA-260 teaches the diagnosis of unknown cryptosystems.

Diagnosis is presented as a 5-step iterative process:

1. gathering the a priori information
2. separating the undifferentiated traffic into homogeneous sets
3. analyzing the sets and making hypotheses
4. testing and proving the hypotheses
5. writing a solution report.

A popular feature of the course is that the student acquires his skills by diagnosing a variety of operational foreign language problems from A, B, and G Groups. Statistical and computer techniques are emphasized.

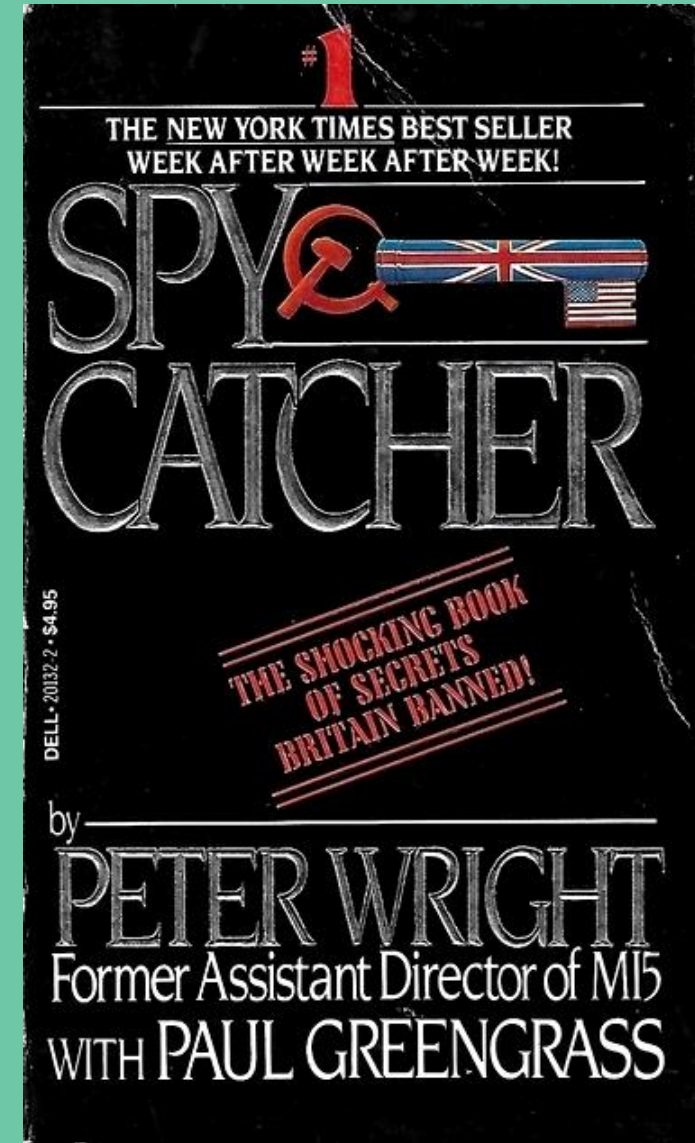
This course is scheduled to be given only once in FY73, from 18 Sep-17 Nov. Successful completion of CA-100 and an entrance exam are required.

Principles of Diagnosis (from NSA Kryptos society newsletter “Tales of the Krypt” May 2002)

1. Look at the data.
2. Let the data tell you what to do.
3. Remember that diagnosticians do not know what they are doing.
4. Use all of the data you can afford.
5. Do not worry that you will not understand the meaning of a result from a diagnostic run. Do worry about being able to determine the significance of an answer.
6. Data quality is important.
7. Know the quality of your data.
8. Believe in yourself and have confidence that you can succeed.
9. Put yourself in a position to be lucky.
10. Cooperate and share data and information and ideas.
11. Document and publish.

Last talk: what is “Traditional” Gromark cipher

- A “running key” system, but expressed in terms of numbers rather than letters
- Generate a long key without repetitions by starting with a five-digit “primer”
- The primer is expanded to a “key” of the length of the ciphertext by using “chain addition”
 - e.g. as seen in the famous “VIC cipher” described by Kahn (“Two Soviet Spy Ciphers”, “Number One from Moscow”). Modulo addition in “Spycatcher” by Peter Wright
- Use a plain alphabet of A to Z (the “standard” alphabet) and a cipher alphabet derived from a keyword
- Described by DUMBO in 1969 and Callimahos (NSA) in 1977



How “close” could K4 be to “traditional” Gromark?

- How does Bayesian statistics help when you are trying to diagnose?
- For example: we say “this is obviously not pure transposition” after just one look at the index of coincidence – 0.03608
- To an experienced cryptanalyst “this is obvious”
- But how close can we get to meaningful English text if we “break all the rules”?
- The obvious way is to combine tortured pangrams
- <https://davelab6.github.io/pangrams/> -- choose length sum = 97

Pangram gluing

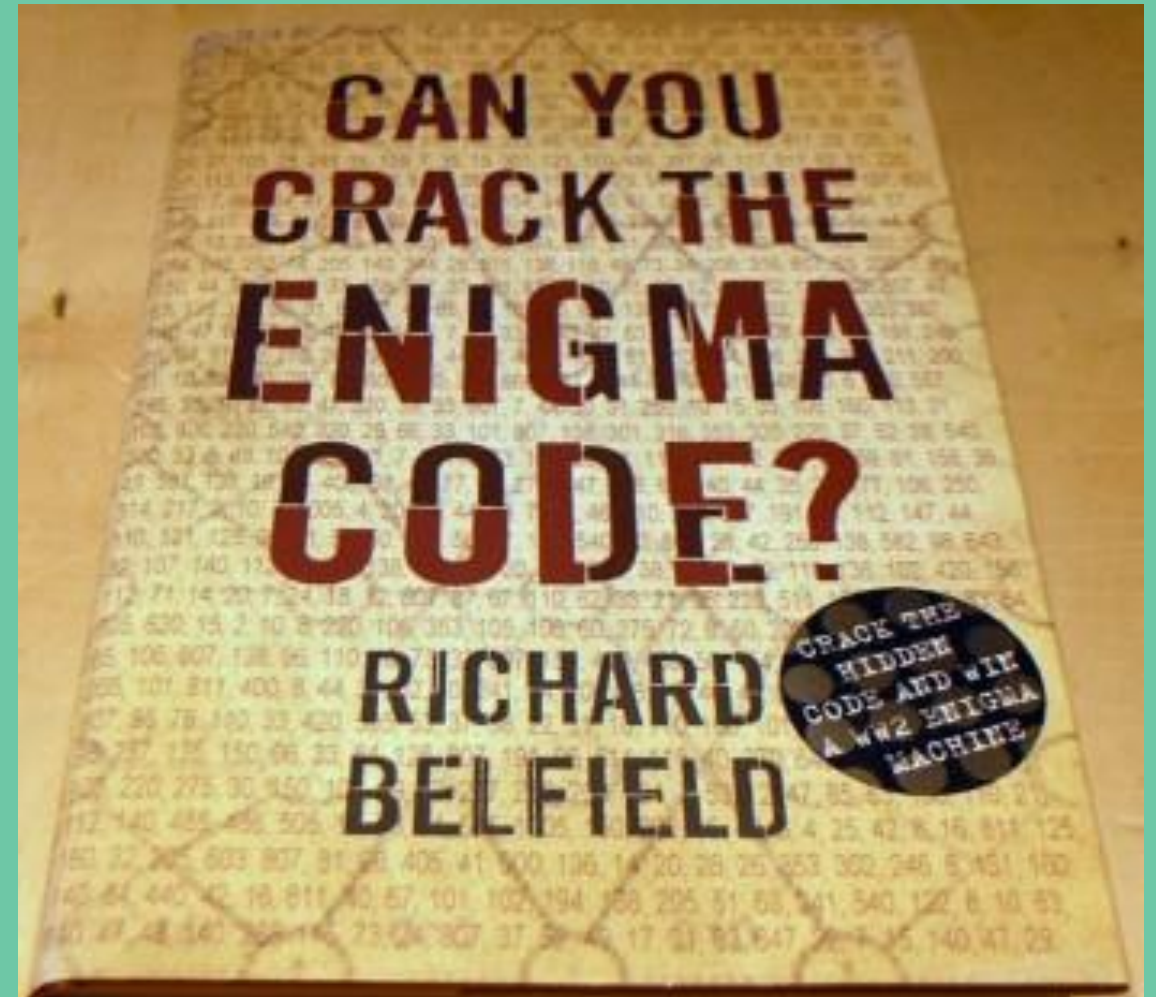
- For example, these 97 letter texts have $IC = 0.03608$
 - Five quacking zephyrs jolt my wax bed. Sex prof gives back no quiz with mild joy. Schwarzkopf vexed Iraq big time in July.
 - Pack my box with five dozen liquor jugs. Five jumping wizards hex bolty quick. Boxers had zap of gay jock love quit women.
- But the probability that *random* English looks like this is very small
- I had to do something *very* contrived to get this
- The informational content of these is very small – they are very constrained and there are very few sentences like this
- “Choose the explanation that best fits the data”

Sentence word count

- 97 letter sentences have 9-34 words.
 - "Recollections retrospectively reconstruct experiential processes into expressively progressive traditions."
 - "All I have to do is run and eat and if I get a chance to write a blog at the end of the day and talk to Gemma then that is a bonus."
- The lengths follow a Weibull distribution ...

“Can you crack the Enigma cipher” Belfield

- Challenge ciphers used pangrams to artificially lower the index of coincidence (IC) to less than 0.05
- How common is it to see an x-letter text with $IC < 0.05$?
 - Simulate with large corpus (e.g. Project Gutenberg, books3) or synthetically
 - Approximate IC by gamma distribution
- <http://www.mountainvistasoft.com/cryptoden/index.php/algorithms/churn-algorithm/20-churn-algorithm.html>
 - "Junk jewelry jingles, jolts jerky jackanapes. Jealous jades jot jabberwocky, jerboa jumps jaguarundi." IC 0.0633

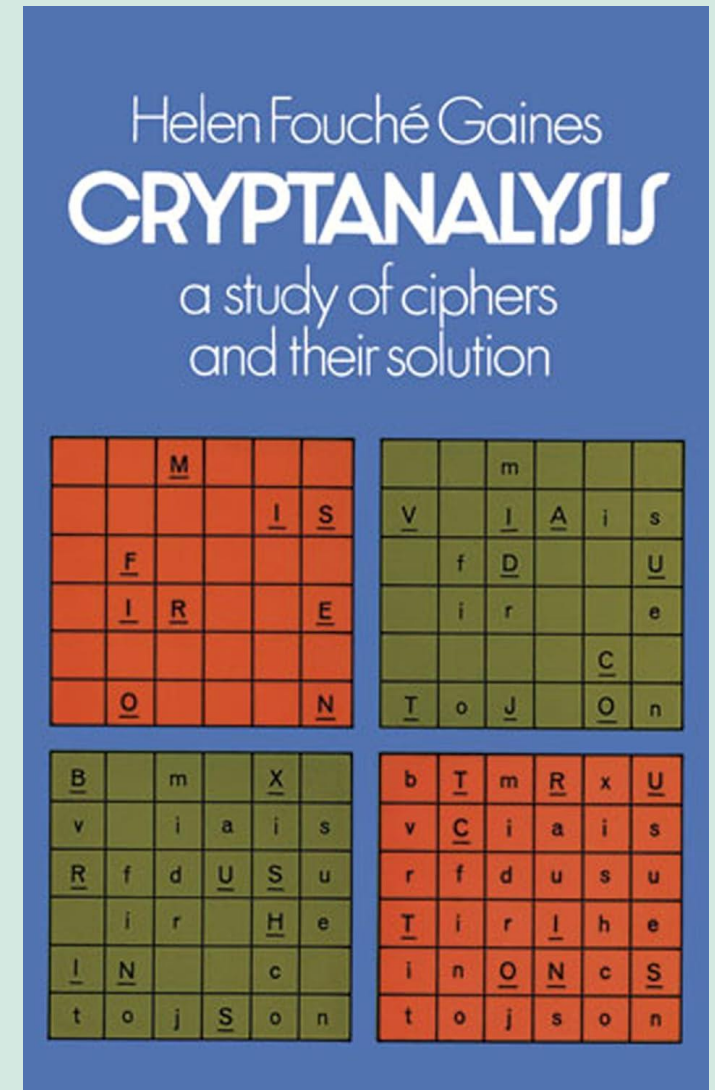


Proceed by elimination

- Transposition alone is eliminated
- Playfair and seriated Playfair variants are eliminated
 - See my HistoCrypt paper for details; IC is a bit low
 - We can force a low IC by careful choice of the key found with computer, but it is difficult today and would have been very difficult in the 1980s, and you also want the **KR/SO/T/YP** on the edges of K4 of the sculpture. Seems impossible.

Eliminate transposition and substitution

- Gaines (1939) suggested when “flat frequency” observed (i.e. low IC) may indicate transposition and substitution used
- However, my HistoCrypt 2021 paper (presented June 2022, Amsterdam) argued against that
- Look at 24 “pieces” of information EASTNORTHEAST
BERLINCLOCK
 - Does Scheidt think he’s provided $\binom{24}{2} = 276$ new pieces of information
 - Also we have extra information: the locations of the texts, and possibly extra hint given that texts are at positions 21/63 (starting index at 0)



Eliminate transposition and substitution (2)

- Assume plaintext standard alphabet and ciphertext standard alphabet
- Look at **pairs of plaintext letters** – some specific subsets of them – what **pairs of ciphertext letters** do they map to?
 - (why even pairs – why not triples)
 - The specific subset I look at is pairs which are “close” in the plaintext alphabet – meaning the distance between the letters is low – say 0, 1 or 2 apart
 - In HistoCrypt 2021 I looked at distance = 0
 - After conference, looking at distance 1 I find even “stronger” patterns

Stronger patterns

- Setting PT alphabet = CT alphabet = standard A-Z
- Look at PT letters 0 or 1 apart
- Eg “B” from “BERLIN” and “C” from “CLOCK” we have BC goes to NM and BC goes to NP; distances 1 and 2
- Of these 34 pairs, sum of distances is 128; look at $128/34 = 3.76$
- Permute ciphertext – with 24 letters, a 1 in 5,000 observation
- Also note count of distances ≤ 3 or 4; a 1 in 35,000 observation (“k4-xy.c” with A-Z and A-Z alphabets)
- Lower probabilities when permuting PT or CT alphabet i.e. not so strong

“1 in 35,000”

- What does this mean exactly?
- 276 pairs of PT/CT letters; where PT difference is 0 or 1 (i.e. same or immediately adjacent), CT difference is 0, 1, 2, or 3 23 times
- This is extremely uncommon in permutations of K4 CT
- The pattern doesn't occur with BERLINLOCK crib alone

pos 24 29 PT S T CT R R diff 0	pos 24 28 PT S R CT R P diff 2
pos 26 27 PT N O CT Q Q diff 0	pos 24 66 PT S R CT R P diff 2
pos 28 66 PT R R CT P P diff 0	pos 64 73 PT B C CT N P diff 2
pos 33 34 PT S T CT S S diff 0	pos 25 33 PT T S CT V S diff 3
pos 22 31 PT E E CT F G diff 1	pos 25 34 PT T T CT V S diff 3
pos 23 32 PT A A CT L K diff 1	pos 26 69 PT N N CT Q T diff 3
pos 24 33 PT S S CT R S diff 1	pos 27 69 PT O N CT Q T diff 3
pos 24 34 PT S T CT R S diff 1	pos 28 33 PT R S CT P S diff 3
pos 29 33 PT T S CT R S diff 1	pos 32 64 PT A B CT K N diff 3
pos 29 34 PT T T CT R S diff 1	pos 33 66 PT S R CT S P diff 3
pos 64 70 PT B C CT N M diff 1	pos 70 73 PT C C CT M P diff 3
pos 23 64 PT A B CT L N diff 2	

Visualizing why this happens

- Sort the plaintext letters into A-Z order

AABCCEEEHIKLLNNOORRSSTTTT (PT)

KLNM^PFG^YNTK^VZQT^Q^FPPRSRRSV (CT)

- Makes you want to write **MZPFK** for CLOCK because the F stands out like a sore thumb. MF much closer than QF. Adjusted version:

AABCCEEEHIKLLNNOORRSSTTTT (PT)

KLNM^FFG^YNTK^VZQT^Q^PPPRSRRSV (CT)

Generating a digital “pseudo-random” key

- “All the principles in the current major electronic key generators involve binary addition of random key streams to digitalized plain language. The big-name principles again are Fibonacci, Koken (There is also something called Kokenacci, combining the features of both) and ciphertext autokey, CTAK.” David G. Boak Lectures, “A History of US Communications Security”, NSA 1973
- “A Koken machine consists of a set of N wheels, each with a prime number, q , of points. The kick of each wheel is some linear combination, mod q , of the position numbers showing on the wheels.” (October 1950 via Frode Weierud)
- “You're going to start to reverse engineer some of these digital algorithms and figure out, well how, how do you get that the answer out of something that starts in English here and works that way” – Scheidt 2015

Autokey in CIA Reading Room website

- **MEMORANDUM FOR:** OC Equipment Board Members
- **FROM:** [REDACTED]
Secretary, OC Equipment Board
- **SUBJECT:** Minutes of OC Equipment Board Meeting No. 2-76

Meeting No. 2-76 of the OC Equipment Board was held on 13 July 1976. The following persons were in attendance: [REDACTED]

- The second and last agenda item concerning the KG-84 cryptographic system was introduced by [REDACTED] who stated that the problems to be discussed were uncovered as a result of OC-CS attempts to get an early in-depth look at the auto-key features of this system. [REDACTED] then proceeded to describe the general features of the KG-84. The KG-84 is a dedicated loop encryption device that is part of the overall Tenley program and features remote rekeying and variable update. It uses the Saville family of cryptologic, the same used in the Vinson program. There are three crypto variables - an update variable (daily), a new traffic variable (monthly), and a rekeying variable (3 months - 1 year). The rekeying and daily variables are updated manually on-site, whereas the monthly variable is usually updated electrically from the remote end.

How close to “traditional” Gromark can we get?

- Tradition: primer is base 10, length 5, use standard Fibonacci addition of first two terms.
- Quite “mathematical” for an “anathemath”
 - Also, plain alphabet is standard A-Z, cipher alphabet is “keyword mixed” (a Friedman and ACA term)

- PT ABCDEFGHIJKLMNOPQRSTUVWXYZ

- CT AJRXEBKSYGFPVIDOUMHQWNCLTZ

- Key: ENIGMA (264351)

Primer: 23452

Transposition block

2 6 4 3 5 1

E N I G M A

B C D F H J

K L O P Q R

S T U V W X

Y Z

K: **23452**579772664982037023072537978066

pt: thereareuptotensubstitutesperletter

CT: NFYCKBTIJCNWZYCACJNAYNLQPWWSTWPJQFL

Gromark in “Military Cryptanalytics III”

- Gromark from ACA DUMBO 1969
- Here explained in 1977 (“pentanome”) with “rule of combination”
- “KRYPTOS” would give numerical key of 1473625 expand to 28 digit sequence
11473621473141
47362514736147

f. In the case of digital cryptosystems, various methods have been used to produce an expanded key from a shorter one. Several examples will now be cited.

(1) The method in subpar. *d*, above, may be adapted so that from the key word CHRISTMAS the basic numerical key 236479518 is expanded into the 45-digit sequence 2 3 6 4 7 9 5 1 | 2 | 2 3 | 2 3 6 4 | 2 3 6 4 7 9 5 | 2 3 6 | 2 3 6 4 7 | 2 3 6 4 7 9 5 1 8 | 2 3 6 4 7 9. Or, this 9-digit basic key may be expanded into an 81-digit key by tying together 9 cycles of the basic key, beginning with 1 8 2 3 6 4 7 9 5 | 2 3 6 4 7 9 5 1 8 | 3 6 . . . and ending with | 9 5 1 8 2 3 6 4 7. Or, again, the 9-digit key may be expanded into a 90-digit key by adding 1 to the digits of the basic key at the end of each cycle, so that the final key will be 2 3 6 4 7 9 5 1 8 | 3 4 7 5 8 0 6 2 9 | 4 5

(2) Another method for producing digital key is by a “Fibonacci series,”² which is a series or sequence generated by the successive addition (almost invariably mod 10, or, in certain specialized usages mod 2) of pairs or larger combinations of elements (usually adjacent), beginning with a specified initial key number. Thus, in its simplest form, if the initial key is the dinome 01, we can generate the Fibonacci sequence 0112358314 . . . , which has a cycle length of 60. If the initial key is the pentanome 00001 and the rule of combination is $a+b=f$ (i.e., the sum of the first and second elements of the sequence

How far is cipher from “traditional” Gromark?

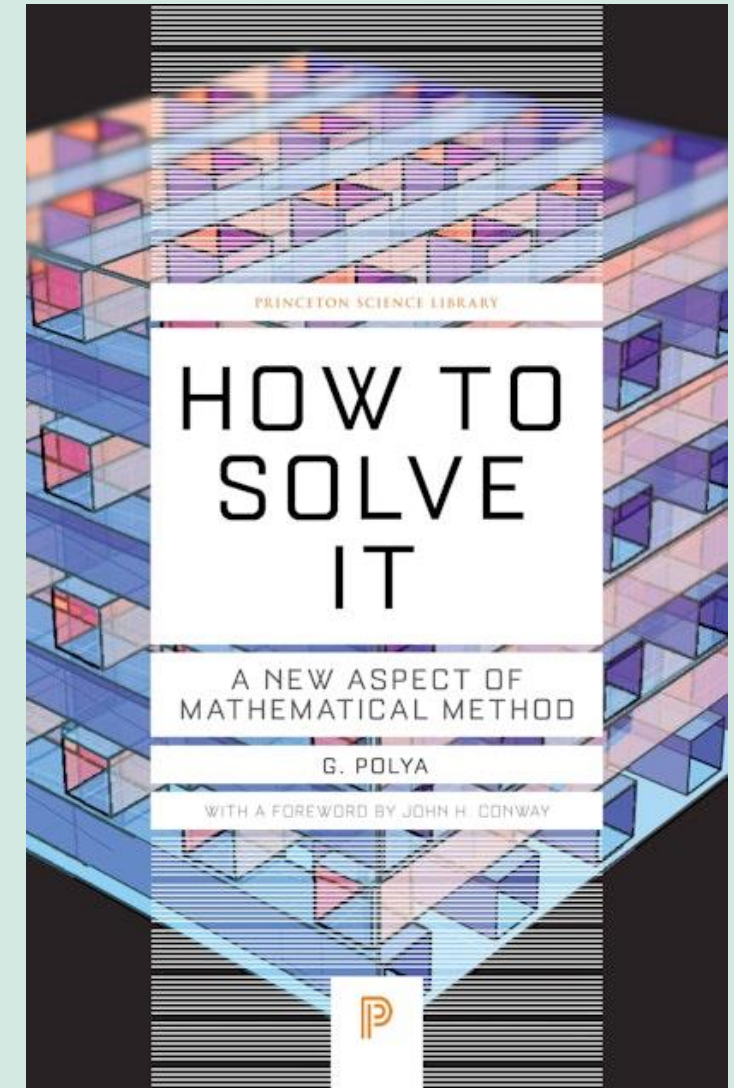
- Was there a mistake made, or is a “slight” variant in use?
- How realistic is it we can guess a method given only 24 letters with matching positions?
- What if we forced the PT alphabet to be A-Z?
 - How many of the 24 letters can we match (in sequence?) with a 0-9 key?
 - E.g. 21 letters from the crib. Cipher “P” needs to map to plain “R” and “C” which are 11 letters apart in the A-Z alphabet - <https://kryptos.richardbean.id.au/gromark.html> (Sep 2018)
 - Also cipher “K” needs to map to plain “A” and “K” which are 10 letters apart in A-Z. “Skip” programs in C

ABCDEFGHIJKLMNOPQRSTUVWXYZ
LAMKFYGNHXIZBTQCDPUVSROJWE

EASTNORTHEAST BERLINLOCK
0030100202321 61085000... SUM = 34
FLRVQQPRNGKSS NYPVTTMZFPK

Questions arising

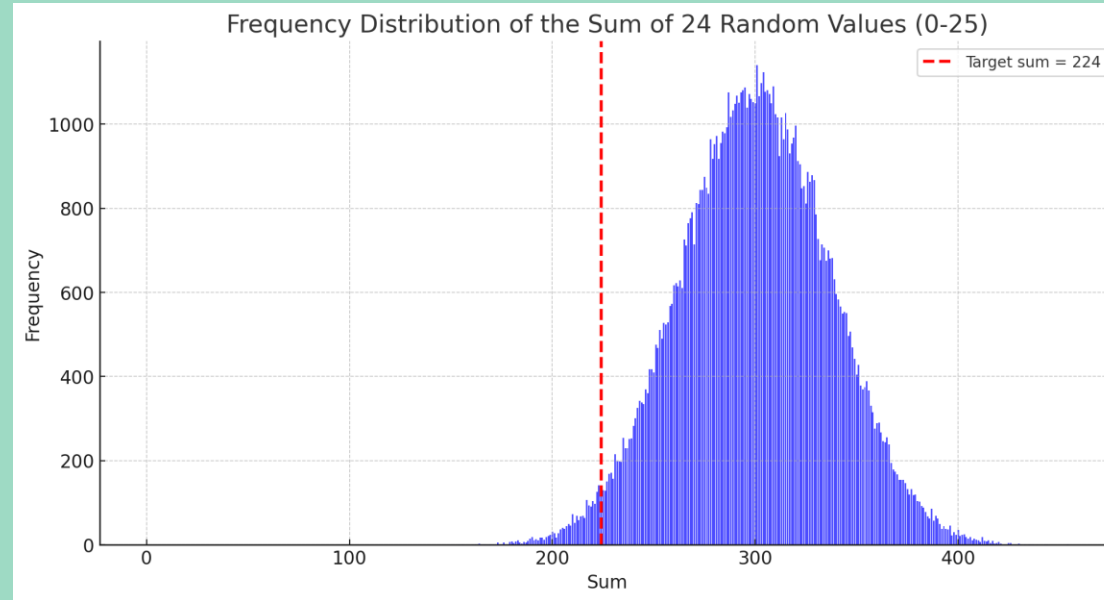
- If it's A-Z plain alphabet and “digital” offsets – base is at least 12, like a clock, to hit all 24 letters. Have some programs to do that ...
- How is the method so simple that **KR/SO/T/YP** can be “chosen” at certain locations? Why do PT letters KRYPTOS appear to move little (Materna)?
- What about autokey? Two major variants are PTAK (plaintext autokey) and CTAK (ciphertext autokey)
- If we assume CT alphabet = PT alphabet = KRYPTOS alphabet as in K1 and K2, the implied key is
 - **RDUM RIYWO YNKY ELYOIE CBAQK**
 - Is there anything unusual about this? We should be expecting something “random” unless perhaps the positions were chosen to give a certain pattern
 - 10 out of 24 letters from “KRYPTOS”, expected 6.46 letters. Not uncommon
 - Assume “good faith” perhaps
- In numeric terms from the KRYPTOS alphabet these sum to 224. If it was “random” it would sum to $(0+25)/2 \cdot 24 = 300$. English letters would sum to somewhat less; about 247. Call this the **Ksum**.
- Let's visualise that (following “How to Solve It” by Polya)



Get ChatGPT to help

- If I pick 24 random values and each of the values is an integer randomly chosen from the numbers 0 to 25 inclusive, I need to visualize and quantify how "rare" it is if the sum of the values is 224 or less. Please write Jupyter Notebook code to produce a plot where the plot shows how unusual that value is.

Response



The plot illustrates the frequency distribution of the sum of 24 random values, each chosen from the range 0 to 25 (inclusive), based on 100,000 trials. The red dashed line represents the target sum of 224.

From the simulation, we can see that the probability of the sum being 224 or less is approximately 0.01993 or about 1.993%.

This indicates that it is quite rare for the sum of these 24 random values to be 224 or less, as it occurs in less than 2% of the cases in this simulation.

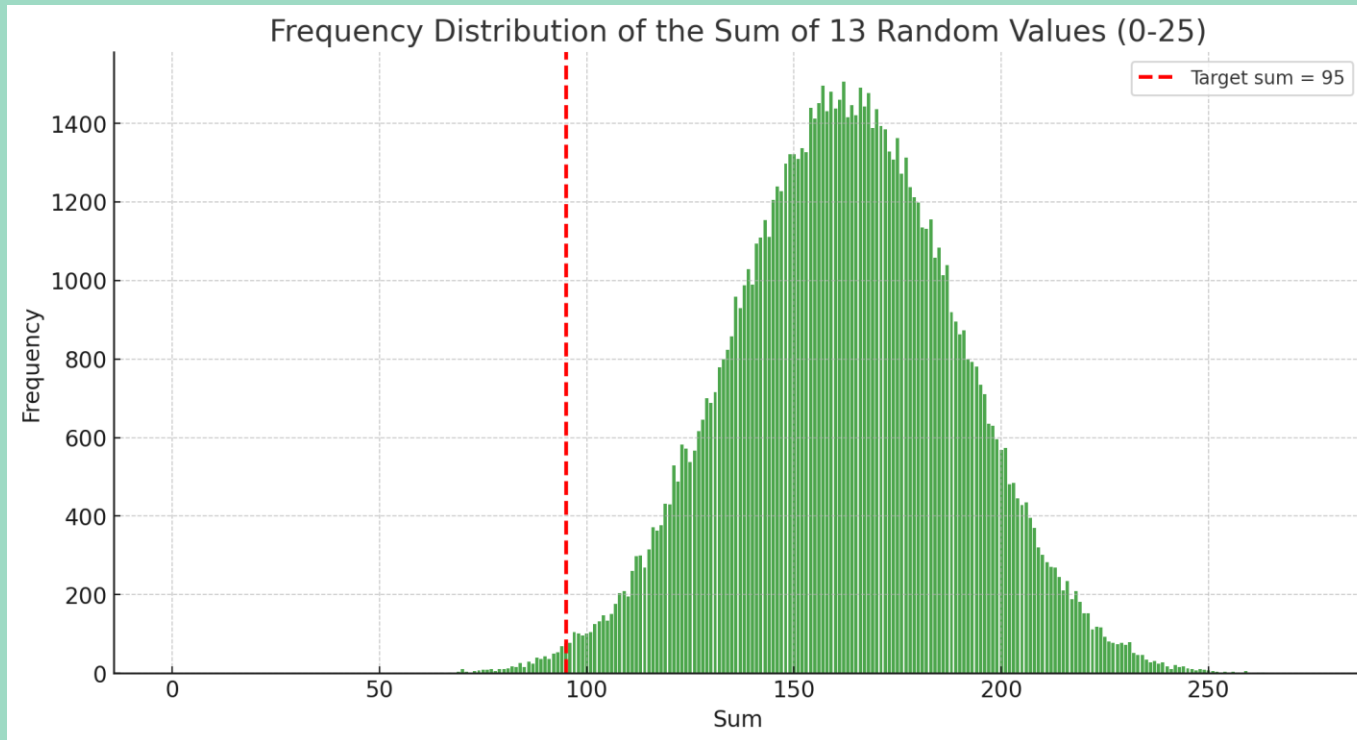
Summary

- The Ciphertext is **FLRV QQPRN GKSS NYPVTT MZFPK**
 - KSum = 252, top 9.5%; for whole 97 letter CT, sum = 1130, top 13%.
- Corresponding Plaintext in English: **EAST NORTH EAST BERLIN CLOCK**
 - KSum = 210, In English: top 9.9%, in all text top 0.7%.
- Implied Vigenere Key with K-alphabets: **RDUM RIYWO YNKY ELYOIE CBAQK**
 - KSum = 224, in English: top 21%, in all text top 2%, as found. Quite “Kryptossy”.
 - Could this be transposed English? (e.g. as Seaman suggested)
 - Chi-squared tests indicate about 99.6% of English scores are lower
 - But it depends on source e.g. 97-letter source with lots of Ks/Ys (e.g. ...)
SAYSTHEMOSTHORRIBLEWORDSSPOSSIBLESHESAYSIKNOWWHATYOU'RETHINKINGYOU'REASKINGYOURSELF
DI DMYSTALKERCHECK
 - Matching to English from Gutenberg/books3, best match has 22 letters in common
WAITINGFORTHEKINGTHEK **INGH ADEXP ECTE** DTHATEVERYTHINGWOULDBEREADYIN **AFEWDA YSBUT**
HEWASDESTINEDTOENCOUNTE (Gutenberg book 25275)
 - This pattern is seen in both EastNortheast and BerlinClock cribs

Consider even positions

- **RURYONY – EYICAK** – sum is 95 – $95/13$ – average 7.3 vs expected 12.5
- `shuffle(pl,13,1); shuffle(pl+13,11,1);` - 1 in 1686 (permute known plaintext)
- `shuffle(k4_perm+21,13,1); shuffle(k4_perm+63,11,1);` - 1 in 1186 (permute sections of ciphertext)
- `shuffle (pl,24,1);` - 1 in 934 (permute all known plaintext)
- `generateRandomString(24,pl);` - 1 in 630 (random English plaintext)
- What's happening?
 - Are the even positions derived from a keyword, or keyphrase, with monoalphabetic sub changing common letters into letters at the start of the KRYPTOS alphabet? E.g. ESTONIAR BCDFGHJKLM ... WXYZ -> KRYPTOS ABC ... VWXZ? Then it's PTAK with K alphabets, plus a substitution?
 - Linotype alphabet has "American roots" ETAOIN SHRDLU ...
- If so can we build left or right and work out what keyword lengths would work?
- Hamid Samak (2018) also noted that E.Y.I.C.A.K was consistent with ErYglmCrAcK "gimcrackery" as a rotated keyword <http://kryptos.ir>

Even positions response



The plot shows the frequency distribution of the sum of 13 random values, each chosen from the range 0 to 25 (inclusive), based on 100,000 trials. The red dashed line indicates the target sum of 95.

From this simulation, the probability of the sum being 95 or less is approximately 0.00635 or about 0.635%. This suggests that it is quite rare for the sum of these 13 random values to be 95 or less, occurring in just over half a percent of the cases in this simulation.

If it's a real pattern what could it mean?

- Elonka 2006 Scheidt B-Roll call

*I was able to be on the conference call when the New York Times reporter interviewed Ed Scheidt. Much of what Ed said did not make it into the article, but here are my miscellaneous notes from the call on what he *did* say. ... The systems used were classical cryptography, "not something weird".*

- i.e. could it just be pure PTAK or CTAK with random alphabets? Or keyword derived alphabets?
- Would we ever find those alphabets?

Autokey ideas

- If it's just **classical cryptography**, could it be:
 - Ciphertext autokey with two unknown alphabets, perhaps one KRYPTOS related (doesn't work at widths 1 to 21)
 - Plaintext autokey with two unknown alphabets, perhaps one KRYPTOS related (ptak21 – widths 5,6,7,9,11,12,13,14)
 - Alternating ciphertext/plaintext autokey (c-and-p, p-and-c)
 - Working with K/K alphabet, but mono sub of plaintext with PTAK (p-bare, nothing works)
 - Working with K/K alphabet, but mono sub of ciphertext with CTAK (c-bare 10 to 14)
- Could we start with a plaintext word? i.e. a primer. Go back to Gaines

PTAK results

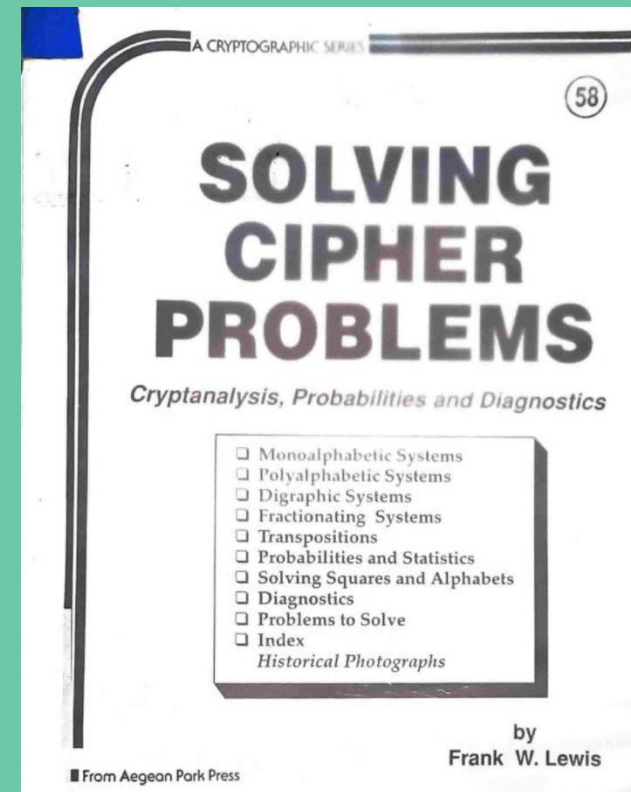
- Forcing PT alpha = K alpha, primer length 12 works and converges e.g.
- DVANMICTPJXKZLUSGYOBQHWERF as CT alphabet
 - plaintext = **VHPSEDHIGHSMWRIAQIOTCEASTNORTHEASTERMHIHOSTBLARETHMUSADMHUUQZERBERLINCLOCKUBIDUUhKIUVJJSSTANCELAY** (ic 0.0490) or
- BMZNGUFHPJRKILESDYVXQCOTWA as CT alphabet
 - plaintext = **FHASSLAVIUSTHRIASINTCEASTNORTHEASTILQTIHOSTBBAGETUBUSARBTMERZEMBERLINCLOCKSVODETT****KTEPTOCYUHRDELHA** (ic 0.0584) great IC but implied primer **DFTTZOFKIFZC** not credible
- PT alpha based on unwind K xpsn or Wheatstone: KEVAMTIRFWBNOJYGXCQSLPHZDU or KAHUOFNPDLXRBIVSGQTEMZYCJW or Hannon ALWHSEPBMXITFQCNYJUGRDOZKV
- Forcing PT alpha = CT alpha, primer lengths 12, 13
- Forcing PT alpha = CT alpha reversed, primer lengths 7, 9, 11, 13
- Forcing a primer, e.g. ANTIPODES; but unlikely to converge
- With no limits on primer or alphabets, won't converge. Best results seem to be at primer length 12
- Lag 7 answers all begin with "O"; letters 1,8,15 all "O"

Autokey obscure ideas

- It could be CTAK with very long primer. Lowest length that works is 34 (e.g. “supercalifragilisticexpialidocious” 34 letters, “andyeshallknowthetruthandthetruthshallmakeyoufree” CIA motto 49 letters)
- Could be PTAK but starting at end going R to L not L to R (8,9,10,12,13)

PTAK, what else is left?

- Find keywords from sculpture?
- Then, pick a primer length (lag) value of 5,6,7,9 and try pairs of related alphabets (with 26 offsets)
- Or, go through primers, shortest first, dyahr/hydra based, find which primers “work”
- Alternatively, iterate between improving PT and CT alphabets – an interesting concept
- PTAK – but transposed. This would be solvable, but a complex pen-and-paper cipher. Could use 97 or 98 letters. 97 letters would be difficult to decipher manually.
 - Lewis notes PTAK is highly error prone.
 - Can we simplify? E.g. Knights move transpositions, skips (like K3), railfence (as in US Civil War), etc.



PTAK lag 5, 6, 9, 11, 12, 13 force 2-5 other letters

- Starting numbering at letter 1: (22-34 forced, 64-74 forced)
- PTAK lag 5: 19 T, 61 A
- PTAK lag 6: 40 R, 60 E
- PTAK lag 9: 43 T, 87 N
- PTAK lag 11: 1 A, 40 A, 43 T, 44 E, 52 H
- PTAK lag 12: 43 T, 49 T, 95 L
- PTAK lag 13: 51 T, 58 E
- These are too few and distant from known PT to help

PTAK lag 7 forces eight other letters

- 1 O
- 9 A
- 15 O
- 21 C
- 40 N
- 59 C
- 78 K
- 84 C
- 21 C is directly adjacent – “...C EAST NORTH EAST”
- 78 K is close – “BERLIN CLOCK ...K”

PTAK lag 7 forcings

O.....

.A.....

O.....C

EASTNOR

THEAST.

....N..

.....

..C....

.....

BERLINC

LOCK...

K.....C

.....

.....

DOMESTIC

ROMANTIC

VOLCANIC

COSMETIC

FORENSIC

MONASTIC

HOLISTIC

LOGISTIC

HORRIFIC

DOGMATIC

SOCRATIC

ZOONOTIC

ORGANIC

OLYMPIC

OCEANIC

OSMOTIC

ONEIRIC

OF THE DC

ON THE DC

OF AN ARC

ON AN ARC

OR AN ARC

O. MAGIC

WORK

TICK

BACK

LOOK

MARK

THEK

TOOK

DESK

JACK

KICK

LOCK

PICK

TALK

WALK

2-word n-grams with EAST and CLOCK from BeijingHouse

- METASTATICEAST 108
- PARAMAGNETICEAST 104
- ADYNAMICEAST 102
- ...

And so on. Either “...IC EAST” or “ARC EAST”

Most likely to be “...TIC EAST”.

In context, more likely to be “...MAGNETIC” than DYNAMIC, STATIC, GENETIC, ISOTROPIC, HISTORIC, PLASTIC, SYMPATHETIC, LINGUISTIC, LOGIC, ELECTRIC ... but can't be “MAGNETIC” because letter 15 is O

CLOCK ... WORK, TICK, TICKS, TICKING

Solving for plain and cipher alphabets simultaneously

- Nothing in “AZDecrypt” like that – seems to solve only for one alphabet at once
- CryptoCrack, CrypTool?
- The obvious approach is just pick plain/cipher alphabet, then a swap within that alphabet
- Gromark convergence is easy with 24 letters
- Digrafid convergence is not too hard either
- Even with 36 letters e.g. “THIS CITY EAST...” ... “CLOCK ARE H...” I could not get convergence with letter swaps
- PTAK is more like Playfair – we have to experiment with simulated annealing parameters like temperature schedules, and different kinds of swaps to get improved performance

Tricky ideas

- Take two keywords
- Build a mixed alphabet from keyword 1/2, unwind the transposition using keyword 2/1
 - I can't really see an easy way of solving those without trying all pairs of keywords
- Perform PTAK using either keyword 1 or 2
- Would the weird nearness patterns we've observed still hold?
- Could we have chosen the **KR/SO/YP/T** patterns on edges of Kryptos (which aren't on e.g. ANTIPODES)?

Cipher Challenges

- **Byrne** Chaocipher
 - Byrne (1953) challenge ciphers in book
 - Kruh and Deavours Challenge (1990) – O/D and U/V errors in published text “Exhibit 5”
 - Calof, Hill and Rubin (2014) – found printout in National Cryptologic Museum
 - Lasry, Rubin, Kopal and Wacker (2016) “Exhibit 6” solution found through Project Gutenberg search. Kruh and Deavours more transcription errors. “Encipherment was done by computer and can thus be considered error-free.”
- **Feynman** (1987 Usenet post – Chris Cole)
 - Vierra (2023) using AZDecrypt
 - Very unaesthetic – doesn’t seem to be a “fair” challenge for a manual solver
- **Code Book** (Simon Singh) book cipher #5
- **Can you crack the Enigma Code** (Richard Belfield) low ICs
- **Decipher Puzzles** (Warren Holland 1983-85) book cipher. <https://kryptos.richardbean.id.au/group/decipher.txt>

Cipher Challenges

- **Gillogly** Nova Double Playfair (1999) “The Double Playfair turned out to be too hard for this kind of a contest. ... I did a quick revision, added a big clue (i.e. one of the keywords), and hoped that would be enough to make it accessible. However, the British typically needed quite a lot more material to begin reconstructing the squares... mea culpa.”
- **Schmeh** (2020) Playfair 24 and 22 letter challenges
 - Solved only with assistance of a colossal language model from 2014
 - A massive step up in difficulty from previous challenges (50, 40, 30, 28, 26 letter challenges)
 - So short that many phrases already found on web could be solutions to either challenge
 - “avoid visual deficiency”, “the verdict would be half”, “firm developed the brief” for 22 letter
 - “gifts bestowed to her family”, “private sector in making his”, “post from other sites using” for 24 letter
 - Schmeh needed to accept a block of solution attempts in order for resolution
- **Call of Duty Zombies** challenge ciphers <https://www.reddit.com/r/CODZombies/wiki/treyarch-ciphers/>
 - Covering games and comics from Treyarch from 2009 to 2020
 - Morbit (ACA 1964), AMSCO (Gaines 1939 from Scott 19th century), Fractionated Morse (Gaines 1939 from Ohaver about 1910)
 - Some ciphers are famous historically but quite obscure for challenge ciphers e.g. Purple
 - Leads to familiar questions like: are cipher types hinted at in context? And how can you diagnose a rare cipher from just CT?

Intermission

- Moving on to the people and the art ...



Dieter Binniger (1938-1991)

“Unter anderem erfand er Pappmöbel, eine Kompostieranlage, Videoüberwachungsanlagen und - nach der Wende - eine rückwärtslaufende DDR-Uhr, die reißenden Absatz fand.”

<https://www.wunschliste.de/spielfilm/binningers-birne>

"Among other things, he invented cardboard furniture, a composting system, video surveillance systems, and – after the reunification – a backwards-running GDR clock, which became a bestseller."

August 1973 Dieter Binninger Berlin Clock patent

<https://worldwide.espacenet.com/patent/search?q=pn%3DDE2339482A1>

An electric clock can be read from a greater distance, **particularly at night**, by replacing the dial and hours/minutes hands by a matrix of rectangles which are illuminated by lamps or light-emitting elements and switched on and off by the clockwork. In the upper row each element is switched on after 5 hours, in the second row hourly, in the third row every 5 minutes and in the bottom row every minute. The elements can have a different colour and can include date and weekday displays.

GO4C 1973 17-00 AT:3.8.73 OT:20.2.75

- 15 -

Fig. 1

2339482

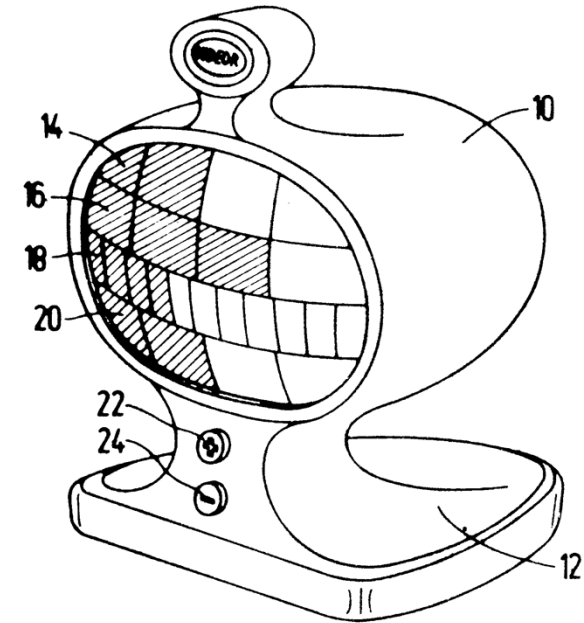
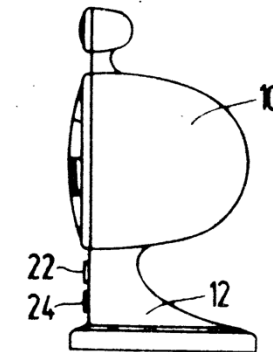


Fig. 2



509808/0508

John le Carré (1931-2020)

- Globe and Mail, 18 November 1989

For a while, in the Cold War's aftermath, the public fascination with espionage may abate, though somehow I doubt it. The spy writer, like the trade he shadows, does not disappear, he merely relocates. If the field thins a little and the quality improves, so much the better for all of us. If only the same thing would happen to the spies. A kind man wrote to me the other day asking me to join him in designing a piece of sculpture for the CIA's headquarters in Langley, Va. Discretion prevents me from telling you the theme of his sketch, but it certainly was not a headstone.

147 A simple code, known by cryptographers as the Caesar mono-alphabetic cypher, is used in the Latin. Its deciphering is simple: just substitute the preceding letter in the alphabet:

Latin:	xknk	qbsuf	tbmkt
	vini	parte	salis
English:	xjnf	qbsut	tbm
	wine	parts	salt

The English version follows the original in failing to encode the *n* in the first word. This chapter provides one of the earliest

known accounts of the making of alcohol. The salt added to the wine before distillation would aid the separation by lowering the vapor pressure of water relative to that of alcohol. For a discussion of the history of alcohol, see Diels (1913, 1924), Degering (1917) and Forbes (1948). The translators wish to acknowledge a helpful correspondence on this chapter with Mr. J. J. McCusker of the University of Maryland.

Another recipe from the same time period is found in the *Mappae Clavicula*, which may predate the recipe by Salernus [7, 10, 11, 49]. This Medieval Latin text, the title of which translates as “Little Key to Painting”, consists of a compilation of recipes for a number of crafts including metalwork, dyeing and other chemical arts [7, 11]. It is thought that the earliest version of this text dates to ~820 CE, but available manuscripts consist of only 10th and 12th century versions [11, 49]. The alcohol recipe is found in the 12th century version, but is not contained in the earlier version [10, 11, 49]. The recipe from the *Mappae Clavicula* was written with portions given in the form of a cryptogram, as shown in the original Latin [7]:

Ad bonum argentum solidandum nedium oboli. De commixtione puri et fortissimi xknk cum iij qbsuf tbmkt, cocta in ejus negocii vasis fit aqua quae accensa flammans in-combustam servat materiam.

Scheidt as cryptanalyst (?!)

CIA biography (“Featured Story” 19 December 2008)

“Scheidt [was] a cryptographer and key player in the Office of Communications” ... “In 1963, he was hired to work as a communications officer ... In the 1980s he became a communications security officer.” (no mention of “head of a/the Cryptographic Center”)

Scheidt has also contributed to cracking codes in the academic world. He helped break a Middle Age manuscript that illustrated an alcohol distilling process by guiding the translator to what he thought was the methodology that provided the key.

“Not too exciting today, but in the 13th century, how to make alcohol would have been a secret and not shared with the masses,” Scheidt said.

This enciphered manuscript appears to be the “*Mappae Clavicula*”

There's an exhaustive bibliography by Seth Rasmussen called [Distillation and the Isolation of Alcohol](#). The only enciphered manuscript in the list is “*Mappae Clavicula*”

<https://web.archive.org/web/20090114013743/https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/ed-scheidt.html>

Tangent ... CIA Enigma page

<https://web.archive.org/web/20090114100410/https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/cracking-the-code.html>

<https://www.cia.gov/stories/story/who-first-cracked-the-enigma-cipher/>

<https://www.cia.gov/legacy/museum/artifact/enigma-machine/>

<https://www.facebook.com/photo.php?fbid=959507670730906&id=857515997596741&set=a.861337030547971>

“The machine was developed by the Dutch to communicate banking secrets. The Germans bought the patent in 1923 for intelligence purposes. Polish intelligence was able to purchase an Enigma at a trade fair and procure a codebook from a French agent. When Poland was overrun in 1939, the Poles realized they wouldn’t have capabilities to solve the code and gave the information and machine to the Allies.”

Claim now cited in books e.g. “Wireless Communication Systems” by Haupt (2019)



F. L. Bauer 1999

CRYPTOLOGIA

July 1999

Volume XXIII Number 3

AN ERROR IN THE HISTORY OF ROTOR ENCRYPTION DEVICES

Friedrich L. Bauer

ADDRESS: 19 Noerdliche Villenstrasse, D-82288 Kottgeisering GERMANY

ABSTRACT: Many historians have erred in giving credit for the Enigma cipher machine of World War II famed to Hugo Koch and not to the rightful inventor, Arthur Scherbius. This is corrected here.

KEYWORDS: Enigma, rotor, NSA, Hugo Koch, Arthur Scherbius, David Kahn, Arvid Gerhard Damm, Siegfried Türkel, Edward Hugh Hebern, patents, Securitas.

TECSEC 1996

P2 is TecSec's "*patented* high performance cryptographic algorithm"

The screenshot shows the homepage of TECSEC, Inc. The browser address bar displays 'http://www.tecsec.com/'. The page features a header with the company logo (a stylized 'ST' in a green box) and the text 'TECSEC, Inc. For All Your Security Needs'. To the right of the logo, contact information is listed: '1953 Gallows Road, Suite 220 Vienna, Virginia 22182-3934 (703) 506-9069 Voice (703) 506-1484 Fax'. Below this, a navigation bar contains three buttons: 'Tecsec, Inc', 'Software', and 'Hardware'. The main content area is titled 'The Company' and contains a paragraph of text describing the company's history and mission.

TECSEC, Inc.
For All Your Security Needs

1953 Gallows Road, Suite 220
Vienna, Virginia 22182-3934
(703) 506-9069 Voice
(703) 506-1484 Fax

[Tecsec, Inc](#) [Software](#) [Hardware](#)

The Company

TECSEC is a small high-technology company devoted to the development of security and privacy products and consultation in the areas of INFOSEC. The company was founded by Mr. Edward Scheidt. His years of government service culminated in a position as Chief of an organization within the Intelligence Community which focused on cryptography and key management issues. He realized that computer and communications security (collectively referred to as "INFOSEC") was not something that should be limited to either the government or the province of big banks. And, having the background in INFOSEC and cryptography, set out to produce a series of hardware and software products that could be used in both the government and private sector, at all levels, to promote the implementation of good security practices and to provide simple and cost-effective security measures to protect computer, data, conversations and other types of transmissions from surveillance and/or compromise.

The screenshot shows the 'Software Division Engine Support' page. The browser address bar displays 'http://www.tecsec.com/software/engines.html'. The page features a header with the company logo (a stylized 'ST' in a green box) and the text 'Software Division Engine Support'. To the right of the logo, contact information is listed: 'TECSEC, Incorporated 1953 Gallows Road, Suite 220 Vienna, Virginia 22182-3934 (703) 506-9069 Voice (703) 506-1484 Fax'. Below this, a navigation bar contains three buttons: 'Tecsec, Inc', 'Software', and 'Hardware'. The main content area is titled 'Encryption Engines Supported:' and contains a list of encryption engines. The engines listed are: DES Codebook, DES Cipher Feedback, DES Triple Codebook, DES Triple Cipher Feedback, DES Triple Output Feedback, TECSEC's P2, IDEA, BLOWFISH, GHOST, FEAL, and FEAL NX. Red arrows point to 'DES Triple Codebook', 'TECSEC's P2', and 'GHOST'.

Software Division
Engine Support

TECSEC, Incorporated
1953 Gallows Road, Suite 220
Vienna, Virginia 22182-3934
(703) 506-9069 Voice
(703) 506-1484 Fax

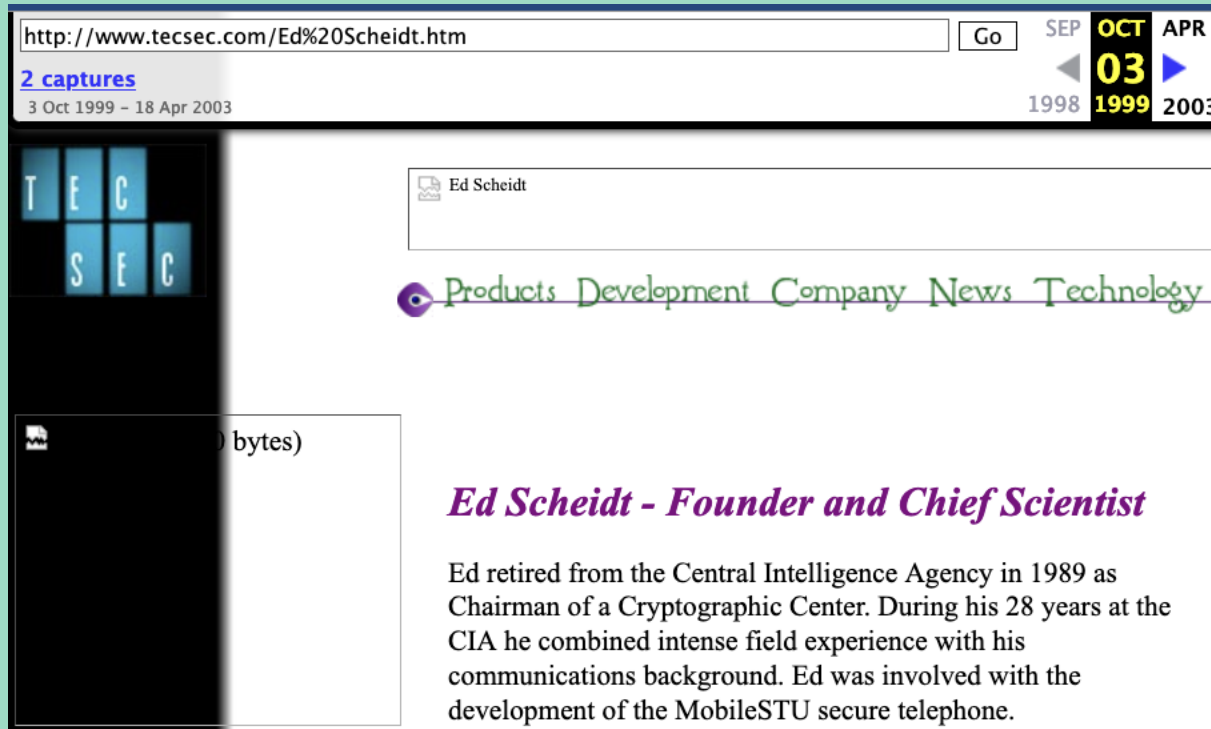
[Tecsec, Inc](#) [Software](#) [Hardware](#)

Encryption Engines Supported:

- DES Codebook
- DES Cipher Feedback
- DES Triple Codebook
- DES Triple Cipher Feedback
- DES Triple Output Feedback
- TECSEC's P2**
- IDEA
- BLOWFISH
- GHOST**
- FEAL
- FEAL NX

TECSEC 1999

Scheidt bio changed from head of “a cryptographic center” to “the cryptographic center” (WaPo, Gillogly, ComputerWorld 1999)



A former CIA official has developed a unique cryptographic management system that provides access control to any data object. Edward M. Scheidt, former head of the CIA's Cryptographic Center, founded TecSec Inc. in Vienna, Va., to commercialize the Constructive Key Management (CKM) system for symmetric key algorithms. It creates a one-time encryption key to access individual databases, documents, photographs or Web pages. The system is now in use by federal agencies and defense contractors, said Scheidt, who recently talked to Computerworld reporter Ann Harrison.

Jim Gillogly

7 Jun 1999, 17:00:00 ☆

to

[tomst...@my-deja.com](#) wrote:

> If you are
> doing just a story on it... It was dropped off in front of the federal
> building by an unknown person some years back. They believe it's some
> quite of substitution (rotating state or something) cipher. No one has
> claimed to drop it off, and as far as anybody knows it's just ciphertxt
> right now. That's all I know anyways.

Uh, that was weird. I think just about everything you said must be wrong. The CIA doesn't let just anybody unload large unknown blocks of masonry in their courtyard. The sculpture was done by James Sanborn and dedicated in Oct 1990. Sanborn said that the CIA "will never figure it out." The cryptographer was Edward M. Scheidt, retired former chairman of the CIA's Cryptographic Center (I didn't know they had one until I saw his bio) and apparently now a beltway bandit. It may be encrypted in sections using different algorithms. I haven't heard that any of it has been decrypted. Given Scheidt's interest in key escrow, I'd expect the key to be hidden in there for somebody who knows what to look for.

Ultimately, he went to the CIA itself. The agency put him in touch with Ed Scheidt, the retiring chairman of its **Cryptographic** Center, and hailed by then-director William Webster as "The Wizard of Codes." A quiet, professorial man who favors ties with hieroglyphic patterns, Scheidt spent four months devising the systems that Sanborn would use.

The P2 Patent

	
US006075865A	
United States Patent [19]	[11] Patent Number: 6,075,865
Scheidt et al.	[45] Date of Patent: Jun. 13, 2000

[54] CRYPTOGRAPHIC COMMUNICATION PROCESS AND APPARATUS	[57] ABSTRACT
[75] Inventors: Edward M. Scheidt , McLean, Va.; C. Jay Wack , Clarksburg, Md.	A communication system, which includes an origination space, a communications channel, and a destination space associated with the origination space via the communications channel. The origination space includes an encryption engine for generating an output symbol O_t based on an input symbol I_t and means for receiving an encrypt key, an encrypt text/key relation, and the input symbol. The destination space includes a decryption engine for generating a decrypted symbol I'_t based on the output symbol received from the origination space via the communications channel and means for receiving a decrypt key and a decrypt text/key relation. The decrypt text/key relation controls the decryption engine such that $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{N-1}[\alpha_{N-2}(t) + \dots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]] \dots]]$, mod W , where $\alpha_N, \alpha_{N-1}, \dots, \alpha_1, \alpha_0$ are $N+1$ additive transformations defined by the encrypt key, where $\pi_N, \pi_{N-1}, \dots, \pi_2, \pi_0$ are N permutations defined by the encrypt key, and where W represents the number of possibilities for each permutation defined by the encrypt key. The decrypt text/key relation controls the decryption engine such that $I'_t = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1} \dots [\pi_{N-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - \dots - \alpha'_3(t)] - \alpha'_2(t) - \alpha'_1(t)] - \alpha'_0(t)$, mod W , where π_i^{-1} is defined by the decrypt key as the inverse of the permutation π_i , where $\alpha'_N, \alpha'_{N-1}, \dots, \alpha'_1, \alpha'_0$ are $N+1$ additive transformations defined by the decrypt key, and where W represents the number of possibilities for each inverse permutation defined by the decrypt key.
[73] Assignee: TecSec Incorporated , Vienna, Va.	
[21] Appl. No.: 09/108,312	
[22] Filed: Jul. 1, 1998	
[51] Int. Cl. ⁷ H04L 9/08	
[52] U.S. Cl. 380/255; 380/28	
[58] Field of Search 380/28, 9, 29, 380/255	
[56] References Cited	
U.S. PATENT DOCUMENTS	
5,375,169 12/1994 Scheidt et al. 380/21	
5,787,173 7/1998 Scheidt et al. .	
5,835,597 11/1998 Coppersmith et al. .	
Primary Examiner—Tod R. Swann Assistant Examiner—Todd Jack Attorney, Agent, or Firm—Rabin & Champagne P.C.	
40 Claims, 2 Drawing Sheets	

Is there anything novel happening here?

No pseudocode or details, more like patenting a *framework* or a *concept*

Without details, can't be assessed or attacked
Unlike e.g. SEAL of Rogaway and Coppersmith cited here, or RC5, RC6, IDEA, RSA etc

Is there anything possibly relevant to Kryptos?

e.g. layers of encryption of “additive transformations” and “permutations”, modulo arithmetic, prime numbers

To be used in a product “VEIL” implementing escrow key management

Sock puppetry for TecSec?

<https://csrc.nist.gov/files/pubs/fips/197/final/docs/fips197-draft-comments-received.pdf>

“extremely high performance” “cutting edge” “strongly feel”

Looks more like advertisement for TecSec than a genuine suggestion;

Rijndael already selected in October 2000?!

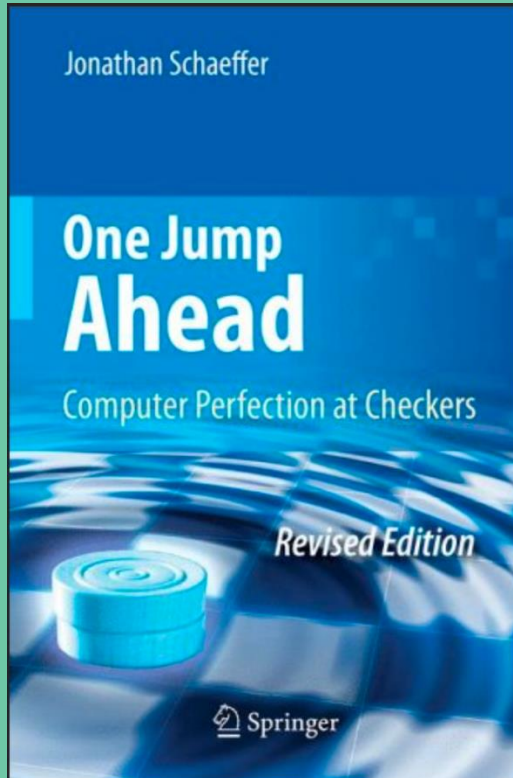
10. Kevin McGowan (04/06/01)

From: "Kevin McGowan" <kevinmcg3@hotmail.com>
To: AEScomments@nist.gov
Subject: AES algorithm
Date: Fri, 06 Apr 2001 13:19:27 -0500
X-OriginalArrivalTime: 06 Apr 2001 18:19:27.0820 (UTC)
FILETIME=[1DBE80C0:01C0BEC6]

I have recently been following the progress and developement of the new AES standard and although Rijndael is a very impressive pick, I feel that one much stronger algorithm has been overlooked. TecSec Inc., a Vienna,VA based cryptography company, produces an extremely high performance cryptographic algorithm called P2. P2 was developed by Ed Scheidt, the former CIA cheif of cryptography, with the utmost regard for producing a cutting edge algorithm. I strongly feel that P2 would outperform Rijndael, and highly recommend that P2 be tested before announcing Rijndael as the standard. I believe P2 to be a much stronger product and I believe the government would greatly benefit by looking into P2. - Kevin

Get your FREE download of MSN Explorer at <http://explorer.msn.com>

Scheidt not son of FBI agent or “Deep Throat of Codes”



- “One Jump Ahead” revised edition (2008), but not first edition (1997), a book about computer checkers, claims Scheidt’s father was the famous FBI agent / checkers player (1903-1993).
- Actually, his father was Edward Henry Scheidt (1892-1976)
- The “Deep Throat of Codes” reference comes from a Washington Times article by Bill Gertz in 1991: *“The sculptor and the Deep Throat of codes conducted business only at secret locations, never by telephone or in writing”*. Webster called him the “Wizard of Codes” (WaPo 1999).
- However, TecSec which Ed Scheidt founded, used the “Deep Throat” quote on their website by 2015.

¹¹ Ed Scheidt, personal communication, March 16, 1991. He was a “G-Man” with the FBI in the 1930s. He moved up the ranks, eventually becoming a senior director in the FBI. His son, also Ed (Edward) Scheidt, is the retired Chairman of the CIA’s Cryptographic Center. Former CIA Director William Webster once referred to him as “the Deep Throat of Codes.”

Scheidt birthplace

From 26 June 2016 to 21 July 2023, the English Wikipedia page claimed his birthplace was “Santa Monica”. However, this was a fabrication inserted by an eccentric Kryptos fan to match Elonka Dunin’s birthplace.

Never believe anything at all from Wikipedia unless you can verify it from an independent, reliable source external to Wikipedia.

Edward Micheal **Scheidt** was born on July 20, 1939 in San Bernardino County, California.

His father’s last name is **Scheidt**, and his mother’s maiden name is **Adema**. If Edward is still alive, he’s now eighty-five years old.

Name	Edward Micheal Scheidt
Sex	male
Birthdate	07/20/1939
Birthplace	San Bernardino County, California
Mother's Maiden Name	Adema

Antipodes (1997)

- This is like a copy of “Kryptos” accessible to the public at the Hirshhorn Museum and Sculpture Garden in Washington DC. It’s slightly shorter (2.4 m vs 3.4-3.7 m for original) and seems to not have verdigris.
- The plaintext mistake “UNDERGRUUND” in K2 plaintext is fixed.
- The header “mistake” rows are removed.
- The **KR/SO/T/YP** pattern is *not* present because of different text justification and layout
- “Antipodes” was a Thomas Jefferson cipher keyword (for Meriwether Lewis cipher)
- “Artichoke” is another keyword for Jefferson cipher
- “Identifiable American roots” in Kryptos design criteria
- *Sanborn: It’s called Antipodes because of the two opposing screens. You’ve got the KGB/Russian stuff on one side, you’ve got the CIA on the other side, and in between that you’ve got the petrified tree, which incidentally before it was petrified, it was in a forest that burned perhaps 200,000 years ago. So it’s a burned-cinder representation of a tree. Having that on the Mall between the Capitol building and the **Washington Monument** is, I thought, probably the most singular, appropriate site for a work that deals with antipodes.*



Yuri Schwebler and Jim Sanborn WaPo 1984

Pipe Dreams The State of Sculpture In Public Places

By Benjamin Forgey Washington Post Staff Writer

25 November 1984

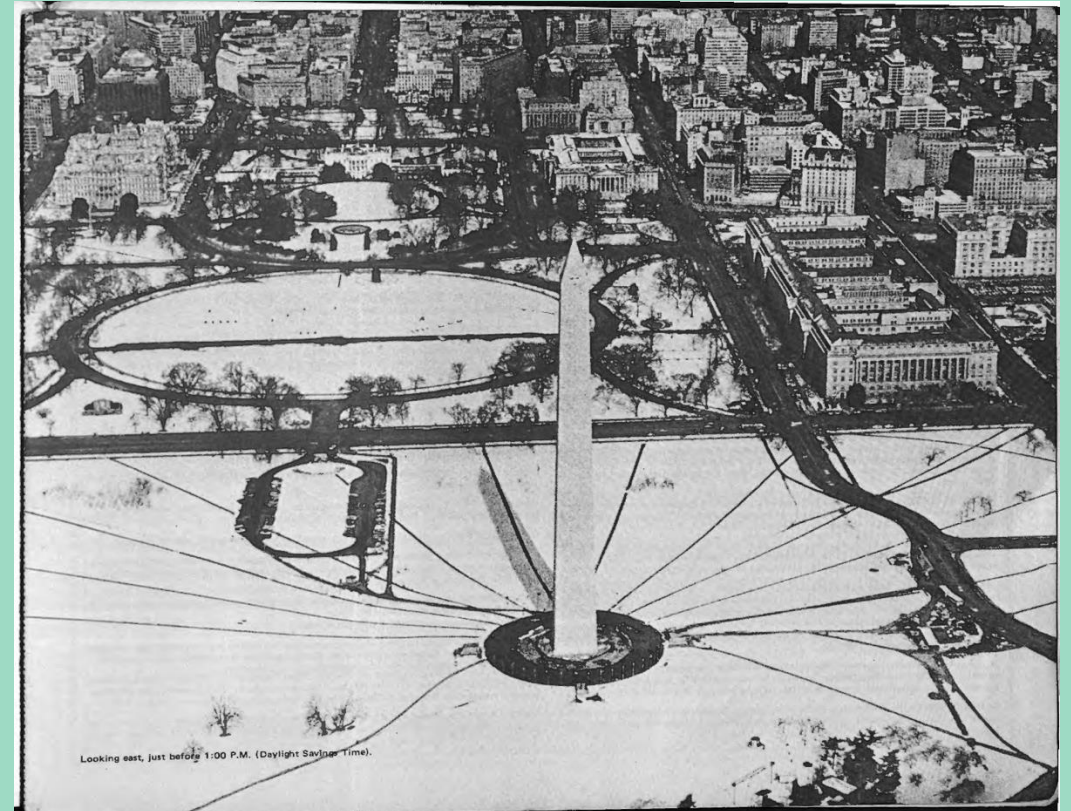
But reactions to the predominance of pure, formalist abstraction have by no means been confined to artists working in traditional figurative modes. Vanguard artists, too, have participated in this process of creative rethinking and, again, one does not have to go farther than Washington to find pertinent examples. Rockne Krebs created here an exhilarating new form of civic sculpture with his inimitably site-specific laser structures. Yuri Schwebler, emphasizing forms and environments related in various ways to basic physical forces or to the history of public art forms (the magnetic North Pole, for instance, or the Russian Constructivists), was an early urban earth artist. Jim Sanborn, whose "Lightning and Other Earthly Forces" was selected for the Hirshhorn's current "Content" exhibition, continues to explore this evocative vein.



Yuri Schwebler and Washington Sundial

- See Yuri Schwebler
"Washington monument as a sundial". There's a YouTube video with CBS News February 1974 footage, a diagram etc.

<https://youtu.be/M5WXcVsflk>



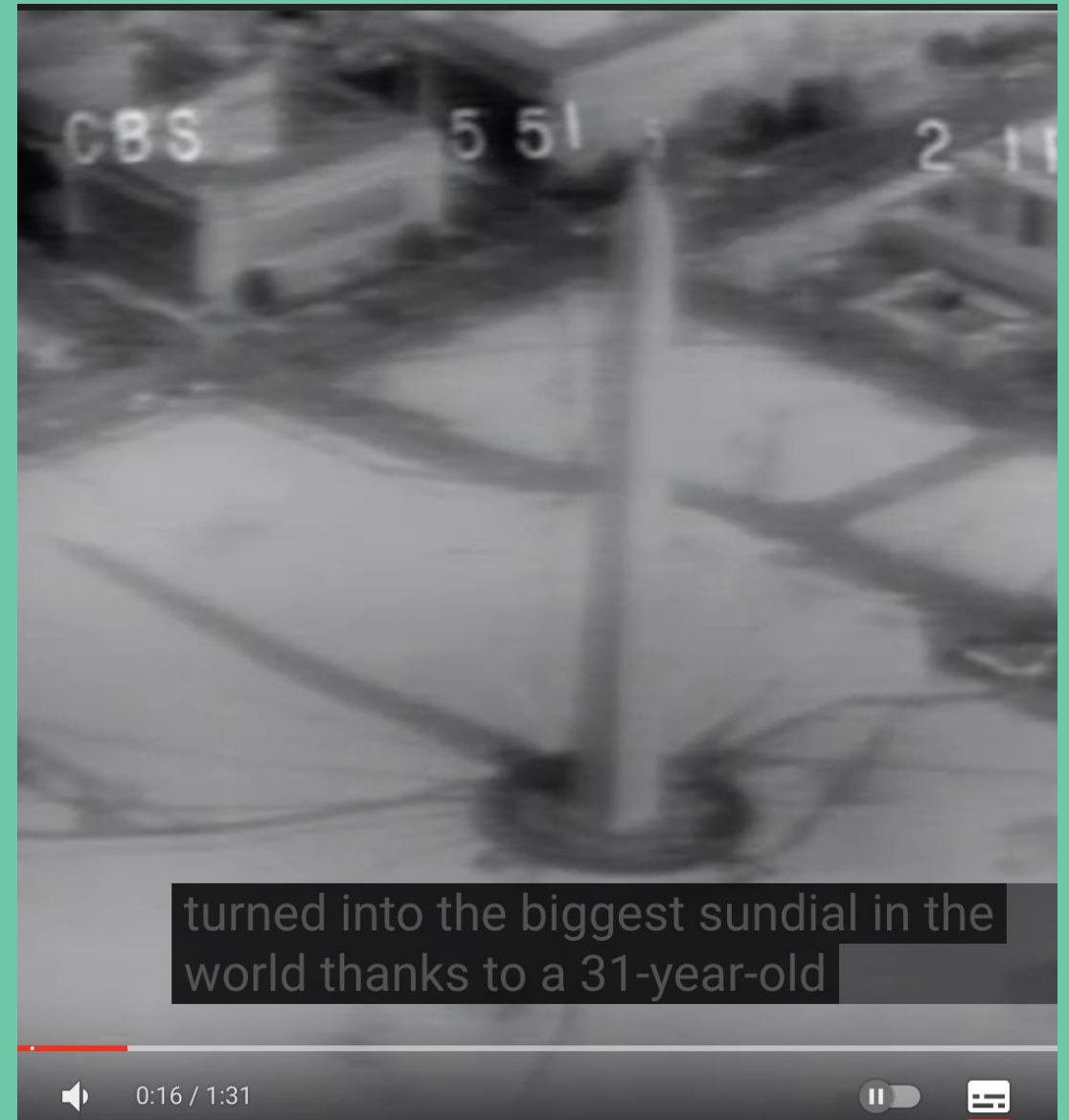
CBS 11 February 1974 transcript

The Washington Monument has turned into the biggest sundial in the world thanks to a 31-year-old Yugoslavian immigrant named Yuri Schwebler. Schwebler works as a newspaper layout editor, but what he is is an artist with an eye for the unusual. Not just the shape, but the shadow.

He got permission for his sundial in the snow three years ago and waited for the right combination of sun and snow and waited. The snow came last Friday. Saturday, Schwebler, a friend and two helpers with a snowplow from the National Park Service went to work, surveying, **raying** their straight lines out across the snow to plot the shadow.

Well, as an artist, one of the things that I do, and I think most artists do, traditionally have done, is point out things people don't see. And one day I realized I'd never seen the shadow of the Washington Monument because it's so huge. And then I looked for it, and I saw it, and it moved. And I was at the end of the shadow. It moves about four feet every minute, you know, so you can actually see the earth move or feel it move by watching that shadow. It just goes right along.

The project cost Schwebler just \$24. The rest of the city has had fun worth much more than that, watching the monument shadow tell the hour.



Alley to Which the Sun was Tied (WaPo 1990)

“The Washington Monument piece, finally executed after a snowfall in 1974, with hour lines cut through the snow, was the noblest of these—it had a grandeur of conception to fit the site. But less conspicuous public works were resonant too. 'Alley to Which the Sun Was Tied,' for instance, consisted simply of stenciled yellow markings on the macadam of a downtown alley (by now long gone), recording the exact location where a sliver of sunlight sliced between buildings on Aug. 23, 1971. As an art object it wasn't much, obviously, but as an idea it was gentle, vivid and life-enhancing. Both were back-to-basics pieces, sharp reminders that on a day-to-day basis we lose perspective and humility. Though in each case Schwebler was but pointing out a recurrent natural event, in an important sense he also was attempting precisely to measure the immeasurable.”

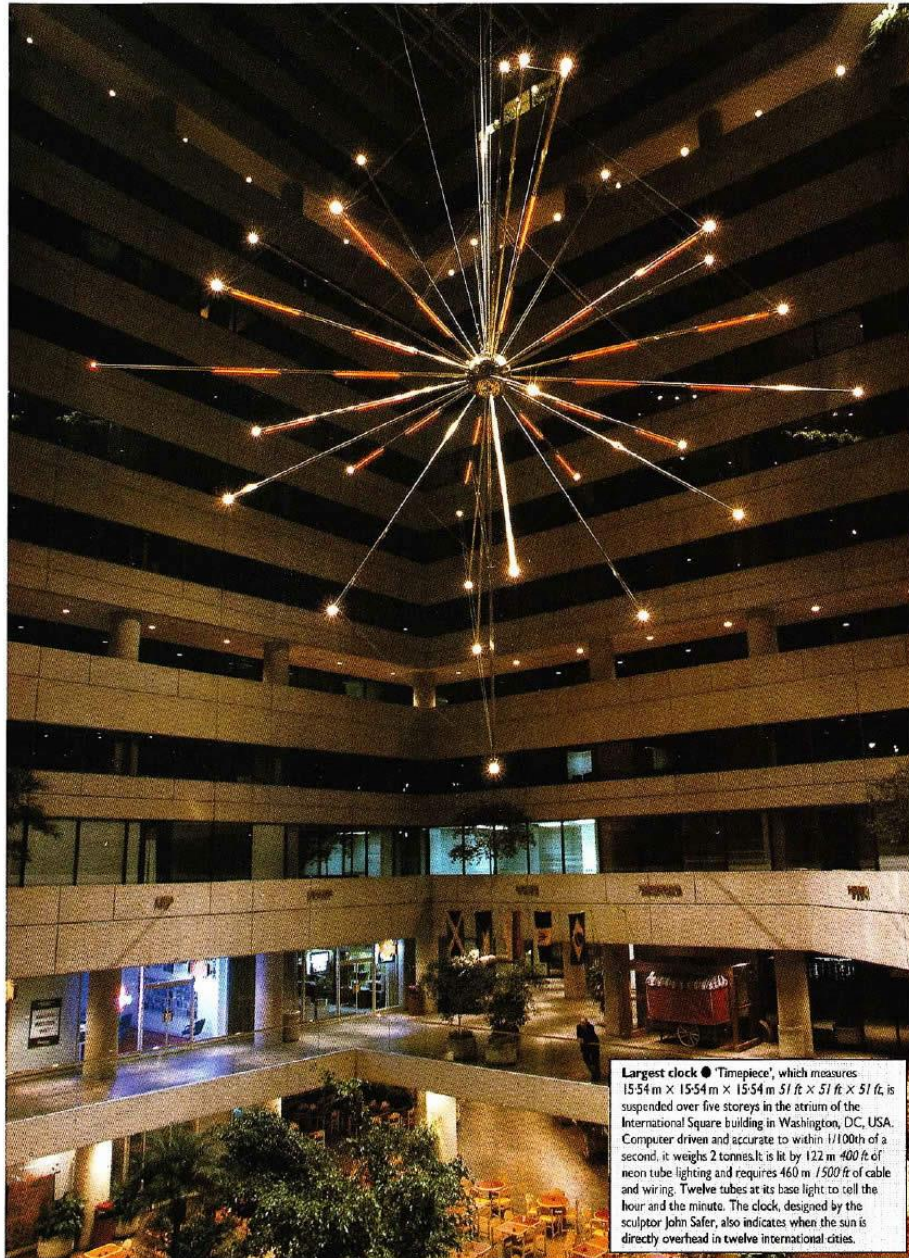
(266 to 274 degrees)



Sundials more generally

- Sanborn talked about Schwebler (21 November 1942 - 3 March 1990) in his 2009 6.5 hour interview; he incorrectly states Schwebler was Russian. <https://www.aaa.si.edu/collections/interviews/oral-history-interview-jim-sanborn-15700>
- One connection to Berlin would be turning the Berlin TV Tower into a sundial.
- Berlin also has Europe's largest sundial (since 1985) - Größte Sonnenuhr Europas in Kalendarplatz in Britzer Garden.
- This connects the themes of light and shadow (K1), magnetism (K2, lodestone and compass rose pointing east-northeast), rays in the snow, and time. At a stretch, connects to sundial in Egyptian Museum (K3) in Berlin too.
- Washington Monument inspired by Egyptomania
- Other Schwebler pieces “Alley To Which The Sun Was Tied, 23 Aug. 1971 5:49 to 6:41” and “Magnetic North” have similar themes.
 - “It’s the interaction of light or shadow on the earth”
<https://youtu.be/JPZsN7n1WA0>
 - What a coincidence!
- For example, a final puzzle could be finding a past or future date, time and place (an alley in Washington DC or Berlin?) when a shadow or ray of light points ENE





Largest clock ● "Timepiece", which measures 15.54 m × 15.54 m × 15.54 m 51 ft × 51 ft × 51 ft, is suspended over five storeys in the atrium of the International Square building in Washington, DC, USA. Computer driven and accurate to within 1/100th of a second, it weighs 2 tonnes. It is lit by 122 m 400 ft of neon tube lighting and requires 460 m 1500 ft of cable and wiring. Twelve tubes at its base light to tell the hour and the minute. The clock, designed by the sculptor John Safer, also indicates when the sun is directly overhead in twelve international cities.

John Safer's "Timepiece" (1985)

Timepiece did not spring fully formed from John's imagination, as had many of his other sculptures. Its genesis was gradual, beginning with a request in 1983 from Oliver Carr, Washington's premier real-estate developer and the owner of the International Square Building there, for John, as one of a group of artists, to submit a design for a sculpture to be hung in the atrium of the building.

...

John had contemplated making a sculpture that was also a clock, telling time in a changing light display.

...

not only the world's largest clock, but a sculpture of universal truth and import, one that clearly unites time, space, and light in a beautiful entity.

"Art in Flight: The Sculpture of John Safer", Walter Boyne (1991)

"Timepiece" is less than successful as a clock for one simple reason: It's hard to tell what it says. The Oliver Carr Company thoughtfully provides a brochure on how to read "Timepiece," but with instructions such as "At the beginning of the fifth minute, the vertical pattern of white tip lights goes out, and the red minute bar on the next horizontal bar goes on," you'll probably be late for wherever you're going by the time you figure out what time it is. – WaPo, John F. Kelly, 30 November 1989 (cf "Odd Couple" modern clock episode)

<https://youtu.be/1dvIWU1uWHM&t=116>

... in addition to keeping accurate time is an electronic sundial for 12 cities around the world – WaPo, Arts Beat, Elizabeth Lazarus, 27 October 1985

Tintin "Le Lotus Bleu" (1934) encryption and direction-finding



Summary

- The implied key for known K4 plaintext using the Kryptos alphabet (as with K1/K2) has a strong bias toward early letters of the Kryptos alphabet (**RDUM RIYWO YNKY ELYOIE CBAQK**)
- The bias is even stronger considering alternate letters (**RU RYO NY EYI CAK**)
- Possible explanations mapping Kryptos alphabet to ETAOIN SHRDLU (Linotype like) alphabets; or key letters based on differences between letters, not sums
- The possibility of a transposed English key (e.g. Seaman 2012) is still open, though the implied key would be unusual English
- Running key would be extremely difficult to solve at ~100 letters (Reddy and Knight 2012)
- Transposed running key virtually impossible to solve
- Plaintext autokey (PTAK) with transposition more likely, but PTAK already error prone and transposition makes it even worse. Searching books for transposed keytext seems unlikely
- John Le Carre referred indirectly to Kryptos in 1989
- Artistically, the work of Yuri Schwebler and John Safer (1970s, 1980s) inspired Sanborn and parallels it
- A review of Scheidt's work has a story about distillation cryptanalysis – a weird anecdote to raise
- A review of historical challenges that were eventually solved points in every direction – experts who turned challenges into unsolvable messes, unaesthetic ciphers, challenges which could not be solved without huge amounts of extra information, creators who vastly misestimated the difficulty of their construction, and “just right” ciphers