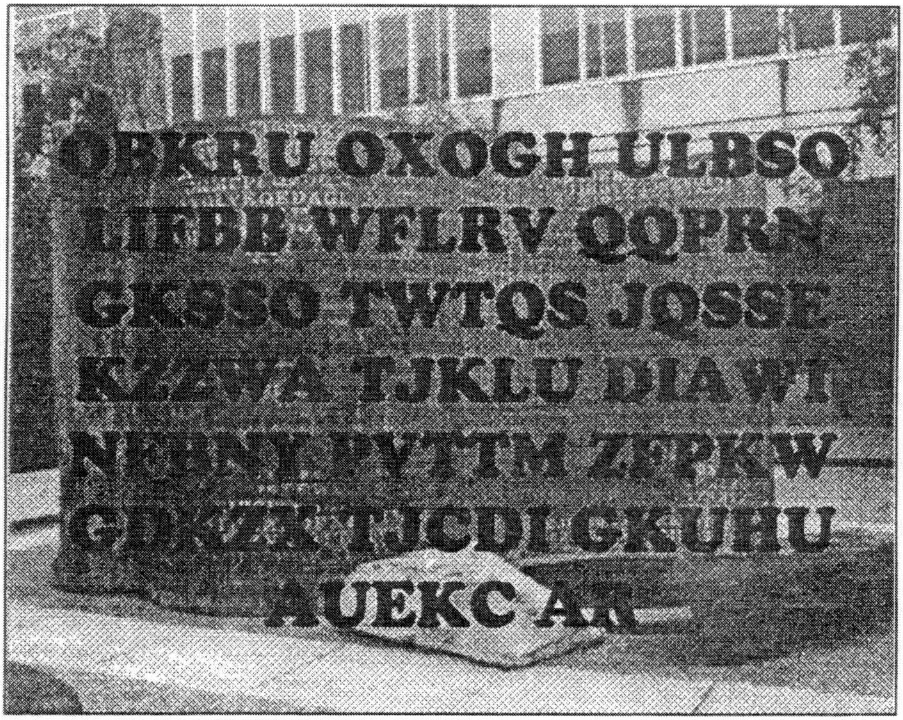
The Cryptogram

Journal of the
American Cryptogram Association, 3613 Piedmont Drive, Plano, TX 75075-6234



CONTENTS

The Kryptos Sculpture Cipher:

A Partial Solution

by SCRYER

In front of the CIA cafeteria stands a sculpture entitled "Kryptos" by James Sanborn. Articles in *The Cryptogram* in the ND91 (various authors) and MA92 (PHOENIX) describe it. The sculpture, in the form of an S, consists of two convex surfaces: one covered with a cipher and the other showing a Vigenère-like table based on the keyword KRYPTOS. Each branch of the S is composed of two plates of copper separated horizontally, with each letter cut completely through the copper plates. The sculpture includes a tall petrified tree on one side, a small circular pool, and a number of other nearby objects including some Morse code hidden in cracks among some jumbled slabs.

Edward M. Scheidt, former chairman of the CIA's Cryptographic Center, chose the types of ciphers used for the encryption. The sculptor encrypted the plaintext. Since its dedication in October 1990, the plaintext has been known only to the sculptor, the cryptographer, and a close-mouthed handful of others. The solutions or the keys were given to the Director of Central Intelligence (then William Webster) in a sealed envelope. It has been passed on to subsequent DCI's.

I first looked at the cipher in 1992 when PHOENIX's article was published, but set it aside after a few days. I looked at again once or twice over the intervening years, and picked up again for a harder look on 7 June 1999 when the topic came up in the Usenet group sci.crypt. Over the course of the next four evenings, I decrypted three separate messages. This article deals with the decryption of all but the last 97 characters of the Kryptos cipher.

The ciphertext of the two "pages" of the sculpture, was transcribed by Doug Gwyn from the MA92 copy by PHOENIX, corrected by Doug's personal observations of the statue, and posted on 1 September 1992 to an Internet mailing list.

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

ENDYAHROHNLSRHEOCPTEOIBIDYSHNAIA
CHTNREYULDSLLSLLNOHSNOSMRWXMNE
TPRNGATIHNRARPESLNNELEBLPIIACAE
WMTWNDITEENRAHCTENEUDRETNHAEOE
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR
EIFTBRSPAMHHEWENATAMATEGYEERLB
TEEFOASFIOTUETUAEOTOARMAEERTNRTI
BSEDDNIAAHTTMSTEWPIEROAGRIEWFEB
AECTDDHILCEIHSITEGOEAOSD@RYDLORIT
RKLMLEHAGTDHARDPNEOHMGFMFEUHE
ECDMRIPFEIMEHNLSSTTRTVDOHW?OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```

In MA92 PHOENIX suggested that the four question marks represented the boundaries between separately-enciphered sections. Accepting this idea provisionally another separation was added between the two pages (separate plates of copper) because of the transposition-like frequencies at the beginning of the second page.

I examined the statistics of each assumed section of the first page using Kasiski and Index of Coincidence (IC) to test for polyalphabeticity. The first section (**EMUFP** to **GWHKK**) was problematical. The period appears to be 5, 10 or 13, but there are two 5-letter repeats, **VJYQT** and **GWHKK,** at separations of 20 and 16, respectively. This would seem to rule out a simple polyalphabetic cipher: the repetitions are so long that they must represent actual plaintext repetitions, and yet the implied period 4 does not agree with suggestions from the IC.

Moving on to the second section (**DQMCP** to **DDUVH**) things look better. Period 8 is strongly suggested, and there are two three-character repeats.

The third section (**DWKBF** to **GGTEZ**) shows a possible period 8 or 9, but there are no repetitions of note.

The fourth section (**FKZBS** to **LAETG**, the end of the page) is more promising yet. Period 4 or 8 is strongly suggested, and there is a 5-letter repetition at an offset of 72, as well as two 3-letter repetitions at compatible offsets. A decision was made to begin work on the fourth section first.

Attempts to solve it as each of our simple polyalphabetic types (Vigenère, Beaufort, Variant Beaufort, and Porta) in turn were tried with no success. Could this cipher be a Quagmire? A Quagmire without a crib is difficult with this little material, but fortunately Sanborn gave us a clue. The other S-branch of the sculpture is a Quagmire table (Vigenère's original design, before it was simplified to direct offset alphabets) using KRYPTOS as the shifted keyword. A Quagmire I, II, or III with a known alphabet keyword is no more difficult than a Vigenère, and so can be solved using the same methods. Trying to obtain a solution as a Quag I and a Quag II was unsuccessful. However, when Quag III using KRYPTOS as the alphabet keyword was tried, the solution popped out of my shotgun hillclimbing program immediately:

```
      FKZBSFDQVGOGIPUFXHHDRKF
      onlywwthiswashislastmes

FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ
sagexthirtyeightdegreesfiftyse

ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE
venminutessixpointfivesecondsno

DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP
rthseventysevendegreeseightminu

DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG
tesfortyfoursecondswestidbyrows
```

The keyword found was AABSCISS. However, the word ABSCISSA did not start at the beginning. Extending this solution back through the cipher, I discovered that it worked for all but the first two lines. The question marks turned out to be textual rather than separators. They appeared whenever the text asked a question. Here is the plaintext to the (newly separated) second section:

> 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. Keys: KRYPTOS, ABSCISSA

The latitude-longitude coordinates correspond to a point at CIA Headquarters in Langley, VA — perhaps the site of the sculpture itself. I have no explanation of the "ID by rows," but the tone of the whole passage sounds to me rather like one of Nikola Tesla's experiments.

Only two lines of unknown ciphertext remained on the first page:

```
EMUFPHZLRFAXYUSDJKZLDKRNSHGNFIVJ
YQTQUXQBQVYUVLLTREVJYQTMKYRDMFD
```

In isolation, this section now clearly shows up as period 10, with the **VJYQT** now no longer contradicted by other period indications. I tried it as a Quag III using KRYPTOS as the alphabet key, and again my shotgun hill-climbing program solved the Vigenère-equivalent cipher immediately. Its 63 characters, or just over 6 periods, are normally enough for a quick solution, despite the ACA guideline of 12-15 cycles.

Here is the plaintext for the first section:

Between subtle shading
and the absence of light
lies the nuance of iqlusion.
Keys: KRYPTOS, PALIMPSEST.

The typos in these two sections (iqlusion and undergruund) are cut into the copper. It has been pointed out that they may have some deeper meaning. The replaced letters are a Q in the first word and a U in the second. Whenever a QU turns up in the same thought, we have a right to be suspicious; but if there is a deeper meaning it is not yet obvious. In addition, the replaced ciphertext characters are **K** and **R** (replacing **X** and **E**), the first letters of KRYPTOS.

The next section of text, up until the question mark, is clearly a transposition: the monoliteral frequencies are right on the textbook marks, including the vowel/consonant ratio. Where does it end? Many of my tests assumed that it ended at the question mark. It is a nice round number (336, which factors into 2*2*2*2*3*7), and the letters after the question mark on that line, **OBKR**, include two low-frequency letters, in keeping with the low-frequency-letter-rich final lines. I also tried many tests including the **OBKR** on that line (since the first two sections broke at the end of a line), for 340 characters, and more tests including the "?", for 337 or 341 characters — a question mark may be permuted as readily as a letter.

Many different kinds of transpositions were tried starting with Complete and Incomplete Columnar for periods as wide as could be handled, Myszkowski, Railfence, a set of 4x4 Grilles like one in a recent Analyst's Corner problem, and Route Transposition. None of them gave any satisfaction.

Two evenings were then spent working with my double transposition solver, another module in the shotgun hillclimbing program. Double transposition with one key used twice was tried and nothing was seen of interest up to about period 16, the highest it can handle in reasonable time.

However, after some work with two-key double transpositions, some provocative results started to be seen. If the first transposition had to have a period of 6, with the second unconstrained, the program picked the first key as FEDCBA and the second a mixed 5-letter key. That is, the columns of the first permutation were to be taken off in reverse order. When the first period was forced to be 7, it gave GFEDCBA, again in reverse order and with a mixed second key. With the first period forced to 8, it chose ABCDEFGH — eight columns taken off in forward order.

The resulting "plaintext" in each case appeared to be garbage, but it was finding enough tetragraphs to determine that this order was preferred, even though nothing useful could be seen. For example, its preferred result with first key of 8 and second of 9 was with keys ABCDEFGH and EGCIBDAFH, yielding the "plaintext":

```
ouseeanythingqomthemistxcanyithinemergedfrailsof
theroomwutpresentlydetlametoflickerbmbercausedth
efpingfromthechanthehotairescandleandpeerediiins
ertedthecatheholealittlendthenwideningefthandcor
neraachintheupperlsimadeatinybrehtremblinghandyw
asremovedwitartofthedoorwaberedthelowerpebristha
tencumainsofpassagedlyslowlytheremslowlydesparat
```

There are provocative segments in here ("eandesparat" and "wideareholything"), however nothing that appears undeniably on the right track.

Unfortunately having the correct first permutation does not help much in a double transposition, since the second one needs to be unwound first on decryption. I tried instead forcing it to hold the second permutation at period 8, and again a regularity was obtained with the permutation HGFEDCBA

— the columns in reverse order. The result was still garbage, but the transformation was one that could be unwound easily. This transposition was removed "by hand" and the process was started again with different transposition methods. This time the columnar transposition gave the following result with period 14:

```
ouseeanythingqomthemistxcanyithinemergedfrailsof
theroomwutpresentlydetlametoflickerbmbercausedth
efpingfromthechanthehotairescandleandpeerediiins
ertedthecatheholealittlendthenwideningefthandcor
neraachintheupperlsimadeatinybrehtremblinghandyw
asremovedwitartofthedoorwaberedthelowerpebristha
tencumainsofpassagedlyslowlytheremslowlydesparat
```

This has many excellent fragments, and can be straightened out almost by eye. Once the transformation has been done, it turns out to be simple. It consists of three route transpositions in different block sizes each consisting of writing it into rows of 14, 24, and 8 letters, then taking it off by columns in reverse order.

The plaintext is:

> 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
>
> Keys: three route transpositions

This is an adaptation of Howard Carter's discovery of King Tutankhamun's tomb in 1922. Again, the misspelling of "desperately" is in the sculpture itself. If one is reading things into the errors, the replaced character is A, extending the error letters to QUA (followed by an omitted E). Is there another message to be found?

The final question in this section was asked by Lord Carnarvon. Carter, stunned by what he saw, was able to reply only "Yes, wonderful things."

After finishing these three parts, I contacted the CIA to let them know I'd solved them and was told that a CIA analyst had solved the same amount a year earlier after about 400 hours of effort, but had not made his solution public. When I received more details, I found that he, David Stein, was also not the first to solve it. The NSA public affairs office told me a team of three NSA analysts spent most of 1992 working on KRYPTOS in their free time, and near the end of the year had solved the same three parts. There is a KRYPTOS Society at NSA that produces newsletters, sponsors an annual Christmas Quiz, and has a UK branch.

We're now left with at least two more mysteries. One is the decryption of the final 97 characters, and the second is what it all means. The sculptor, Jim Sanborn, has indicated that there is a puzzle within a puzzle which we will not be able to start solving until we've solved the final part. This time we're fairly confident that nobody else has solved it first.

Have at it, Krewe!

```
                            OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR
```