Examples of Solving *Cm* Cons*

Solving P-2 from Sample *Cm* Patristocrat

* “*Cm* Cons” means “cipher constructions in *The Cryptogram*” -- the bi-monthly publication for members of the American Cryptogram Association (ACA) -- www.cryptogram.org

Examples of Solving

This series shows specific examples of solving ACA ciphers. It tries to give successive hints of what to look at, then follows through by using each hint, building to the solution.

Try to solve the cipher on your own, using as many hints as you need, or just read along.

Please report errors or send suggestions to nudge@cryptogram.org

References

- The ACA and You, Ch. 4, How to Solve a Problem in *The Cryptogram*.
- The ACA and You, Ch. 8, ACA Guidelines (for keyword alphabets).
- Beginner's Guide to the American Cryptogram Association, by CODE PENGUIN.

What is simple substitution?

In a simple substitution cipher, plaintext letters are replaced according to a cipher alphabet. No letter replaces itself. There are four standard arrangements of keyed alphabets.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ  K1   GTD CDEFGHI
xzkeywordabcfghijlmnpqstuv       one keyword

XZKEYWORDABCFGHIJLMNPQSTUV  K2   HGY BYUSILE
abcdefghijklmnopqrstuvwxyz       one keyword

XZKEYWORDABCFGHIJLMNPQSTUV  K3   DQW YWORDAB
uvxzkeywordabcfghijlmnpqst       one keyword

XZKEYWORDABCFGHIJLMNPQSTUV  K4   CZQ MBEZQTGU
vwxyzalphbetcdfgijkmnoqrsu       two keywords
```

Getting started on a Patristocrat

- A Patristocrat is a simple substitution cipher without word divisions. Plaintext letters are replaced according to a cipher alphabet.
- Look for common letters (E,T,A,O,N,R,I,S), common digrams (TH, AN, ER…) or trigrams (THE, YOU...)
- There may be a crib word that appears in the message. Use letter frequencies or patterns to help locate its possible positions.
- Guess a word. See how that affects other words.
- Build a reference alphabet to look for patterns/keywords.

Solving P-2 from Sample *Cm*

P-2. K2 [86/19] An eternal game (NSAJSYJI) BOATTAIL
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.

What does the first line tell us?

Cipher ID: P-2.

Title: “An eternal game.” A clue to plaintext content?

Key type is K2 -- watch for a keyword in the ciphertext alphabet.

Cipher length is 81 letters. 19 different letters are used.

Crib word (in Caesar cipher) is NSAJSYJI – a pattern word!

Created by ACA member BOATTAIL.

Solving P-2 from Sample *Cm*

The crib was given in Caesar cipher (in case one might want to try solving without a hint). We will use the crib word, so we first need to solve the Caesar cipher.

```
Crib word: NSAJSYJI
```

Solving P-2 from Sample *Cm*

The crib was given in Caesar cipher (in case one might want to try solving without a hint). We will use the crib word, so we first need to solve the Caesar cipher.

Caesar cipher shifts all letters the same amount. Try shifting the letters either forward or backward until they make sense.

	Forward	Backward
Crib word: NSAJSYJI	OTBKTZKJ	MRZIRXIH
	PUCLUALK	LQYHQWHG

Solving P-2 from Sample *Cm*

The crib was given in Caesar cipher (in case one might want to try solving without a hint). We will use the crib word, so we first need to solve the Caesar cipher.

Caesar cipher shifts all letters the same amount. Try shifting the letters either forward or backward until they make sense.

```
                      Forward   Backward
Crib word: NSAJSYJI   OTBKTZKJ  MRZIRXIH
                      PUCLUALK  LQYHQWHG
                      QVDMVBML  KPXGPVGF
                      RWENWCNM  JOWFOUFE
                      SXFOXDON  INVENTED(***) Crib word: invented
```

Solving P-2 from Sample *Cm*

The crib word, “invented,” has a repeated N and E. The crib might be located wherever ciphertext letters repeat similarly.

Where might the crib be placed?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
----- ----- ----- ----- ----- ----- ----- ----- -----
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
----- ----- ----- ----- ----- ----- ----- ----- -.


   --------------------------   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

Where might the crib be placed? There seems to be one place.

`MUEIUYIH` matches the pattern of `INVENTED`.

Fill those in. Look for possible words or K2 alphabet clues.

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
--n-- ----- -inve nted- ----- -e-d- ----i nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
-i-t- t--ee ei--t --i-- i-n-- -ie-- -ve-e en--- d.

   ---HI---M----U-----Y-E----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

The K2 alphabet suggests that “`JKL`” might stand for “`fgh`.” The words NINETEEN THIRTY THREE suggest themselves, and that is consistent with the K2 alphabet guess.
Let’s try those.

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
--n-- --y-- -inve nted- y-h-r -e-d- rr--i nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight y-i-- i-n-- -ie-h -ve-e en--- d.

   ---HIJKLM----U---O-Y-E--T-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

In the second line, just after “eighty”, is SMRRMVU, with M=i and U=n. What might this be? Does the K2 alphabet give any clue?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
--n-- --y-- -inve nted- y-h-r -e-d- rr--i nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight y-i-- i-n-- -ie-h -ve-e en--- d.

   ---HIJKLM----U---O-Y-E--T-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

In the second line, just after “eighty”, is SMRRMVU, with M=i and U=n.

Maybe V=o? And maybe R=l, and S=m? Giving the word MILLION? Let’s try that.

What’s next? What’s at the beginning of the cipher?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
mono- oly-- -inve nted- y-h-r le-d- rro-i nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight ymill ion-o -ie-h -ve-e en-ol d.

    ---HIJKLM--RSUV--O-Y-E--T-   CIPHERTEXT (K2)
    abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

V=o, so maybe W=p? And that would give us MONOPOLY as the first word. Sounds like a good guess.

So what might come between MONOPOLY and INVENTED?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
monop oly-- -inve nted- y-h-r le-d- rro-i nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight ymill ion-o pie-h -ve-e en-ol d.

   ---HIJKLM--RSUVW-O-Y-E--T-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

It looks like it could start MONOPOLY WAS INVENTED BY…
Let’s try that.

What could the final letter be? And how does the K2 alphabet finish up?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
monop olywa sinve ntedb y-har lesda rrowi nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight ymill ion-o piesh avebe ensol d.

   BC-HIJKLM--RSUVW-OXY-EN-T-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

F=c completes the plaintext.

And how does the K2 alphabet finish up?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
monop olywa sinve ntedb ychar lesda rrowi nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight ymill ionco piesh avebe ensol d.

   BCFHIJKLM--RSUVW-OXY-EN-T-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

And how does the K2 alphabet finish up?
PQ are the missing letters between M & R.
Z probably comes right after W.
The remaining letters to be placed are: A, D, G. Can you find the keyword?

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
monop olywa sinve ntedb ychar lesda rrowi nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight ymill ionco piesh avebe ensol d.

   BCFHIJKLMPQRSUVWZOXY-EN-T-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving P-2 from Sample *Cm*

Looks like OXYGENATED could be the keyword.

Record the solution so you could later submit it for credit

P-2 OXYGENATED monopoly was invented by charles darrow in

```
SVUVW VRTNB XMUEI UYIHC TFLBO RIXHB OOVNM UUMUI YIIUY
monop olywa sinve ntedb ychar lesda rrowi nnine teent
LMOYT YLOII IMKLY TSMRR MVUFV WMIXL BEICI IUXVR H.
hirty three eight ymill ionco piesh avebe ensol d.

   BCFHIJKLMPQRSUVWZOXYGENATD   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

AMERICAN CRYPTOGRAM ASSOCIATION

Cryptograms "The Aristocrat of Puzzles"

Thank you. Try another. Try the ACA!

The American Cryptogram Association (ACA) is a non-profit organization dedicated to promoting the hobby and art of cryptanalysis – learning to break ciphers. And we write ciphers, too. Our Sample Issue and all its solution tutorials are available on our website:

www.cryptogram.org/resource-area/sample-issue-cryptogram/