Examples of Solving *Cm* Cons*

Solving P-1 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-1 from Sample *Cm*

```
P-1. K1 [81/19] Inherited wisdom. (KFYMJW) ALCHEMYST
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
```

What does the first line tell us?

Cipher ID: P-1.

Title: “Inherited wisdom.” A clue to plaintext content?

Key type is K1 -- watch for a keyword in the plaintext alphabet.

Length is 81 letters, 19 letters of that alphabet are used.

Crib word (in Caesar) is KFYMJW. No repeated letters.

Created by ACA member ALCHEMYST.

Solving P-1 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: KFYMJW
```

Solving P-1 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: KFYMJW   LGZNKX    JEXLIV
                    MHAOLY    IDWKHU
```

Solving P-1 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: KFYMJW  LGZNKX    JEXLIV
                   MHAOLY    IDWKHU
                   NIBPMZ    HCVJGT
                   OJCQNA    GBUIFS
                   PKDROB    FATHER(***) Crib word: father
```

Solving P-1 from Sample *Cm*

The crib word has no repeated letters. Count all the cipher letters to see which are most frequent, looking also for repeated digrams or trigrams. This might give a clue for where to place the crib.

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
----- ----- ----- ----- ----- ----- ----- ----- -----
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
----- ----- ----- ----- ----- ----- ----- -.


   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   --------------------------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

Letter frequencies, also repeated digrams/trigrams.

D	O	F	I	H	P	E	G	A	S	T	U	Y	J	N	W	B	M	R	(CKLQVXZ)
10	10	8	8	7	6	4	4	3	3	3	3	3	2	2	2	1	1	1	0

HO	OF	DI	DH	DS	FD	OD	OP	PI	TD	UG	HOF
5	4	3	2	2	2	2	2	2	2	2	3

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
----- ----- ----- ----- ----- ----- ----- ----- -----
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
----- ----- ----- ----- ----- ----- ----- -.


   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   --------------------------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

The most frequent digram in English: TH;   Trigram: THE

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
----- ----- ----- ----- ----- ----- ----- ----- -----
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
----- ----- ----- ----- ----- ----- ----- -.


  ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
  --------------------------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

The most frequent digram in English: TH; Trigram: THE
HO appears five times, and HOF occurs three times.
Let’s guess that HOF represents THE.

After that is in place, can we spot where to fit FATHER?

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the t--e- ----e ----e -th-t ----e h---- the-- -----
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- ----- -h--- ----h -th-- --he- ----- -.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   -----e-t------h-----------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

The most frequent digram in English: TH;   Trigram: THE
HO appears five times, and HOF occurs three times.
Let’s guess that HOF represents THE.

Now, can we find a place for the crib, FATHER?

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the t--e- ----e ----e -th-t ----e h---- the-- -----
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- ----- -h--- ----h -th-- --he- ----- -.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   -----e-t------h-----------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

There is only one place where FATHER will fit.

“--eh--father” suggests a word to precede FATHER…

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the t--ea -a-re a---e -that -a--e h--fa ther- a-r--
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- --a-- -ha-a ----h -th-- --he- --r-- -.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---are-t----f-h-----------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

The EH preceding FATHER suggests HIS FATHER. Try it!
This also creates HAS A in the second line.
P=i fits nicely in the K1 plaintext alphabet.

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the ti-ea -a-re a-i-e sthat -a--e hisfa ther- asri-
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- --a-- -hasa s---h -thi- --hei s-r-- -.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---are-ts---f-hi----------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

What else does the K1 plaintext alphabet suggest?

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the ti-ea -a-re a-i-e sthat -a--e hisfa ther- asri-
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- --a-- -hasa s---h -thi- --hei s-r-- -.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---are-ts---f-hi----------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

What else does the K1 plaintext alphabet suggest?
"F*HI" suggests G might fill that gap. Try N=g.

Now we see: HIS FATHER *AS RIGHT HE. What word?

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the ti-ea -a-re a-i-e sthat -a--e hisfa ther- asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- --a-- -hasa s---h -thi- -shei s-r-- g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---are-ts---fghi----------   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

W would give us HIS FATHER WAS RIGHT HE… Try Y=w.

At the beginning, THETI*EA suggests a letter that could be added to the K1 plaintext alphabet. And perhaps a few more…

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the ti-ea -a-re a-i-e sthat -a--e hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- --a-- -hasa s--wh -thi- -shei swr-- g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---are-ts---fghi--------w-   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

M would give us THE TIME A… Try T=m.
The K1 alphabet also suggests QRS=jkl. Try those, too.

Could the K1 alphabet be extended from W?

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
--the timea ma-re ali-e sthat ma--e hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- --all -hasa s--wh -thi- kshei swr-- g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---are-ts---fghijklm----w-   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

The K1 alphabet might contain ZAB=xyz. Try those.

Sight reading now might allows us to fill in some words…

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
-ythe timea ma-re alize sthat may-e hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
hthe- s-all yhasa s--wh -thi- kshei swr-- g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   yz-are-ts---fghijklm----wx   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

Sight reading now suggests:

- the first word looks like BY
- the fifth word looks like MAN
- the second word on second line looks like USUALLY

Try J=b, G=n, W=u (and X=v, too).

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
bythe timea manre alize sthat maybe hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
htheu suall yhasa s-nwh -thin kshei swr-n g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   yz-arentsb--fghijklm--uvwx   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

Sight reading suggests the final letter is U=o, giving words SON, WHO, and WRONG.

Try filling in the rest of the K1 alphabet to discover the key.

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
bythe timea manre alize sthat maybe hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
htheu suall yhasa sonwh othin kshei swron g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   yz-arentsb--fghijklmo-uvwx   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

Ciphertext V must be either “p” or “q” (“rst” are already used).
Ciphertext K, L suggest “c”, “d” to fill an alphabetic gap.

The keyword will start with whatever was not used for V…

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
bythe timea manre alize sthat maybe hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
htheu suall yhasa sonwh othin kshei swron g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   yz-arentsb--fghijklmo-uvwx   plaintext  (K1)
```

Solving P-1 from Sample *Cm*

After filling in everything, the keyword is PARENTS.

Record the solution so you could later submit it for credit

```
P-1 PARENTS by the time a man realizes that maybe his
```

```
JAHOF HPTFD TDGEF DSPBF IHODH TDAJF OPIMD HOFEY DIEPN
bythe timea manre alize sthat maybe hisfa therw asrig
OHOFW IWDSS AODID IUGYO UHOPG RIOFP IYEUG N.
htheu suall yhasa sonwh othin kshei swron g.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   yzparentsbcdfghijklmoquvwx   plaintext  (K1)
```

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/