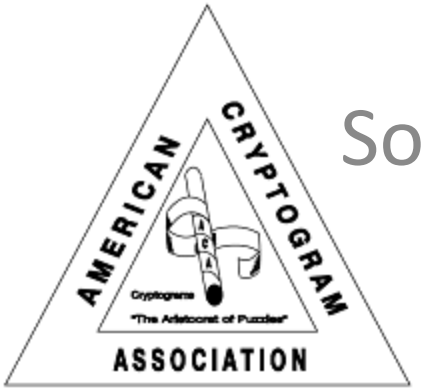
Examples of Solving *Cm* Cons*



Solving the Cover from Sample *Cm* Ornamental Aristocrat

* "*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.

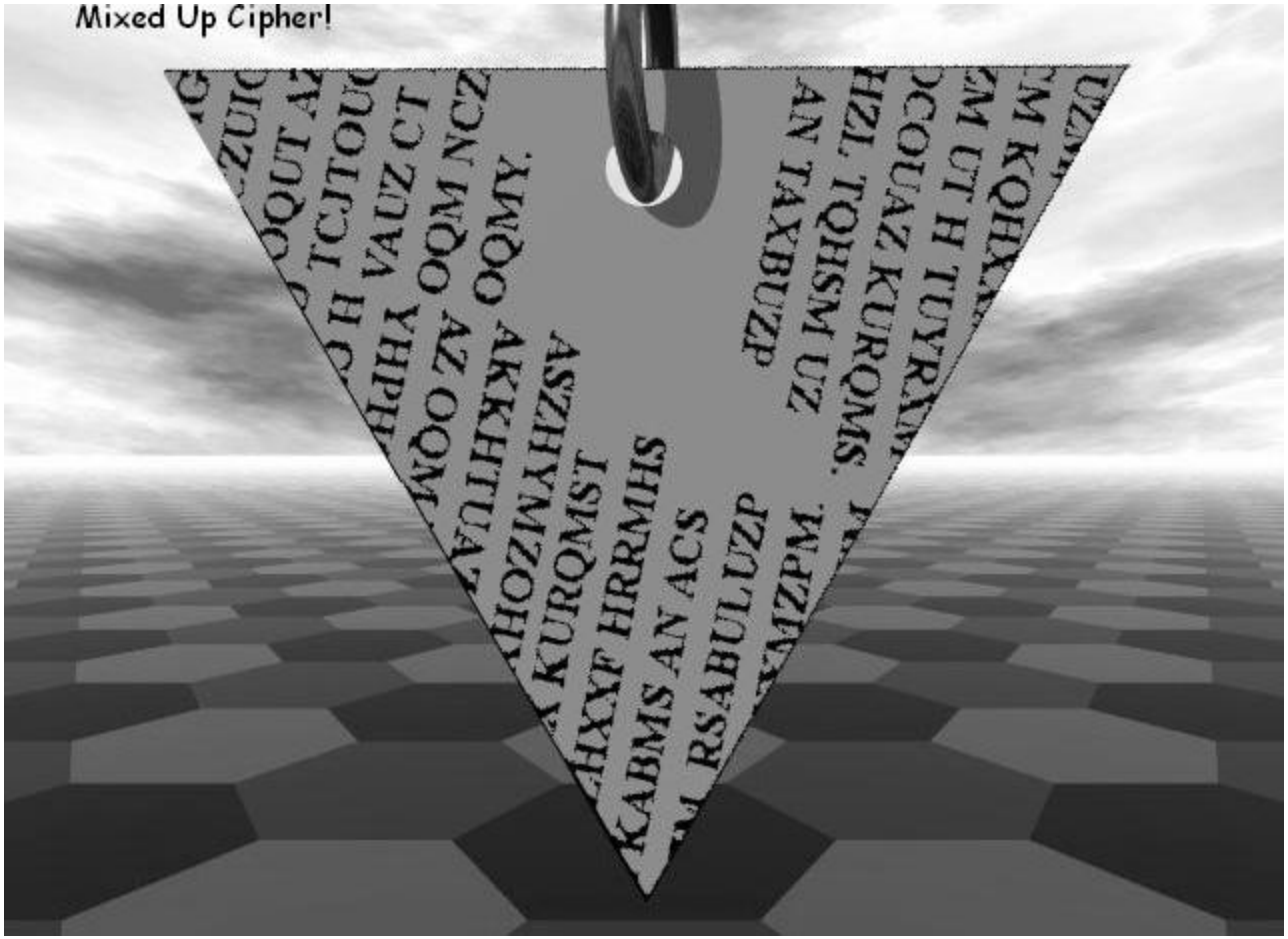
```
ABCDEFGHIJKLMNOPQRSTUVWXYZ  K1   GTD CDEFGHI
xzkeywordabcfghijlmnpqstuv       one keyword

XZKEYWORDABCFGHIJLMNPQSTUV  K2   HGY BYUSILE
abcdefghijklmnopqrstuvwxyz       one keyword

XZKEYWORDABCFGHIJLMNPQSTUV  K3   DQW YWORDAB
uvxzkeywordabcfghijlmnpqst       one keyword

XZKEYWORDABCFGHIJLMNPQSTUV  K4   CZQ MBEZQTGU
vwxyzalphbetcdfgijkmnoqrsu       two keywords
```

Getting started on an Aristocrat

- An Aristocrat is a simple substitution cipher. Plaintext letters are replaced according to a cipher alphabet. The cipher shows the individual words.
- Look for common words like THE, YOU, I, A, etc. Look for pattern words like PEOPLE, THAT, SAYS, ELSE, etc..
- Look for apostrophe use, as in I'M, I'D, IT'S, CAN'T, WON'T, SHOULDN'T, or *BILL'S, WORLD'S, etc.
- Guess a word. See how that affects other words.
- Build a reference alphabet to spot patterns/keywords.
- An asterisk (*) precedes a capitalized word.

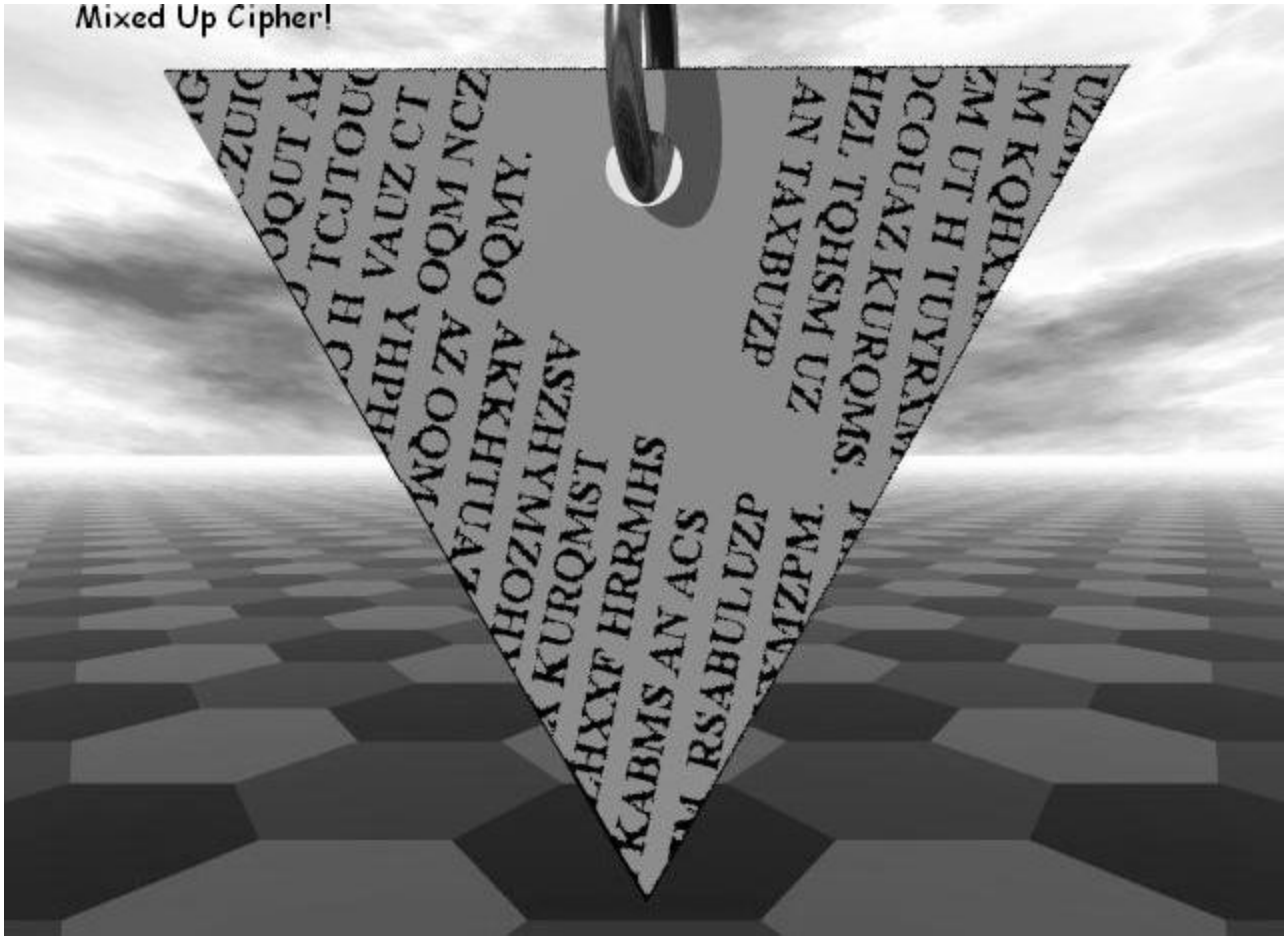
Solving Cover from Sample *Cm*

```
Cover. Mixed Up Cipher!  BION
```



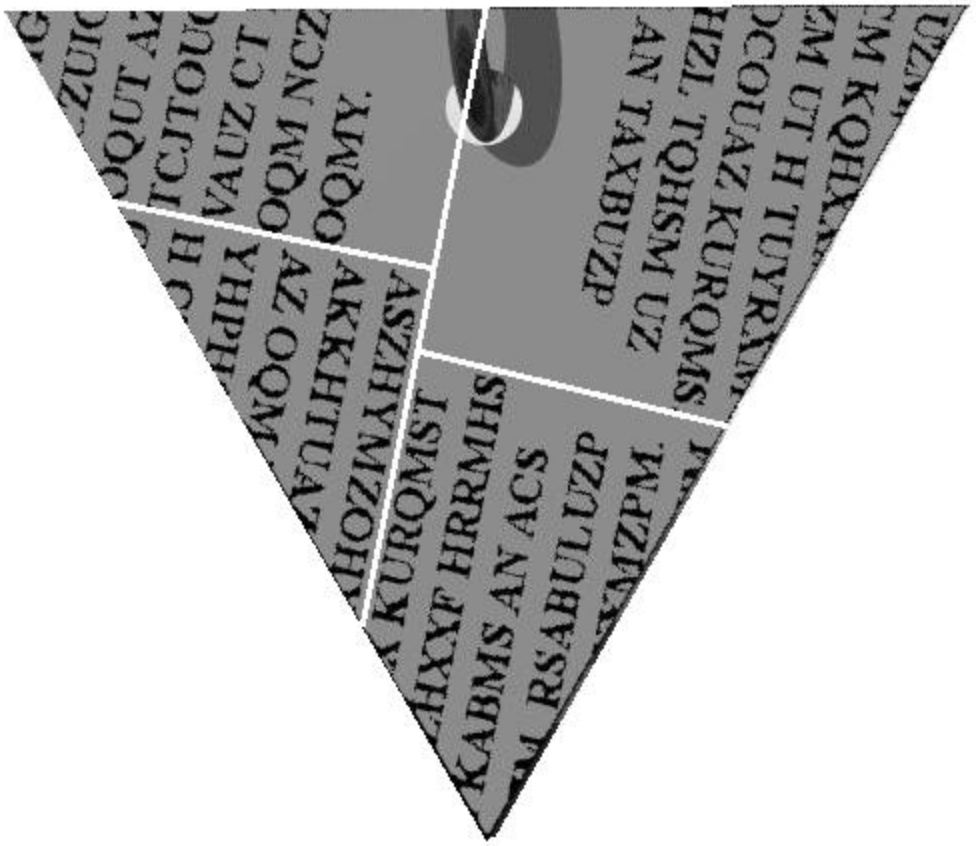
Solving Cover from Sample *Cm*

How many different orientations of text can you find?



Solving Cover from Sample *Cm*

Seems like four distinct regions of ciphertext in the image.



Solving Cover from Sample *Cm*

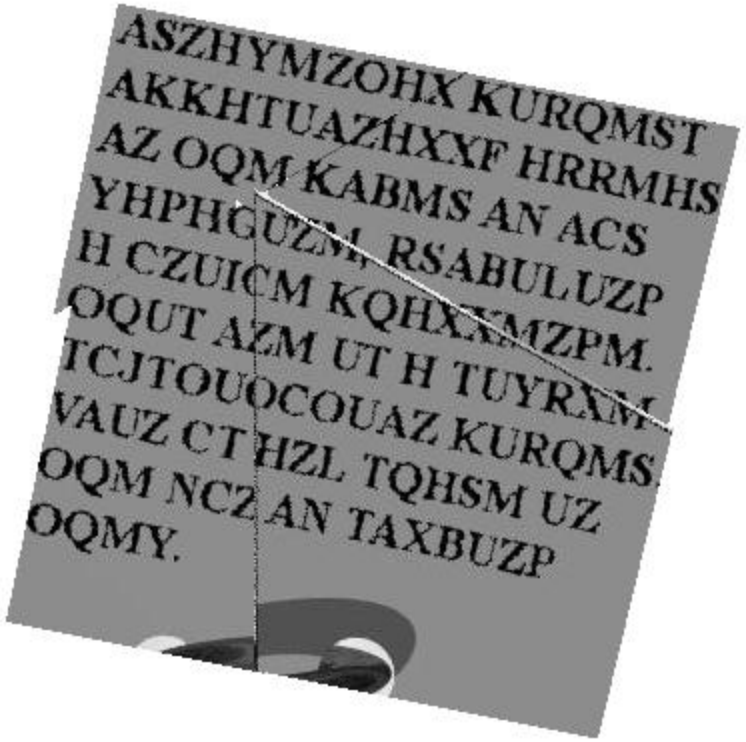
Print the image and cut out the sections along right angles.

Solving Cover from Sample *Cm*

Rotate the sections and realign to form rough square.

Solving Cover from Sample *Cm*

Align them more carefully and read the ciphertext. There appear to be individual words and punctuation!



Solving Cover from Sample *Cm*

The ciphertext has been copied below. How to start?
Frequent words or pattern words: THE, YOU, THAT, A, I

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
---------- ------- ----------- ------ -- --- ----- -- ---
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
-------- --------- - ------ ---------.  ---- --- -- - ------
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
------------ ------ ---- -- --- ----- -- --- --- -- ------- ----.

   --------------------------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

H stands out.
OQM, OQUT, OQMY stand out.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
---------- ------- ----------- ------ -- --- ----- -- ---
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
-------- --------- - ------ ---------.  ---- --- -- - ------
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
------------ ------ ---- -- --- ----- -- --- --- -- ------- ----.

   --------------------------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

H and HZL suggest H=a.
OQM, OQMY could be YOU, YOUR, but OQUT, UT are odd.
OQM, OQMY, OQUT, UT could be THE, THEM, THIS, IS.
Try O=t, Q=h, M=e, Y=m, U=i, T=s.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
---ame-ta- -i-he-s ---asi--a--- a--ea- -- the ---e- -- ---
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-i-e ----i-i-- a --i--e -ha--e--e.  this --e is a sim--e
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
s--stit-ti-- -i-he- --i- -s a-- sha-e i- the --- -- s---i-- them.

   H---M--QU---Y-----TO------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

Can the alphabet give any clues of what to try next? What might X and Z represent?

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
---ame-ta- -i-he-s ---asi--a--- a--ea- -- the ---e- -- ---
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-i-e ----i-i-- a --i--e -ha--e--e.  this --e is a sim--e
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
s--stit-ti-- -i-he- --i- -s a-- sha-e i- the --- -- s---i-- them.

   H---M--QU---Y-----TO------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

H..M..QU..Y seem to be in order. If Y=m, then maybe X=l and Z=n. Try X=l, Z=n.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
--namental -i-he-s ---asi-nall- a--ea- -n the ---e- -- ---
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine ----i-in- a -ni--e -hallen-e.  this -ne is a sim-le
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
s--stit-ti-n -i-he- --in -s an- sha-e in the --n -- s-l-in- them.

   H---M--QU--XYZ----TO------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

AZ suggests a word.
HZL suggests a word.
AN suggests a word.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
--namental -i-he-s ---asi-nall- a--ea- -n the ---e- -- ---
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine ----i-in- a -ni--e -hallen-e.  this -ne is a sim-le
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
s--stit-ti-n -i-he- --in -s an- sha-e in the --n -- s-l-in- them.

   H---M--QU--XYZ----TO------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

AZ could be ON.
HZL could be AND.
AN could be OF.
Try A=o, L=d, N=f.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
o-namental -i-he-s o--asionall- a--ea- on the -o-e- of o--
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine --o-idin- a -ni--e -hallen-e.  this one is a sim-le
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
s--stit-tion -i-he- -oin -s and sha-e in the f-n of sol-in- them.

   H--LMN-QU--XYZA---TO------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

AZYHYMZOHX and AKKHTUAZHXXF suggest words.
CT and NCZ suggest words.
TUYRXM suggests a word.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
o-namental -i-he-s o--asionall- a--ea- on the -o-e- of o--
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine --o-idin- a -ni--e -hallen-e.  this one is a sim-le
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
s--stit-tion -i-he- -oin -s and sha-e in the f-n of sol-in- them.

   H--LMN-QU--XYZA---TO------   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

AZYHYMZOHX and AKKHTUAZHXXF could be ORNAMENTAL and OCCASIONALLY. Try S=r, K=c, F=y.
CT and NCZ could be US and FUN. Try C=u..
TUYRXM could be SIMPLE. Try R=p.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
ornamental ciphers occasionally appear on the co-er of our
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine pro-idin- a uni-ue challen-e.  this one is a simple
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
su-stitution cipher -oin us and share in the fun of sol-in- them.

   H-KLMN-QU--XYZAR-STOC---F-   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

Our added letters are fitting nicely with the existing alphabet. Right now the alphabet helps show K2 (keyword in ciphertext alphabet). This ornamental did not tell what key type was used. Sidebar: What if we had assumed K1? What if the CIPHERTEXT alphabet was A-Z, and we fill in the plaintext alphabet as we go?

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
ornamental ciphers occasionally appear on the co-er of our
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine pro-idin- a uni-ue challen-e.  this one is a simple
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
su-stitution cipher -oin us and share in the fun of sol-in- them.

   H-KLMN-QU--XYZAR-STOC---F-   CIPHERTEXT
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

Sidebar: The top 2 lines show K2 (keyword in ciphertext alphabet), the bottom 2 lines show K1 (keyword in plaintext alphabet). In K1, the large gap between CDEF and H make it unlikely, so then switch to check K2.
Generally, it's not too hard to recognize K1 vs K2.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
ornamental ciphers occasionally appear on the co-er of our
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine pro-idin- a uni-ue challen-e.  this one is a simple
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
su-stitution cipher -oin us and share in the fun of sol-in- them.

   H-KLMN-QU--XYZAR-STOC---F-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext       ciphertext
   o-u—-y-a-cdef---h---i--lmn                   plaintext  (K1)
```

Solving Cover from Sample *Cm*

CZUICM suggests a word.
Our alphabet suggests some more guesses.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
ornamental ciphers occasionally appear on the co-er of our
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
ma-a-ine pro-idin- a uni-ue challen-e.  this one is a simple
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
su-stitution cipher -oin us and share in the fun of sol-in- them.

   H-KLMN-QU--XYZAR-STOC---F-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving Cover from Sample *Cm*

CZUICM could be UNIQUE. Try I=q.
Our alphabet allows some more guesses. G=z, J=b, P=g, V=j, W=k.
B, D, E remain to be placed.

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
ornamental ciphers occasionally appear on the co-er of our
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
magazine pro-iding a unique challenge.  this one is a simple
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
substitution cipher join us and share in the fun of sol-ing them.

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

Solving Cover from Sample *Cm*

KABMS must be COVER. B=v, leaving D=w, E=x.
Solved! And the keyword appears to be ARISTOCRAT.

Record the solution so you could later submit it for credit

```
Cover. ARISTOCRAT ornamental ciphers occasionally
appear on the cover
```

```
ASZHYMZOHX KURQMST AKKHTUAZHXXF HRRMHS AZ OQM KABMS AN ACS
ornamental ciphers occasionally appear on the cover of our
YHPHGUZM RSABULUZP H CZUICM KQHXXMZPM.  OQUT AZM UT H TUYRXM
magazine providing a unique challenge.  this one is a simple
TCJTOUOCOUAZ KURQMS VAUZ CT HZL TQHSM UZ OQM NCZ AN TAXBUZP OQMY.
substitution cipher join us and share in the fun of solving them.

   HJKLMNPQUVWXYZARISTOCBDEFG   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

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/