Examples of Solving *Cm* Cons*

Solving A-2 from Sample *Cm*

Aristocrat (Simple Substitution)

* "*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
xz**keyword**abcfghijlmnpqstuv		one keyword
XZ**KEYWORD**ABCFGHIJLMNPQSTUV	K2	HGY BYUSILE
abcdefghijklmnopqrstuvwxyz		one keyword
XZ**KEYWORD**ABCFGHIJLMNPQSTUV	K3	DQW YWORDAB
uvxz**keyword**abcfghijlmnpqst		one keyword
XZ**KEYWORD**ABCFGHIJLMNPQSTUV	K4	CZQ MBEZQTGU
vwxyz**alphbet**cdfgijkmnoqrsu		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 A-2 from Sample *Cm*

```
A-2. Identity crisis? K2 [96] (XVEWL) WABBIT
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA
RPSEF NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP
NSPQA!"
```

What does the first line tell us?

Cipher ID: A-2.

Title: “Identity crisis?” A clue to plaintext content?

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

Length is 96 letters. Created by ACA member WABBIT.

Crib is XVEWL in Caesar cipher; TRASH in plaintext.

Solving A-2 from Sample *Cm*

Possible locations for crib TRASH:

JAVGX, RPZQC, RPSEF, NBEFQ, NSPQA.

Do any look promising?

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
----- ------ *-------, ------ ----- --- ------ --- ------- -----
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
----- -- --, --------, "--- ----! --- ------- ---- -----!"


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

Solving A-2 from Sample *Cm*

Possible locations for crib TRASH:

JAVGX, RPZQC, RPSEF, NBEFQ, NSPQA.

Note that the letters of the crib include R, S, T.

Do any words have similarly consecutive letters?

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
----- ------ *-------, ------ ----- --- ------ --- ------- -----
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
----- -- --, --------, "--- ----! --- ------- ---- -----!"


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

Solving A-2 from Sample *Cm*

Possible locations for crib TRASH:

The letters of the crib include R, S, T.

RPZQC has P, Q, R in places where the crib has R, S, T.

Try P=r, Q=s, R=t, Z=a, C=h.

(If this doesn’t work out, come back and try the rest.)

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
----- -a---- *-art-a-, s----- trash -a- t----- --- -ar-a-- tr---
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
----s -t --, sh--t---, “h-- -a--! --- -r----- ---r --rs-!"


   Z------C---------PQR------   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

BR suggests a word.

The endings of *HZPRBZJ, QAABJI, QCKSRBJI stand out…

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
----- -a---- *-art-a-, s----- trash -a- t----- --- -ar-a-- tr---
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
----s -t --, sh--t---, “h-- -a--! --- -r----- ---r --rs-!"


   Z------C---------PQR------   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

BR can’t be AT, so it must be IT. B=i.
The words *HZPRBZJ, QAABJI, QCKSRBJI could end in -IAN, -ING, -ING. Try J=n, I=g.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
n---- -an--- *-artian, s--ing trash -an t----- --- gar-ag- tr---
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
-i--s it --, sh--ting, “h-- -a--! --- -r----- ---r --rs-!"


   Z-----ICB----J---PQR------   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

QAABJI suggests a word. Then EZJ suggests a word.
Note QCKSRBJI... The alphabet suggests where K, S might go.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
n---- -an--- *-artian, s--ing trash -an t----- --- gar-ag- tr---
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
-i--s it --, sh--ting, “h-- -a--! --- -r----- ---r --rs-!"


   Z-----ICB----J---PQR------   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

QAABJI suggests SEEING. EZJ suggests CAN. A=e, E=c.
Note QCKSRBJI... The alphabet suggests that K, S might go right after J,R in the plaintext alphabet. K=o, S=u.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne--- -an-e- *-artian, seeing trash can to---e o-- gar-age truc-
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
-ic-s it u-, shouting, “he- -a--! -ou -ro--e- -our -urse!"


   Z-E-A-ICB----JK--PQRS-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

*HZPRBZJ, IZPMZIA, RPSEF, SN, XKS all suggest words.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne--- -an-e- *-artian, seeing trash can to---e o-- gar-age truc-
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
-ic-s it u-, shouting, “he- -a--! -ou -ro--e- -our -urse!"


   Z-E-A-ICB----JK--PQRS-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

*HZPRBZJ could be *MARTIAN, IZPMZIA could be GARBAGE, RPSEF could be TRUCK, SN could be UP, XKS could be YOU. Try H=m, M=b, F=k, N=p, X=y.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne--y -an-e- *martian, seeing trash can topp-e o-- garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey -a-y! you -roppe- your purse!"


   ZME-A-ICB-F-HJKN-PQRS---X-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

TPKNNAT, GZJTAT, KLL all suggest words.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne--y -an-e- *martian, seeing trash can topp-e o-- garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey -a-y! you -roppe- your purse!"


   ZME-A-ICB-F-HJKN-PQRS---X-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

TPKNNAT could be DROPPED, GZJTAT could be LANDED, KLL could be OFF. Try T=d, G=l, L=f.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne-ly landed *martian, seeing trash can topple off garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey lady! you dropped your purse!"


   ZMETALICB-FGHJKN-PQRS---X-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

TPKNNAT could be DROPPED, GZJTAT could be LANDED, KLL could be OFF. Try T=d, G=l, L=f.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne-ly landed *martian, seeing trash can topple off garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey lady! you dropped your purse!"


   ZMETALICB-FGHJKN-PQRS---X-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

How can the alphabet be finished off? What is the keyword(s)?

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
ne-ly landed *martian, seeing trash can topple off garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey lady! you dropped your purse!"


   ZMETALICB-FGHJKN-PQRS---X-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

Fitting the missing letters into the alphabet, we discover the first word is NEWLY.

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
newly landed *martian, seeing trash can topple off garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey lady! you dropped your purse!"

            D      O    UVW Y
   ZMETALICB-FGHJKN-PQRS---X-   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

Solved! And the keyword appears to be METALLIC.

Record the solution so you could later submit it for credit

```
A-2 METALLIC newly landed *martian, seeing trash can
```

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF
newly landed *martian, seeing trash can topple off garbage truck
NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
picks it up, shouting, “hey lady! you dropped your purse!"


  ZMETALICBDFGHJKNOPQRSUVWXY   CIPHERTEXT (K2)
  abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving A-2 from Sample *Cm*

Sidebar: What if I had chosen unwisely in positioning the crib?

Below are four other possible crib locations with a short word from the cipher that demonstrates it was an unlikely location.

```
JAVGX: CAX,   RPSEF: XKS,   NBEFQ: BR,   NSPQA: SN
trash: -rh,   trash: --a,   trash: r-,   trash: rt
```

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/