Examples of Solving *Cm* Cons*

Solving A-1 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
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 A-1 from Sample *Cm*

A-1. City living. K1 [90] PRIME
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.

What does the first line tell us?

Cipher ID: A-1.

Title: “City living.” A clue to plaintext content?

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

Length is 90 letters. Created by ACA member PRIME.

No crib – must look for clues in words and phrasing.

Solving A-1 from Sample *Cm*

Possible places to start:

Pattern words: EFBE, AKFA.

Shared-letter words: F, FA, YFA, AKFA.   Also ZE, EQ, QI.

Apostrophe use: YFP’A.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ------ *--- ---- --- ------ ---- -- -- ----- ---- --- ---'-
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
----- -- --- --- ------- ------- - -------- -- ----.


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

Solving A-1 from Sample *Cm*

The apostrophe word might be a contraction. Try: P=n, A=t.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ----n- *--- ---- --- ----n- ---- -- -- ----- t--t --- --n‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
----t -t t-- --t --t---t --tt-n- - ---t---- -- ----.

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

Solving A-1 from Sample *Cm*

Pattern word AKFA stands out…

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ----n- *--- ---- --- ----n- ---- -- -- ----- t--t --- --n‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
----t -t t-- --t --t---t --tt-n- - ---t---- -- ----.

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

Solving A-1 from Sample *Cm*

Pattern word AKFA could be THAT. Try K=h, F=a.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ----n- *--- -a-- h-- ----n- ---- -- -- --a-- that --- -an‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
-h--t at th- -at --th--t --tt-n- a ---th--- -- ha--.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   t----a----h----n----------   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

The word AKD stands out...
The word YFP’A stands out...

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ----n- *--- -a-- h-- ----n- ---- -- -- --a-- that --- -an‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
-h--t at th- -at --th--t --tt-n- a ---th--- -- ha--.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   t----a----h----n----------   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

The word AKD could be THE. Try D=e.
The word YFP’A could be CAN’T. Try Y=c.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ---en- *--- -a-- h-- ----n- ---- -- -- --a-- that --- can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
-h--t at the cat --th--t -ett-n- a ---th--- -- ha--.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   t--e-a----h----n--------c-   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

NZUZPJ and JDAAZPJ have the same three letter ending…

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- ---en- *--- -a-- h-- ----n- ---- -- -- --a-- that --- can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
-h--t at the cat --th--t -ett-n- a ---th--- -- ha--.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   t--e-a----h----n--------c-   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

NZUZPJ and JDAAZPJ have the same three letter ending.
Could this common ending be ING? Try Z=I, J=g.
Note: J=g fits nicely next to K=h in the plaintext alphabet.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- --ien- *--- -a-- hi- -i-ing ---- i- -- --a-- that --- can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
-h--t at the cat -ith--t getting a ---th--- -- hai-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   t--e-a---gh----n--------ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

EFBE KZE stands out… Guessing what E represents would fill in three letters!

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-- --ien- *--- -a-- hi- -i-ing ---- i- -- --a-- that --- can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
-h--t at the cat -ith--t getting a ---th--- -- hai-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   t--e-a---gh----n--------ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

EFBE KZE could be SAYS HIS. Try B=y, E=s.

Note: after B=y, CITY appears in the plaintext alphabet.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-y --ien- *--- says his -i-ing ---- is s- s-a-- that y-- can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
sh--t at the cat -ith--t getting a ---th--- -- hai-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa---gh----n--------ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

EQ and BQT stand out…

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-y --ien- *--- says his -i-ing ---- is s- s-a-- that y-- can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
sh--t at the cat -ith--t getting a ---th--- -- hai-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa---gh----n--------ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

BQT looks like it could be YOU. Try Q=o, T=u.

Note: Q=o fits nicely next to P=n in the plaintext alphabet.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-y --ien- *-o- says his -i-ing -oo- is so s-a-- that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat -ithout getting a -o-th-u- o- hai-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa---gh----no--u----ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

OB, VZAKQTA, QI, EOFNN, SQQO all stand out as words to guess.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
-y --ien- *-o- says his -i-ing -oo- is so s-a-- that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat -ithout getting a -o-th-u- o- hai-.

  ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
  ty-esa---gh----no--u----ci   plaintext  (K1)
```

Solving A-1 from Sample Cm

OB, VZAKQTA, QI, EOFNN, SQQO look like they could be MY, WITHOUT, OF, SMALL, ROOM. Try O=m, V=w, I=f, N=l, S=r. Note: these letters all fit nicely in the plaintext alphabet.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
my frien- *-o- says his li-ing room is so small that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat without getting a mouthful of hair.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa--fgh--lmno-ru-w--ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

ISZDPH and NZUZPJ stand out…

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
my frien- *-o- says his li-ing room is so small that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat without getting a mouthful of hair.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa--fgh--lmno-ru-w--ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

ISZDPH could be FRIEND. NZUZPJ could be LIVING. Try I=f, H=d, U=v.

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
my friend *-o- says his living room is so small that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat without getting a mouthful of hair.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa-dfgh--lmno-ruvw--ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

Still missing *GQG…
Does the plaintext alphabet suggest anything?

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
my friend *-o- says his living room is so small that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat without getting a mouthful of hair.

  ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
  ty-esa-dfgh--lmno-ruvw--ci   plaintext  (K1)
```

Solving A-1 from Sample *Cm*

Fitting missing letters into the alphabet allows us to discover *GQG is *BOB.
Solved! But what is the keyword?

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
my friend *bob says his living room is so small that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat without getting a mouthful of hair.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ty-esa-dfgh--lmno-ruvw--ci   plaintext  (K1)
     p   b    jk    q    xz
```

Solving A-1 from Sample *Cm*

Final look at the plaintext alphabet shows the keyword could be CITY TYPES, or CITY PETS, or even CITY PEST. Probably CITY PETS.

Record the solution so you could later submit it for credit

```
A-1 CITYPETS my friend *bob says his living room is so
```

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A
my friend *bob says his living room is so small that you can‘t
EKQTA FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
shout at the cat without getting a mouthful of hair.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   typesabdfghjklmnoqruvwxzci   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/