Examples of Solving *Cm* Cons*

Solving X-2 from Sample *Cm*

Xenocrypt: French 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 X-2 from Sample *Cm*

```
X-2. French. Big is Beautiful? K2 (qui; EYB) OOBOO
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
```

<u>What does the first line tell us?</u>

Cipher ID: X-2. An Aristocrat in French.

Title: “Big is Beautiful?” A clue to plaintext content?

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

Crib word is QUI. (This word appears in the plaintext.)

Additional crib word is EYB (in Caesar cipher).

This cipher created by ACA member OOBOO.

Solving X-2 from Sample *Cm*

Find a location for the crib word. Three letters, matching QUI.
(We'll save the additional crib for later – see if we need it)
There are four possible three-letter words.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
--- ---------- ---------: "---- --- -'---------- ---- --- -------
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
------ ---------- ------------ ---------- --- -------."

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

Solving X-2 from Sample *Cm*

Crib word is QUI. Four possible locations.
ERQ looks unlikely (KEF would be -Q-).
DEW looks possible. Other uses of D are followed by E.
KEF looks unlikely. Other uses of K not followed by E.
PQO looks unlikely. Four words ending in -QO.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
--- ---------- ---------: "---- --- -'---------- ---- --- -------
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
------ ---------- ------------ ---------- --- -------."

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

Solving X-2 from Sample *Cm*

DEW could be QUI. Try D=Q, E=u, W=i.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
u-- -------i-- ---------: "--u- qui -'----iqu--- ---- -u- ---i---
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
------ ---i------ ---i--i------ i--------- --- -------."

   --------W-------D---E-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

ERQ suggests an initial word for the cipher.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
u-- -------i-- ---------: "--u- qui -'----iqu--- ---- -u- ---i---
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
------ ---i------ ---i--i------ i--------- --- -------."

   --------W-------D---E-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

A French sentence might start out with LA, LE, LES, UN, UNE. ERQ could be UNE. Try R=n, Q=e.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une e---e--i-n -e------e: "-eu- qui -'----iquen- ---- -u- -e-i-e-
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
----e- -e-iennen- ---in-i-e-en- in------e- -e- ---n-e-."

   ----Q---W----R--D---E-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

Three words end with -QRS.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une e---e--i-n -e------e: "-eu- qui -'----iquen- ---- -u- -e-i-e-
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
----e- -e-iennen- ---in-i-e-en- in------e- -e- ---n-e-."

   ----Q---W----R--D---E-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

-QRS could be –ENT. Try S=t.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une e---e--i-n -e------e: "-eu- qui -'----iquent t--- -u- -etite-
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
----e- -e-iennent ---in-i-e-ent in------e- -e- ---n-e-."

   ----Q---W----R--D--SE-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

NQSWSQO suggests a word.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une e---e--i-n -e------e: "-eu- qui -'----iquent t--- -u- -etite-
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
----e- -e-iennent ---in-i-e-ent in------e- -e- ---n-e-."

   ----Q---W----R--D--SE-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

NQSWSQO could be PETITES. Try N=p, O=s.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une e-p-essi-n -e------e: "-eu- qui s'-pp-iquent t--p -u- petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
---ses -e-iennent ---in-i-e-ent in--p---es -es ---n-es."

   ----Q---W----R-ND-OSE-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

(A keyword starts peeking out from the alphabet)
QFNIQOOWAR suggests a word common to English.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une e-p-essi-n -e------e: "-eu- qui s'-pp-iquent t--p -u- petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
---ses -e-iennent ---in-i-e-ent in--p---es -es ---n-es."

   ----Q---W----R-ND-OSE-----   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

QFNIQOOWAR could be EXPRESSION. Try F=x, I=r, A=o.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression -e-or---e: "-eux qui s'-pp-iquent trop -ux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
--oses -e-iennent or-in-ire-ent in--p---es -es -r-n-es."

   ----Q---W----RANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

KEF stands out, and K should be a vowel (after the apostrophe).
PQO stands out.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression -e-or---e: "-eux qui s'-pp-iquent trop -ux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
--oses -e-iennent or-in-ire-ent in--p---es -es -r-n-es."

   ----Q---W----RANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

KEF could be AUX. Try K=a.
PQO could be DES. Try P=d.
(PQO might have been LES, but the last word seems more likely to end with -RANDES than with -RANLES.)

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression -e-ora--e: "-eux qui s`app-iquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
--oses de-iennent ordinaire-ent in-apa--es des -randes."

   K--PQ---W----RANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

The cipher title, “Big is Beautiful?” suggests the final word.
The emerging keyword and alphabet suggest almost everything else.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression -e-ora--e: "-eux qui s‘app-iquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
--oses de-iennent ordinaire-ent in-apa--es des -randes."

   K--PQ---W----RANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

Big? UIKRPQO could be GRANDES. Try U=g.
GQGAIKLZQ could be MEMORABLE. Tru G=m, L=b, Z=l.
MVAOQO could be CHOSES. Try M=c, V=h.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression memorable: “ceux qui s‘appliquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
choses de-iennent ordinairement incapables des grandes."

   KLMPQ-UVW--ZGRANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

Complete the keyword alphabet and discover where letter B goes.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression memorable: “ceux qui s‘appliquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
choses de-iennent ordinairement incapables des grandes."

   KLMPQ-UVW--ZGRANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

Complete the keyword alphabet and discover where letter B goes.

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression memorable: “ceux qui s‘appliquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
choses de-iennent ordinairement incapables des grandes."
        T   XY          BC HJ
   KLMPQ-UVW--ZGRANDIOSE--F--   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

Google Translate suggests this means:

a memorable expression: "those that apply too much to small things become ordinarily incapable of the great. "

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression memorable: “ceux qui s‘appliquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
choses deviennent ordinairement incapables des grandes."

   KLMPQTUVWXYZGRANDIOSEBCFHJ   CIPHERTEXT (K2)
   abcdefghijklmnopqrstuvwxyz   plaintext
```

Solving X-2 from Sample *Cm*

GRANDIOSE appears to be the key.

Record the solution so you could later submit it for credit

```
X-2 GRANDIOSE une expression memorable ceux qui s’appliquent
```

```
ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO
une expression memorable: “ceux qui s‘appliquent trop aux petites
MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."
choses deviennent ordinairement incapables des grandes."

   KLMPQTUVWXYZGRANDIOSEBCFHJ   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/