Examples of Solving *Cm* Cons*

Solving X-1 from Sample *Cm*

Xenocrypt: Spanish 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-1 from Sample *Cm*

```
X-1. Spanish. A Naked Foot! K1 (dejada) HUMBUG
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
```

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

Cipher ID: X-1. An Aristocrat in Spanish.

Title: “A naked Foot!” A clue to plaintext content?

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

Crib word is DEJADA.

Cipher created by ACA member HUMBUG.

Solving X-1 from Sample *Cm*

Find a location for the crib. A six letter word matching DEJADA:

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
-- ---, ----- -- --- ----, -- ---------- ------------------ ---
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
-- -- ----- -- -- ----- -- --------- ------ --- -- --- -------.


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

Solving X-1 from Sample *Cm*

There is one possible location for the crib: NOQENE. N=d, O=e, Q=j, E=a.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
-- d-a, -e--a de -a- d--e, -e -----e-d-- e---a--d--a--a-e--e -e-
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
e- -a a-e-a de -a --a-a -a ----e---- dejada --- -- --e de---d-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ----a---------de-j---------   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

SE suggests a word.
NJE suggests a word.
Then FD suggests an intial word.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
-- d-a, -e--a de -a- d--e, -e -----e-d-- e---a--d--a--a-e--e -e-
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
e- -a a-e-a de -a --a-a -a ----e---- dejada --- -- --e de---d-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ----a--------de-j---------   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

SE could be LA. Try S=l.
NJE could be DIA. Try J=i.
FD could be UN. Try F=u, D=n.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, -e--a de la- d--e, -e -----endi- e---a--dina-ia-en-e -e-
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la a-ena de la -la-a la i---e-i-n dejada --- un -ie de-nud-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---nau---i---de-j-l-------   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

EHODE suggests a word.
Then SEW suggests a word.
Then UKH, UJO suggest two words.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, -e--a de la- d--e, -e -----endi- e---a--dina-ia-en-e -e-
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la a-ena de la -la-a la i---e-i-n dejada --- un -ie de-nud-.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---nau---i---de-j-l-------   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

EHODE could be ARENA.   Try H=r.
SEW could be LAS. Try W=s.
UKH, UJO could be POR, PIE. Try U=p, K=o.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, -er-a de las do-e, -e sorprendio e--raordinaria-en-e -er
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la pla-a la i-presion dejada por un pie desnudo.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---nau-r-io--de-j-l-p-----   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

MOHME suggests a word.
OAXHEKHNJDEHJETODXO suggests a word.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, -er-a de las do-e, -e sorprendio e--raordinaria-en-e -er
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la pla-a la i-presion dejada por un pie desnudo.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   ---nau-r-io--de-j-l-p-----   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

MOHME could be CERCA. Try M=c.
OAXHEKHNJDEHJETODXO could be EXTRAORDINARIAMENTE.
Try A=x, X=t, T=m.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, cerca de las doce, me sorprendio extraordinariamente -er
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la pla-a la impresion dejada por un pie desnudo.

  ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
  x--nau-r-io-cde-j-lmp--t--   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

Try to place some of the missing letters into the alphabet.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, cerca de las doce, me sorprendio extraordinariamente -er
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la pla-a la impresion dejada por un pie desnudo.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   x--nau-r-io-cde-j-lmp--t--   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

Many letters can be placed. It looks like one of (F, G, H) goes between E and J, and the other two into NAU-R-IO.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, cerca de las doce, me sorprendio extraordinariamente ver
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la playa la impresion dejada por un pie desnudo.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   x--nau-r-io-cde-j-lmp--t--   plaintext   (K1)
    yz         b     k   qs vw
```

Solving X-1 from Sample *Cm*

A trip to Google Translate tells me the text means:

one day, about twelve o'clock, I was astonished to see, on the sand of the beach, the impression left by a naked foot.

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, cerca de las doce, me sorprendio extraordinariamente ver
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la playa la impresion dejada por un pie desnudo.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   xyznau-r-iobcde-jklmpqstvw   plaintext  (K1)
```

Solving X-1 from Sample *Cm*

A quick check in a Spanish dictionary. . . NAUFRAGIO means SHIPWRECK – that must be the keyword.

Record the solution so you could later submit it for credit

```
X-1 NAUFRAGIO un dia, cerca las doce, me sorprendio
```

```
FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH
un dia, cerca de las doce, me sorprendio extraordinariamente ver
OD SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.
en la arena de la playa la impresion dejada por un pie desnudo.

   ABCDEFGHIJKLMNOPQRSTUVWXYZ   CIPHERTEXT
   xyznaufrgiobcdehjklmpqstvw   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/