The Logogryph of Euler

By *Hans Rohrbach* at Mainz

To Helmut Hasse on his 75th birthday

---

1. The problem

At the end of a rather long letter on differential calculus written July 4, 1744 to Christian Goldbach, Leonhard Euler (1707—1783) proposed the problem to solve a certain logogryph, i. e. a cryptogram, the cipher for which was worked out by Euler himself. And he expressed his conviction that the deciphering would be no easy task. In his letter, the passage in question runs as follows:

"Ich habe vor einiger Zeit nachfolgenden logogryphum entworfen, worin alle characteres Buchstaben bedeuten und der Text latein ist:

(1)
pxqſwlznjdvynſtiddkqxhleebfpxdfgtlzbccfbkſodxokfnglqxnſchejmlckzxhrfwjgfh
xvzjnbgyxcdgixkoxjmlncoigdxvzflmeſnfyjqfangvnylrcxfonbfjalrkwſnbfpjoizoxq
knubroſadgiaxwkcbrbcklofrnjwgnſzfhgjfcbcfvqjtxeevtbzfyjsbzhſmlnbgſsqjwgl
nxvzfkonbcoigdxvrkfjalzxtſnilenfgvcboofcfxnnfgnkbcjnnjynxvplgnbfzfoxeejgdxbcj
cnſdyvdbhzlnvyxmbcblobbcyfekonbceiobfplwsxzxfjcndbhrlzqxsſonbcoljffyqfm
jeevhleexoiexmgicfdnktvoldxnfbxoſcktvpxrnv

Ungeachtet hier die Bedeutung der characterum nicht veränderlich ist, so deucht mich doch, daß dergleichen Schrift nicht leicht dechiffriert werden kann." [2])

The reaction of Goldbach towards the problem proposed to him is unknown. Within the correspondence of the two mathematicians there is no answer nor any other hint to be found. Apparently Goldbach succeeded in deciphering the logogryph — he certainly was able to find the solution — but had no further interest in it. Real mathematical problems seemed to be of more importance to both of them — to the inventor of the code as well as to the code-breaker.

---

[1]) P. H. Fuss, Correspondance mathématique et physique de quelques célèbres géomètres de XVIIIe siècle. **1**, 278—293, St. Petersburg 1843. Or: A. P. Juškevič and E. Winter, Leonhard Euler und Christian Goldbach, Briefwechsel 1729—1764, Abhandl. Deutsche Akad. Wiss. Berlin 1965, 200. In a footnote on p. 201 the paper of P. Speziali[3]) is mentioned. — The text of the cryptogram as given in the book of Juškevič and Winter is in some way confusing since the character ſ is printed as *s* which is one character itself. In addition there are some misprints.

[2]) Translation: "Some time ago I constructed the following cryptogram all characters of which have the meaning of letters and the plaintext is written in Latin: *pxq . . . rnv*. In spite of the fact that there is no change in the meaning of the characters I think that a cryptogram of that kind may not be easily deciphered."

Nevertheless, each proposed problem — the solution of which is unknown — has a right of being treated and even more so if the proposer is one of the world's most famous mathematicians. So, Ferdinand Rudio, then president of the Euler Committee at Basel (Switzerland) which is in charge of editing Euler's Collected Papers, in 1907 — when the Committee was constituted at the 200th anniversary of Euler's birth day — announced a competition and an award for the solution of the logogryph. Again, there was no answer. In 1953 the competition and the award were announced anew. This time within a few weeks the solution was given by P. Speziali and published in an at least for mathematicians rather unknown periodical[3]).

At the same time (spring 1953) a Swiss friend of mine knowing of my being interested in cryptanalysis notified me of the competition. Then I, too, worked on the solution but put it aside when I heard of the work of Speziali.

In 1957, when I was teaching as Visiting Professor at the University of North Carolina, Chapel Hill, N.C., I was invited to present a One Hour Address on 'Mathematical Methods on Ciphering and Deciphering' at the Meeting of the American Mathematical Society, held in November 1957 at the University of Miami, Coral Gables, Florida[4]). Within that speech I gave a short account of my solution for the logogryph of Euler. Later on, a more detailed report was given at the 542nd Meeting of the Elisha Mitchell Scientific Society at Chapel Hill, N.C.[5]). It was only then that I was looking for the paper of Speziali.

In the meantime I repeatedly was asked to publish the solution for the logogryph because a problem proposed by Euler should be dealt with by a mathematician and the solution should be accessible through a mathematical periodical. So I take the opportunity for publication where a special volume of Crelle's Journal is dedicated to my friend Helmut Hasse since I know that he, too, is interested in cryptanalysis. Some time ago both of us, for a couple of years, were officially busy with, to be sure, more difficult material of that kind.

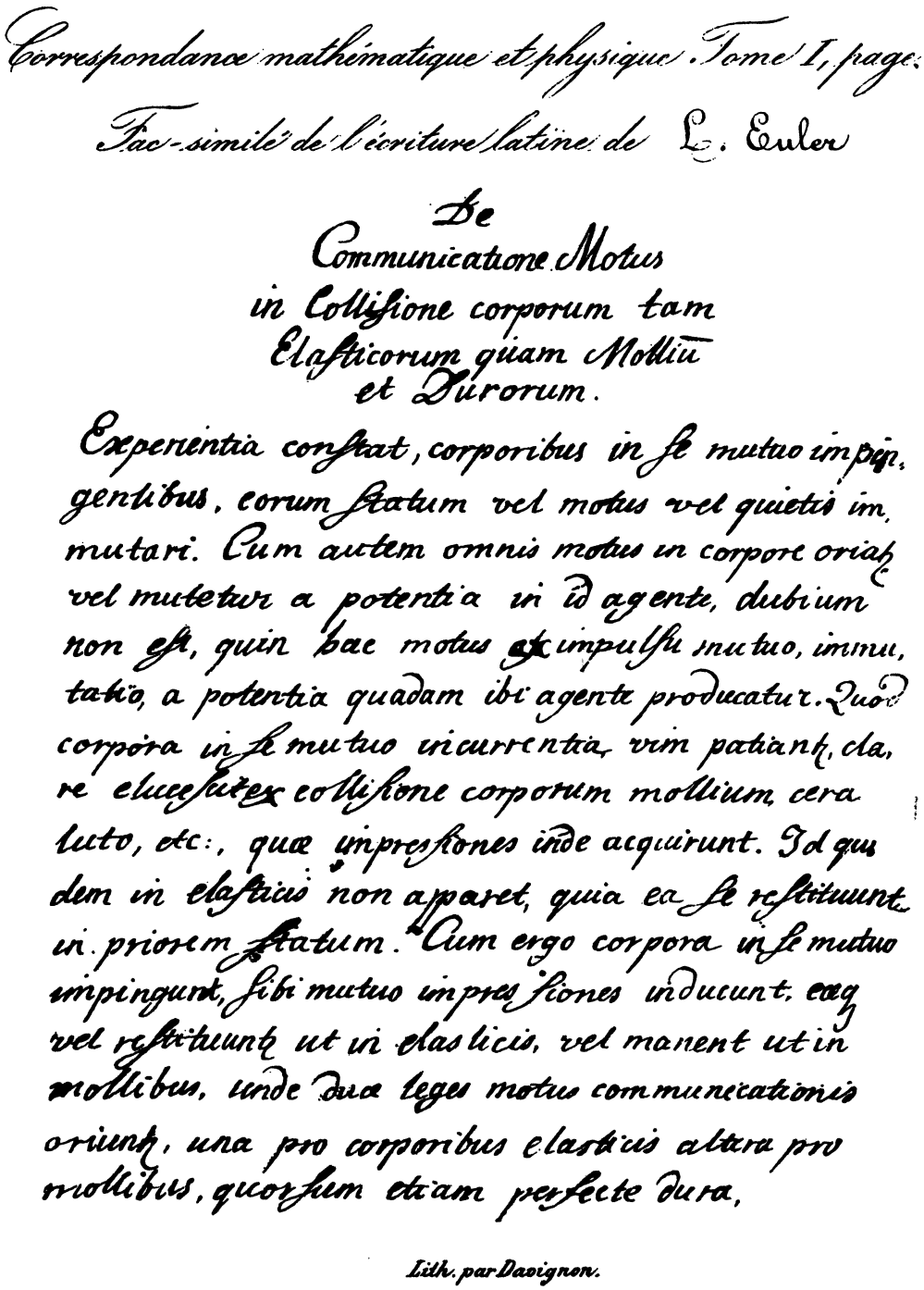
2. The solution

In order to break a cipher the first thing one has to find out is the method of enciphering. The two most simple methods are the transposition and the substitution cipher. If the characters of the plaintext are merely rearranged in order without any change in their identity, i. e. if some permutation is applied to the original characters, the system is called a *transposition cipher.* If however, the characters of the plaintext are replaced by equivalents (letters, figures, arbitrary symbols) without getting changed in their original order, the system is called a *substitution cipher.* Very probably Euler used the second one of these possibilities. To get a decision we need information about the relative frequencies of the characters in question. Valuable information is given by Euler himself since he says that all characters are letters and the underlying language is Latin. So we need two frequency statistics, one for the Latin language, one for the cipher text. But Euler does not say what kind of material he enciphered. It may have been part of a

[3]) P. Speziali, Le logogriphe d'Euler, Stultifera navis, Bull. Soc. Suisse d. Bibliophiles **10** (1953), 6—9. In May 1954, A. Linder (Genf University) reported about the paper of Speziali at a meeting of the Austrian Mathematical Society in Vienna, cf. the short notice (without any details) in International Math. News Austr. Math. Soc. 8 (1954), Nr. 33/34, p. 69.

[4]) Cf. The November Meeting at Coral Gables, Bull. AMS **64** (1958), 57.

[5]) The meeting took place on Feb. 11, 1958. Cf. Journ. Elisha Mitchell Scient. Soc. **74** (1958), 95.


Correspondance mathématique et physique. Tome I, page 3.

Fac-simile de l'écriture latine de L. Euler

De
Communicatione Motus
in Collisione corporum tam
Elasticorum quam Mollium
et Durorum.

Experientia constat, corporibus in se mutuo impingentibus, eorum statum vel motus vel quietis immutari. Cum autem omnis motus in corpore oriat vel mutetur a potentia in id agente, dubium non est, quin hae motus et impulsu mutuo, immutatio, a potentia quadam ibi agente producatur. Quod corpora in se mutuo incurrentia vim patiantur, clare elucescit ex collisione corporum mollium, cera luto, etc., quae impressiones inde acquirunt. Id quidem in elasticis non apparet, quia ea se restituunt in priorem statum. Cum ergo corpora in se mutuo impingunt, sibi mutuo impressiones inducunt, eas vel restituunt ut in elasticis, vel manent ut in mollibus, unde duae leges motus communicationis oriuntur, una pro corporibus elasticis altera pro mollibus, quorsum etiam perfecte dura,

Lith. par Davignon.

Fig. 1

mathematical paper (at that time scientific papers were mainly written in mediæval Latin, cf. fig. 1). It may have been taken out of a work of a Roman writer, then of course, the enciphered language is classic Latin.

Therefore I prepared a frequency statistic for the Latin language using both mediæval and classic Latin texts. The result is (fig. 2) that four letters (*k*, *w*, *y*, *z*) do not occur at all and nearly the same is true for the letter *j*. Now comparing this statistic with the

frequency statistic for the cipher text (fig. 3) one realizes at once that the method of enciphering used by Euler can not be a transposition cipher. Very probably it will turn out to be a substitution cipher, more precisely a *monalphabetic substitution cipher with homophones*, i. e. for some frequent letters obviously multiple substitutes were used[6]).

	50 100 150 200 250	Total	%
e	———————————	250	12.5
i	———————————	222	11.1
a	———————	153	7.6
t	———————	152	7.6
u	—————	139	7.0
n	—————	134	6.7
r	—————	132	6.6
s	—————	131	6.6
m	————	123	6.1
o	————	122	6.1
d	——	71	3.5
c	——	65	3.2
l	——	56	2.8
p	——	43	2.1
q	—	35	1.7
v	—	35	1.7
h	—	27	1.3
b	—	26	1.3
g	—	17	0.8
f	—	14	0.7
x	—	12	0.6
j	-	7	0.03
k		0	0
w		0	0
y		0	0
z		0	0

Fig. 2
Frequency statistic (about 2000 letters)
Plain Latin text

	10 20 30	Total	%
n	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 ////	34	8.5
f	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 //	32	8.0
x	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 /	31	7.75
b	𝍸 𝍸 𝍸 𝍸 𝍸 ///	28	7.0
c	𝍸 𝍸 𝍸 𝍸 ////	24	6.0
l	𝍸 𝍸 𝍸 𝍸 //	22	5.5
o	𝍸 𝍸 𝍸 𝍸 //	22	5.5
j	𝍸 𝍸 𝍸 𝍸 /	21	5.25
g	𝍸 𝍸 𝍸 ///	18	4.5
e	𝍸 𝍸 𝍸 /	16	4.0
v	𝍸 𝍸 𝍸 /	16	4.0
d	𝍸 𝍸 𝍸	15	3.75
k	𝍸 𝍸 𝍸	15	3.75
z	𝍸 𝍸 𝍸	15	3.75
ſ	𝍸 𝍸 𝍸	15	3.75
i	𝍸 𝍸	10	2.5
y	𝍸 𝍸	10	2.5
h	𝍸 ////	9	2.25
q	𝍸 ////	9	2.25
r	𝍸 ////	9	2.25
m	𝍸 //	7	1.75
t	𝍸 //	7	1.75
w	𝍸 //	7	1.75
p	𝍸 /	6	1.5
a	𝍸	5	1.25
s	////	4	1.0
u	/	1	0.25

Fig. 3
Frequency statistic (about 400 letters)
Cipher text

To confirm this assumption we study the cipher text and mark repetitions of groups of four or more letters by underlining. Since there are repetitions (cf. (3)) and in addition many bigrams and trigrams which occur twice, three times or more often, we can be sure that the cipher in question is a substitution cipher. Remarkable is that Euler used two different forms of the letter '*s*', besides the usual form '*s*' the stretched form '*ſ*' (cf. fig. 1). By this he had a set A of 27 letters at his disposal, $A = R \cup \{ſ\}$ where R is the set of the 26 letters of the Roman alphabet. The set A is to be mapped onto the set B of 20 letters, namely

$$B = R \setminus \{j, k, v, w, y, z\} = A \setminus \{j, k, v, w, y, z, ſ\} \tag{2}$$

with the agreement to replace within the plain text (before enciphering) each *j* resp. *v* which may occur by *i* resp. *u*[7]). The mapping of A onto B is surjective but not injective.

[6]) Cf. D. Kahn, The Codebreakers (The Story of Secret Writing), New York 1967. In this book which gives the first comprehensive history of secret communication from ancient to modern times also the logogryph of Euler is mentioned (p. 765).

[7]) In general, in texts of mediæval Latin *j* and *i* resp. *u* and *v* are represented by the same sign.

Now we have to check the repetitions. For a precise denoting we provide the cipher text (1) with a system of coordinates by dividing it into groups of 5 letters each (the last group of each row contains 6 letters) and numbering the rows by 1 through 8, the columns by a through j.

	a	b	c	d	e	f	g	h	i	j
	1 *pxqfw*	*lznjd*	*vynft*	*iddkq*	*xhlee*	*bfpxd*	*fgtlz*	*bccfb*	*kfodx*	*okfngl*
	2 *qxnfc*	*hejml*	*ckzxh*	*rfwjg*	*fhxvz*	*jnbgy*	*xcdgi*	*xkoxj*	*mlnco*	*igdxvz*
	3 *flmef*	*nfyjq*	*fangv*	*nylrc*	*xfonb*	*fjalr*	*kwfnb*	*fpjoi*	*zoxqk*	*nubrof*
(3)	4 *adgia*	*xwkcb*	*rbckl*	*ofrnj*	*wgnfz*	*fhgjf*	*cbcfv*	*qjtxe*	*evtbz*	*fyjsbz*
	5 *hfmln*	*bgfsq*	*jwgln*	*xvzfk*	*onbco*	*igdxv*	*rkfja*	*lzxtf*	*nilen*	*fgvcbo*
	6 *ofcfx*	*nnfgn*	*kbcjn*	*njynx*	*vplgn*	*bfzfo*	*xeejg*	*dxbcj*	*cnfdy*	*vdbhzl*
	7 *nvyxm*	*bcblo*	*bbcyf*	*ekonb*	*ceiob*	*fplws*	*xzxfj*	*cndbh*	*rlzqx*	*sfonbc*
	8 *oljff*	*yqfmj*	*eevhl*	*eexoi*	*exmgi*	*cfdnk*	*tvold*	*xnfbx*	*ofckt*	*vpxrnv*

Our aim is to find *alternates*, i. e. different originals which have the same image with respect to the mapping $A \to B$. Take for instance the 7 letter group '*coigdxv*' in 2i,j and in 5e,f. The first one is followed by *z*, the second one by *r*. And the same is true with the 4 letter group '*fjal*' in 5g,h and in 3f. So it may be allowed to identify *r* and *z*. This step is confirmed by the 5 letter group '*dbhzl*' in 6j if compared with '*dbhrl*' in 7h,i. The 4 letter group '*xvzf*' occurring twice, in 2j, 3a and in 5d, has the possible equivalent '*xvzj*' in 2e,f. So *j* and *f* may be alternates. Now consider the 5 letter group '*nnfgn*' in 6b and the 5 letter group '*nnjyn*' in 6c,d. If *j* and *f* are alternates then *g* and *y* should be alternates too. This is supported by the trigrams '*fyj*' in 3b and 4j and the trigram '*jgf*' in 2d,e and by the trigrams '*nyl*' in 3d, '*ngl*' in 1j.

A possible further identification is to be gained from the 9 letter group '*fjalrkwfn*' in 3f,g compared with the group '*fjalzxtfn*' in 5g,h,i. Since *r* and *z* are already known as alternates it seems to be at hand to identify *k* and *x* as well as *w* and *t*. This step may be supported by the groups '*nnfgnk*' in 6b,c and '*nnjynx*', i. e. '*nnfgnx*' in 6c,d, the groups '*koxj*', i. e. '*koxf*' in 2h and '*xokf*' in 1i, j, and the groups '*zxfj*', i. e. '*rxfj*' in 7g and '*rkfj*' in 5g.

Using now the five so far assumed identifications

(4) $$j = f, k = x, w = t, y = g, z = r$$

(it may not be accidental that all of them are to be subtracted from *R* in (2)!) the reduced cipher text runs as follows:

	pxqft	*lrnfd*	*vgnft*	*iddxq*	*xhlee*	*bfpxd*	*fgtlr*	*bccfb*	*xfodx*	*oxfngl*
	qxnfc	*hefml*	*cxrxh*	*rftfg*	*fhxvr*	*fnbgg*	*xcdgi*	*xxoxf*	*mlnco*	*igdxvr*
	flmef	*nfgfq*	*fangv*	*nglrc*	*xfonb*	*ffalr*	*xtfnb*	*fpfoi*	*roxqx*	*nubrof*
(5)	*adgia*	*xtxcb*	*rbcxl*	*ofrnf*	*tgnfr*	*fhgff*	*cbcfv*	*qftxe*	*evtbr*	*fgfsbr*
	hfmln	*bgfsq*	*ftgln*	*xvrfx*	*onbco*	*igdxv*	*rxffa*	*lrxtf*	*nilen*	*fgvcbo*
	ofcfx	*nnfgn*	*xbcfn*	*nfgnx*	*vplgn*	*bfrfo*	*xeefg*	*dxbcf*	*cnfdg*	*vdbhrl*
	nvgxm	*bcblo*	*bbcgf*	*exonb*	*ceiob*	*fplts*	*xrxff*	*cndbh*	*rlrqx*	*sfonbc*
	olfff	*gqfmf*	*eevhl*	*eexoi*	*exmgi*	*cfdnx*	*tvold*	*xnfbx*	*ofcxt*	*vpxrnv*

The number of repetitions as indicated by underlining is larger than in the original cipher text (3). But as trials show there is not much advantage to look for more repetitions in order to get the (probably) last two alternates. A better way is to prepare a new frequency statistic from the reduced cipher text (5).

In this new statistic, the occurrence of a letter will not be marked, as usual, by a dash but by registering the immediately following letter. By this procedure the statistic does not only indicate the frequency of the letters, but in addition that of the bigrams. If a bigram happens to occur several times the repetition is marked by a dot (fig. 4).

The entrance column of this statistic contains 22 letters which are to be reduced to 20 in order to be mapped bijectively to the 20 elements of B. Certainly the letter '$\int$' will be one alternate and probably the v the second one. But first the bigrams are to be studied.

One of the most characteristic and frequent bigrams of the Latin language is '*qu*'. But within the entrance column there is no equivalent for a q to be found, i. e. a letter which is followed by one and the same other letter (equivalent to u). So we have to assume that Euler considered '*qu*' as one symbol in B and took as original for this bigram a single element of A. Now, q is a letter of rather low frequency and *qu* is followed by vowels only. The vowels, however, have very high frequencies. Combining both facts, by studying fig. 4 one is led to map $p \in A$ to *qu* ($q, u \in B$) and then $f \in A$ to $e \in B$, $x \in A$ to $i \in B$, and $l \in A$ to $a \in B$. By this we get '*que*', '*qui*', '*qua*' of the Latin plain text. Of course, the frequency of $l \in A$ so far does not correspond to that of $a \in B$. So it could be advisable to map $l \in A$ to $o \in B$; this would lead to '*quo*' of the plain text.

But there is one more striking fact in the statistic, the bigram '*ee*'. Since $e \in A$ obviously has to correspond to a consonant and is of low frequency it could be the image of d, l, or $p \in B$. With this and the above in mind we turn to the groups of the cipher text (5) containing *ee* to find the answer:

	i all equi		*e il l*		*ille*		*e e ll a lli*
1e,f	*xhlee bfp xd*	4h,i	*qftxe evtbr*	6g	*xeefg*	8b,c,d	*gqfmf eevhl eexoi*

Especially 6g is in favour for the correspondence of $e \in A$ to $l \in B$. At any rate, 1e,f, 4h,i, and 8c show that $b \in A$ and $v \in A$ have to be vowels. According to the frequency of b resp. v the correspondences of $u \in B$ to b and of $o \in B$ to v seem to be at hand, and then the very frequent bigram '*bc*' ($b, c \in A$) could stand for '*us*' ($u, s \in B$). Taking that for granted correct frequencies for $a \in B$ and $o \in B$ will be reached by pairing $l \in A$ and $v \in A$ with alternates. To find them we look through the statistic (fig. 4) for suitable sets of followers. So v and i (of the entrance column) are followed by sets of letters the intersection of which is remarkable large, the same being true for l and $\int$. Therefore, in addition to the identifications in (4) we suggest to identify $v = i$ and $\int = l$. Thus the statistic (fig. 4) gains its (probably) final shape (fig. 5).

Now, after having put the $o \in B$ above v and i in the groups 8c,d it is easy to guess the missing letters (and again it is verified that, in general, the beginning or the end of a cipher text will serve as a good starting-point for breaking the cipher):

	de b e llo ga ll ico
8b,c,d	*gqfmf eevhl eexoi*

and then the complete last row of the cipher text (5) gives all information necessary:

(6) *caesa rdeb e lloga ll ico li b ro septi mocap i tevi cesim oquinto*
olffl gqfmf eeihl eexoi exmgi cfdnx t iold xnfbx olcxt ip xrni

		abs.	%
f	*g*:::. *f*:: *c*:. *t*:. *a*: *m*: *n*: *p*: *o*: *d*. *b*. *h*. *r*. *e*. *x*. *l q v s* ſ	53	12.99
x	*o*::. *f*:: *v*:: *t*:: *n*:. *q*: *r*: *h*. *c*. *b*. *e*. *m*. *d x l s* ſ	46	11.28
n	*b*:::. *f*::: *x*:. ſ:. *g*: *n*. *v*. *c d i u*	34	8.33
b	*c*:::::. *f*:: *r*:. *g*. *h*. *x*. *b l o*	28	6.86
g	*f*:: *n*:: *v*: *d*: *l*: *i*: *x*. *g q t* ſ	28	6.86
c	*f*::. *b*:. *x*:. *o*: *n*. *c h d e g*	24	5.88
r	*f*::: *x*:: *n*: *b*. *o*. *l*. *c h q*	24	5.88
l	*r*::. *n*:. *e*: *o*. *c d g m f q*	22	5.39
o	*x*:. *n*:. *i*:. *b*. *f*. *l*. ſ. *d*	22	5.39
e	*e*:: *x*: *f*. *v*. *b i n* ſ	16	3.92
v	*r*: *g*. *p*. *c d o n h t q*	16	3.92
d	*x*::. *g*: *b*. *d f n v*	15	3.67
ſ	*n*: *t*. *o*. *c*. *r d g m a s*	15	3.67
t	*x*. *g*. *l*. ſ. *v*. *f i b s*	14	3.43
i	*g*. *r c d o a x l e*	10	2.45
h	*r*: *l*. *x e g* ſ	9	2.20
q	*f*:. *x*:. ſ	9	2.20
m	*l*: *b e f g*	7	1.71
p	*x*: *l*. *f*	6	1.47
a	*l*. *d n x*	5	1.22
s	*x b q* ſ	4	0.98
u	*b*	1	0.24
j	—		
k	—		
w	—		
y	—		
z	—		

Fig. 4
Cipher text, frequencies after the identifications

$j = f,\ k = x,\ w = t,\ y = g,\ z = r$

		abs.	%
f	*g*:::. *f*:: *c*:. *t*:. *a*: *m*: *n*: *p*: *o*: *d*. *b*. *h*. *r*. *e*. *x*. *l*. *q i s*	53	12.99
x	*o*::. *f*:: *i*:: *t*:: *n*:. *q*: *r*: *h*. *c*. *b*. *e*. *m*. *l*. *d x s*	46	11.28
l	*r*::: *n*::: *o*:. *e*: *t*: *c*: *d*. *g*. *m*. *f q s*	37	9.06
n	*b*:::. *f*::: *x*:. *l*:. *g*: *i*: *n*. *c d u*	34	8.33
b	*c*:::::. *f*:: *r*:. *g*. *h*. *x*. *b l o*	28	6.86
g	*i*::. *f*:: *n*:: *l*:. *d*: *x*. *g q t*	28	6.86
i	*r*:: *g*:. *p*. *c*. *d*. *o*. *a e h l n q t x*	26	6.37
c	*f*::. *b*:. *x*:. *o*: *n*. *c h d e g*	24	5.88
r	*f*::: *x*:: *n*: *b*. *o*. *l*. *c h q*	24	5.88
o	*x*:. *n*:. *l*:. *i*:. *b*. *f*. *d o*	22	5.39
e	*e*:: *x*:. *i*:. *f*. *b l n*	16	3.92
d	*x*::. *g*: *b*. *d f i n*	15	3.67
t	*l*:. *i*: *x*. *g*. *b f s*	14	3.43
h	*r*: *l*: *e x g*	9	2.20
q	*f*:. *x*:. *l*	9	2.20
m	*l*: *b e f g*	7	1.71
p	*x*: *l*. *f*	6	1.47
a	*l*. *d n x*	5	1.22
s	*x b l q*	4	0.98
u	*b*	1	0.24
j	—		
k	—		
v	—		
w	—		
y	—		
z	—		
ſ	—		

Fig. 5
Cipher text, frequencies after cancellation of all alternates

3. Final remarks

The mapping $A \to B$ which works from cipher text to plain text is given in extenso by

B:	x	u,v	s	p	l	e	r	g	o	e	i,j	a	b	t	c	qu	d	n	f	m	h	o	m	i,j	r	n	a
↑																											
A:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	f

For enciphering one has to take the opposite direction $B \to A$

A:	$l = f$	m	o	q	$f = j$	s	h	u	$k = x$	e	$t = w$	$r = z$	$i = v$	d	p	$g = y$	c	n	b	a
↑																				
B:	a	b	c	d	e	f	g	h	i,j	l	m	n	o	p	qu	r	s	t	u,v	x

In Cesar's work 'De Bello Gallico', book VII, chapter 25 (according to (6)) one finds the following passage:

Quidam ante portam oppidi Gallus, qui per manus
sebi ac picis traditas glaebas in ignem e regione turris
proiciebat, scorpione ab latere dextro trajectus
exanimatusque concidit. Hunc ex proximis unus jacen-
tem transgressus eodem illo munere fungabatur;
eadem ratione ictu scorpionis exanimato alteri suc-
cessit tertius et tertio quartus, nec prius ille
est a propugnatoribus vacuus relictus locus quam
restincto aggere atque omni ex parte submotis hostibus
finis est pugnandi factus.

In enciphering this passage Euler seemingly made some mistakes. He skipped line 9 and passed from 'quam' immediately to 'finis'. In line 2 he read '*glebas*' instead of '*glaebas*', in line 3 '*projiciebat*' and '*transjectus*', in line 6 '*altero*' but it may be that the differences are due to the edition of the text he used. Real mistakes in enciphering are that sometimes *e* was enciphered by ſ instead by *f*, rather often *s* by *f* instead by *c*, and once *b* by *u* instead by *m*. The first one of these mistakes is certainly caused by the first printed reproduction of Euler's letter to Goldbach. There it may have happened that Euler's handwritten letters *f* and ſ were confounded with each other; they look very alike (cf. fig. 1). The other mistakes in my opinion are due to a known customary error of cipher clerks to interchange the keys for enciphering and deciphering[8]). Two mistakes of that kind (*f* into *s* in the first group, *l* into *e* in the group before the last one) are corrected when deciphering the last row of the cipher text (cf. (6)).

In spite of these mistakes the deciphering was not difficult. The assumption of 'substitution cipher with homophones' is confirmed.

[8]) In the cipher text as given in the book of Juškevič and Winter (cf. [1])) the group 5b of (3) runs as *bgfſq* instead of *bgſsq*. Deciphering of the first running gives the correct version of the plain text. So the mistakes mentioned above could be entirely due to wrong forwarding by printing the original version as it was written by Euler in his letter to Goldbach.

Mathematisches Institut der Universität, 65 Mainz, Postfach 3980

Eingegangen 12. Mai 1973