

~~TOP SECRET~~

INTRODUCTION

This series of "problems" is the outgrowth of a highly informal discussion of "phenomena" presented to a recent gathering of certain technical personnel of operations, at which time passing reference was made to historical solutions, citing certain properties which had to be noted before further analysis was fruitful.

The idea occurred that perhaps a series of example (in which one does not have to reconstruct entire messages of plain text, etc.) would serve as a useful adjunct to the ordinary crypt courses. It is realized that the ground upon which the author is treading is far from firm -- opinions as to what one might be expected to observe and consider "phenomenal" differ! Also, hind-sight-often blinds one to the fact that even so-called obvious properties are often obscured in a person's zeal to tackle such a problem from all angles at once. With so many things to look for, it is surprising that so often the weak link is spotted relatively quickly!

It is my feeling, however, that as an over-all indication of a person's ability to react quickly to cryptographic stimuli, these problems might be an interesting challenge to those who are desirous of testing their perceptive judgement, at the same time offering a chance for learning a few of the countless properties which have been encountered in the past. As experience is probably the biggest factor in success with these (along with cryptanalytic imagination) the acolyte is at a serious disadvantage, but on the other hand has the opportunity for greater rewards as far as gaining information and explanation is concerned.

For the benefit of the aforementioned acolyte, it might be worth outlining some of the possible approaches and "things to look for".

Some properties are obvious (usually properties of identify, rather than relationship). If a message uses only 10 letters of the 26, one can hardly help but notice the fact on simple inspection! If every fourth digit of text is a 1, 2, or 3, it might take a few more glances to notice.

Many properties are latent however - in keeping with the laws of physics one must put some effort into the operation to produce a "phenomenal" result. This manipulation might involve more complex establishment of identify (unusual frequencies, heavy vowel content, etc.) or else an establishment of relationship between individual positions or groups (by subtraction, comparison, sequential relationship, positional relationship, etc.). One must be familiar with established procedures and technical vocabulary, such as differencing (major and minor), delta effects (horizontal or vertical), isomorphs, sum-checking, sliding cribs, and the like. No attempt is herein made to clear up any questions which arise in regard to techniques, and it is assumed that answers to such questions are readily available elsewhere. It is felt that in the process

~~TOP SECRET~~

~~TOP SECRET CANOE~~~~TOP SECRET~~

of doing these problems, certain techniques now unfamiliar to some individuals, will become clear. Certain statistical measurements such as the I.C. (Index of Coincidence) should become familiar tools, for example. Cyclic properties - either of identity or relationship 0 that show up only when a given interval or width is considered, are obviously not to be ignored.

Appended to the collection of problems is a brief discussion of the basic principles involved in each, often with reference to the actual system upon which the problem is based. The original historical problem has sometimes been distorted almost beyond recognition in an attempt at simplification -- the general principle has been the goal rather than specific application, and no pretense is made that one could learn about the actual historical problem (German keyword, for example) by reading the appended remarks. It is hoped that later a more complete bibliography would enable the reader to follow up on any point to get the true facts of the case rather than a smattering of concepts, but it is felt that such an attempt is beyond the scope of this presentation.

One further caution -- the reader should not spend an undue amount of time pounding on any given problem. If a "reaction" is not forthcoming after a relatively short time (measured in minutes rather than hours) one could best profit by accepting the comments made in the appendix, and turning to the next problem, (it is to be hoped, with one more memory cell alerted for possible reoccurrence some time some place of the same phenomena).

~~TOP SECRET~~
~~SECURITY INFORMATION~~~~TOP SECRET CANOE~~

~~TOP SECRET~~

PROBLEM 1

Following are common groups of a certain code:

2912
0741
6635
7175
2462
9313

It is suspected that some time offset juxtaposition of the following cipher represents an overlap. Can you confirm this suspicion, after an examination of the code and cipher?

A 0473 9615 2807 1134 2886 7130 5520 0106 7022 8349 3474 etc.

B 3202 7736 3988 5217 0514 8261 4917 8372 3036 8971 4592 etc.

PROBLEM 2

Is there anything in the following list of cipher beginnings, sorted by date, which is phenomenal?

DATE	(1)	(2)	(3)	(4)	(5)
1/1	09411	02178	91380	55079	65503
3/1	77365	20417	89103	75319	77168
7/1	34051	61239	76219	20132	52587
11/1	16737	54188	10116	17083	34198
13/1	41070	75034	86705	40930	02930
19/1	02918	91725	59741	62622	09164
25/1	63152	83132	30247	60030	76293
2/2	49052	44068	45088	98967	73108
3/2	34701	78643	65539	23553	89121
5/2	81098	91227	70342	48138	40333
8/2	27763	33198	61982	93000	72847

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

PROBLEM 3

What do the following beginnings of message suggest?

ABURZ DAXYB	GOQON OOWKF
BSKPI IMACL	CRSOB DUXZM
IMLXH DDORC	LESPO RKIST
OOSGS WZDBA	OLPUV XMPSH
ASEST CLGSK	NHHUR XINGZ
DNCUA HFRET	ACOCO PLIQO
QFTAU FUQPT	DSPAO WPYUA
KRJLJ BEFSE	AANVX QAWCR
HSIKU IIRVF	OAIQE VYSTG
MAGMK OGVUJ	GROBS YJZXH
BPSVV JGAED	NDHXP EMZKY
EDHSS MIDIU	LNHDT RUVQL
BGDVY ADHWC	FJMDQ CAIWF
DHLBL TBQHU	ONFOF RNAVM
EFRNA NKCXJ	ERFRX SOBRX
EAMAC ZYPEV	QKBEF UBWDN
FQCTA WJNRJ	QKBEF UBWDN
FQCTA WJNRJ	PLAEG APCOE
INOAN AOQHS	

PROBLEM 4

What explanations are possible for the manifestations of the following cipher:

2193 4709 2890 1919 2703 8193 4743 6232 7890 6623 7703

PROBLEM 5

Can you detect any property of the following:

19273 62019 09821 31988

PROBLEM 6

-Country X is thought to be using a double-additive system, involving an 8-letter keyword which somehow designates two starting points in a series of additive lines; both additive streams are added to the plain code to obtain cipher. In testing possible cribs (with a recovered code) when the following crib is run against the cipher, certain evidence about the hypothesis of double additive is obtained.

Crib: 09436 02145 00107

To be tested all juxtapositions. (1st. group of plain against 1st. group, 2nd. group 3rd. etc of cipher).

Message: AEROABRO 19274 24983 72109 01474 88583 20363 65438 71002

-2-

~~TOP SECRET~~

~~SECURITY INFORMATION~~

PROBLEM 7

What is the peculiarity of the following portion of cipher text, and what might it imply?

PUKFH TCFGU OLZDX CBZAR: JOEVB NWZAO

PROBLEM 8

Background:

This country's main system seemingly involved one-time usage of literal key (or unique settings of machine encipherment). Indicators seem to be first groups, as in the past, these groups were patternized and progressive, e.g., AABBC, AABBE, etc.

New series of messages shows no repeats of letters within first groups, and no continuity from message to message, e.g. XRBDA, IOARQ, etc.

Eventually one reusage (?) of key was noted - two message with first group identical. The I. C. of these two messages, when compared, was approximately 1.8.

In the process of analysis, differences (on a normal alphabet) were taken vertically (message B subtracted from message A) with the following tabulation of occurrence.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
28	13	19	11	16	15	23	15	18	18	19	17	16	11	12	11	19	17	18	10	15	16
22	23	24	25																		
19	10	15	14																		

Can you detect and explain the property which instilled sufficient confidence to enable the reading of the depth?

PROBLEM 9

As a separate problem to the preceding, the following key was recovered by reading the overlap mentioned, and the property tentatively established that each line of 25 letters of key consisted of 25 unique values of the 26 possible.

CAPHOFNBKGMDOYSEJTXVRIUZW
JKSDRHCTEPTUBXQFLZAWGMOVN
RMCDTJOBUNFAKHZL...etc.

On the basis of cribs the following additional key looked reasonable. Can you predict any subsequent key?

~~TOP SECRET~~

RBKNYEMCLZAGASJVHWQITTFUOF
HLJGTNR

MOGNBPCQEZHLYLKXWJVSUTRF
XE

PROBLEM 10

What kind of system does the following case of two cipher beginnings suggest?

/38961240758329117125709848673

/38961791870989183768929741611

PROBLEM 11

Following is a list of first four and last four digraphs of a series of messages, sorted on first digraph. (Evidence has been noted that the system is probably a book-type literal key used to encipher digraphs from a basic chart page, and row-column coordinates of the starting and ending points are probably indicated.) Is anything apparent which might initiate solution of the indicator system?

AB KL OR AH...SS XA LX CF
AB CR BA ZI...KP AB CS OI
AB OF CL DW...TP BR VO LD
AB KM HI IG...EX YQ DC AQ
AB ZL BX IS...YQ AC RZ OK

AC PA FR OB...VP AA BF MB
AC RL ZC AK...AB OV CJ BB
AC TD NN LF...TJ ZX AH TV
AC LZ TB MB...QV AC MA SI
AC CN DG CH...XT AB KZ RD

AD BR RS NU...KZ GI KV SK
AD NO EL VP...OF ER DN NT
AD OV ML EE...NG AD OV LE

PROBLEM 12

A certain system with plenty of traffic, has a type of indicator which is probably not going to yield to ordinary analysis, however, certain depths (?) seem to imply reuse of key, probably from a key book. Can you note anything about the following two messages, seemingly in depth, which would suggest an obvious method of attack on the entire system?

/0913 6428 1097 6819 2281 2908 4376 etc.
/0913 6428 0322 0734 7365 2908 9281 etc.

~~TOP SECRET~~

~~SECURITY INFORMATION~~

PROBLEM 13

Three isologs (same plain code, different additive) are suspected in the following cases. Is there any property which would enable you to make a conjecture about the type of underlying additive?

A	16854	69919	39414	70324	02849
B	36852	48787	31638	68223	02848
C	58074	36686	53850	89445	91738
A	43351	18111	71353	96670	
B	40127	06090	69232	94650	
C	85570	32333	58121	05761	

Country X has been using one-time additive on 5-digit code. Additive pads were serially numbered (different series on each link). Pads have 48 groups on each page, with pad number preceding each block of 48 groups. Thus, the first group of a message might be 0001, the 50th 0002, the 99th 0003, etc.

A body of traffic showed us such sequence of indicators yet unrelated 4-digit numbers were intersperced at the proper intervals. The following is a list of pad (?) numbers as they appeared in order of usage within 4 separate links, giving the groups immediately following each 4-digit number.

Link A		Link B		Link C		Link D	
Enc.	<u>Cipher</u>	Enc.	<u>Cipher</u>	Enc.	<u>Cipher</u>	Enc.	<u>Cipher</u>
<u>Pad</u>		<u>Pad</u>		<u>Pad</u>		<u>Pad</u>	
7772	32179	0633	40713	5572	45945	6298	57764
2873	28103	5342	33101	8016	83454	3779	44851
3331	53520	3166	75919	7957	04416	0724	84479
3139	55684	7732	52818	0130	20192	8248	37657
6849	71902	6993	98358	9804	58217	1079	75892
2660	20729	5906	38061	3804	17280	8082	39320
3142	55900	3813	81282	5116	91305	2860	60553
3878	61199	5619	30260	1759	36429	6203	57808
3149	55991	0503	47036	0493	27516	2726	14641
7603	10955	6936	98938	8804	82270		
4944	98337						
7580	17048						

-5-

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

PROBLEM 15

The following key represents the first 4 groups on several one-time pad pages. It is suspected that some simple device was used to print successive pages, but the order of generation has been shuffled. However, collateral information implies the first two pads listed happen to have been generated sequently.

0439	9305	1237	9981
4337	7942	5896	7705
4284	7827	5103	7057
6104	2187	4643	7057
3396	6932	2071	6742
7761	5770	0365	5638
5652	0163	9722	0753
0955	9710	1425	9674
9971	1998	8461	1732
6711	2760	4915	2690
7180	5129	0744	5559
1076	8492	3871	8342
1755	8664	3952	8194
9688	1623	8900	1113
3203	6886	2149	6027
2622	4513	7628	4279
8128	3559	6680	3269
0580	9257	1604	9819
3782	6653	2388	6163
4725	7614	5322	7173
8311	3960	6455	3770
2416	4970	7411	4798
5466	0398	9061	0932
6097	2035	4896	2445
9849	1801	8539	1086

PROBLEM 16

The following is suspected to be the same plain text of two messages enciphered by a simple 5-wheel Hagelin device (non-overlapped). Is anything apparent which enables the reconstruction of at least one portion of the machine's set-up?

- (1) BSDEF IMIHO RYAWQ EEJTF HJRV5 OSPXQ VUGKS BPTNB OQVMB
- (2) BSDFG XMIHA FYMKC LAXAM QSVTF VVFVE CEDXC JUSYE BPHZP

PROBLEM 17

This is a message and a resend sent the next day.

SCDS	CQSJ	PXRH	NECJ	LWBD	SBFM	TEJS	WTEJ	YLUU	PKMD	QRDS	MCDJ	QCTU	HIPP
SCDS	CQRJ	IXDG	MHPK	LWCI	SCSN	MCHQ	WBCH	YKUO	OKNI	QSDT	STAJ	QPAT	GFQM
YRRB	PFLY	LBPD	KOYK	UWBF	GFIS	BROP	BQKI	LPKB	DDLO	KNPP	SDLR	KHRH	PESS
YCJC	MDAY	MCOD	KEYJ	UWCH	FJKS	CSBL	CQJH	KQLC	DRMP	JMLQ	SAAS	LJSG	LNCR

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

TLRL DVPB HRCC RPSS PCJH IIWA RCQC FSTC KHQC CLQK BIHK BFNC SOLI QAGY
RKTR AVIC JSBD SMRQ LPKG HFWB SBQP HRRD LJQB DMOJ LFHL CSAP SQAF RBFY

PQSS AHBQ BLEX
IRSR OHCQ CAMX

PROBLEM 18

What type of system does the following message suggest, and how far can you go in deciphering?

EBKDV CGJKN OVYGC KMJVP HNKSU
ERGKX BVDJK YVZDI KOMVP BFKXV
BTZKM RVXKB VEGCK MIVDO HKNFV
ZLJKX AVYTK DVBKM VOELK CNVPS
YKHVE GRKXB VCHMK BFCVE IKNVJ
XKYGV QUKCW VPARK XG

PROBLEM 19

What are the properties of the following modified example of certain pages of additive? (The size of the page has been reduced for purpose of illustration.)

00849 12593 44620 35201 96070
34165 31521 34298 58736 12184
22017 23371 73817 79408 39721
38496 64855 04629 87589 84165
79774 60802 59631 06965 03452
23015 07764 15782 31024 58967
56162 96048 87065 26741 98603
83598 49978 30159 21439 42537

PROBLEM 20

The following represents a typical page of key used by country "Z". How would you describe the property which appears?

14792 81469 57035 02479 58147
36925 14703 92580 57036 25703 etc.

PROBLEM 21

In the following series of cipher beginnings it will be noted that there is one point between successive columns through which off-set repeats do not pass as hits. (They may pick up again as continuations of hits). What simple explanation is there for this?

-7-

~~TOP SECRET~~
~~SECURITY INFORMATION~~

PWODGTZHQWHNJXHUU
OAZPWODGTZVEKHNVY
AQWTZPWODGHNIULUD
TGHZAQWTIPWCRUHNIU
KPZTGRNAZVENOEKHN
TGRNAKPTZAEEKHNDKC
PWODGTZHKXUNUYWXJ
HQWTZVJTGGNLYNNOE
OAZHQWTZVJHUUNIUL
XHQWTZVJTGLNLYNNO
ZHQWTZHQWTNLYNLXX

PROBLEM 22

The following cipher count suggest in general what type of encipherment (assuming underlying plain-text rather than code)?

A	14
B	2
C	4
D	6
E	15
F	3
G	5
H	7
I	13
J	1
K	3
L	8
M	7
N	6
O	12
P	8
Q	9
R	9
S	7
T	7
U	14
V	7
W	8
X	8
Y	16
Z	9

PROBLEM 23

The beginnings of a large body of traffic, when examined showed certain letters to have a very low frequency in certain columns. Thus, in the first column, B, N and X were either absent or low; in the second column A and U; in the third K, M, and Q; in the fourth B and Y; in the fifth E; in the sixth R and S. What type of system does this suggest?

-8-

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

PROBLEM 24

In a long cipher message a significant repeat showed up, beginning at the 103rd, and 545th, positions. In addition, a significant isomorph was observed beginning with the 16th, and 101st. positions. Although many explanations are loosely "possible", what specific idea might you be inclined to pursue?

PROBLEM 25

A certain country has been known to use a 2-part code of four digit groups, enciphered with book additive. Indicators in the past have listed which book (of 3 or 5), 2-digit page, and row and column coordinates, e.g., Book 1, Page 53, Row 6, Column 4. This starting point might be indicated by two 4-digit groups of various patterns, using the extra digits as checks, by either sum-checking or by repetition. Thus, Book, Page Units, Page Tens, and the sum of these three digits (abbreviated as BPPS) would be 1539 in the above example, and the row-columns, checked by repetition, would be 6464. This plain indicator (1539 6464) might be enciphered in various ways, often by means of a separate chart of 100 8-digit additives. The control for this additive (i.e., which of the 100 indicator additives were used) might be hidden in the message, or actually dependent upon fixed positions of cipher; for example, the first 2 digits of the 4th group might be used as such a control. Even the group count as transmitted might be used as part of the control. The enciphered indicator might appear in various pre-arranged places for given period. Occasionally a check on the ending point might also be made by inserting a second indicator towards the end of the message. The problem given involves a consistent method of enciphering within a homogeneous period. (Sorted on first group.)

0238	4058	5312	(last three)	4301	1750	1007
0475	0953	2936		1811	9317	6022
1418	8561	0393		1799	1390	2808
2387	6216	2906		0811	1218	2880
2422	5959	7178		5338	1703	3124
3757	3345	9021		2487	8430	7103
3956	4166	1268		3625	6643	4465
4703	9204	9317		5034	1709	8130
5223	2468	1117		1919	4731	1529
6790	8686	0778		9478	6023	9289
7631	9921	4487		0676	7173	9877
9217	3326	2308		4031	2802	5466
9502	2235	5518		2518	9513	3346
9598	8517	2417		1108	2062	7070

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

PROBLEM 26

This problem is related to Problem 25, with the same country and general type of indicator involved. In logging messages, a clerk noticed certain peculiar behavior of cipher digits. What phenomenon of these groups (the first 4 of each message can you detect, and how far can you go in recovering certain elements?

9224	0661	9499	1200
2715	4254	1272	7184
4134	4931	6600	2277
4139	4953	9898	5881
0021	5156	7705	3324
4090	7494	8988	9755
1900	7795	1531	9835
2901	2434	1116	5687
0590	5330	6644	0006
8216	6756	9490	1230
3178	7472	9280	9667
4920	0423	5659	0713
3521	7349	4494	3205
6734	3240	3209	2370
4172	0450	9925	4462
2817	6173	2306	2569
0059	8656	5201	0202
0769	3031	7736	1367
1691	9574	4411	9422
1800	4337	0991	0349
3018	7972	6837	1975
5967	0501	0707	7979
6172	3724	2306	2569
5253	7209	7194	3812
6486	6460	3108	3576
3576	4336	7833	9600
5343	3662	1167	1902
6424	0340	1482	4593
3335	4572	5829	4771
2901	2434	6837	1975
3281	5633	5891	5285
7102	6092	0480	6167
7005	2922	9624	6429
9980	4242	8622	0834
9129	0110	8892	1196
7202	3958	7408	4327
9215	6373	3410	9813
8833	3414	8864	8791
8396	6044	8123	1625
8964	1731	2826	4315
9907	6754	1477	4533
4050	0932	8811	8799
2901	2434	2222	6655
0053	5947	7126	3815
2401	4459	9408	1227
4549	4403	7823	9625

~~TOP SECRET~~

~~SECURITY INFORMATION~~

~~TOP SECRET~~

PROBLEM 27

It is suspected that the following two messages were enciphered on the same page of additive, and might overlap at some point. Can you prove the case?

- A. 8276 6498 6629 3081 7416 8811 3905 4578 2083 6283 1706
B. 2287 2538 9092 6255 2830 6558 5015 0685 4710 9210 8863

PROBLEM 28

The following ciphers were received a few days apart.

- A. RRFPC IGEOE NHNSR FYGOC OPOGS RANSD NEPEA MERTS TSNM EOALE
COORU OEEFI EIMAL KRNXX
B. RUORC OPOFY GTSDT MEOAL ANSDN EPPCI GIMAE EFIEG SRLKR NRTSI
EAMEE OEHEC OORRF EHNSR

PROBLEM 29

Indicator evidence not shown implies the following messages start at the same point in an additive book. Can you detect and explain a property which should yield a quick relative solution?

- A. 90219 22043 20699 14802 22127 92817 etc.
B. 67436 94200 97816 23356 96746 14372 etc.
C. 06916 50742 13709 55906 01235 83969 etc.
D. 90216 61488 26699 16994 22122 43083 etc.
E. 29114 62823 34679 83123 94020 43206 etc.

PROBLEM 30

A machine cipher is being employed which necessitates knowing the setting of 10 wheels, of length 15, 15, 15, 15, 10, 10, 17, 19, 21 and 23 respectively. The first and last few groups are likely candidates for disguising the indicator. Can you recover the entire indicating system on the following messages, the first of which has been read and definitely fixes the first four wheels (each length 15) at the 3rd, 5th, 1st and 8th setting point, respectively?

-11-

~~SECURITY INFORMATION~~

~~TOP SECRET~~

~~TOP SECRET~~

First 3 Groups

Last 3 groups

DAHFG MECDD OSHHU
 BBCDS MNMQP JRIHS
 CFAED CVUFY OINEL
 DSRXD BGGHN QQOUB
 XBBHC ERVRW ISHHC
 EOQRQ MBWIX DFJLK
 ACORA QXQPS PPFVB
 RFQXB BWWIL LIVRD
 QMHRF BACFD XVSLL
 SDZSO QBALF NNVEW
 FHMVQ FSUEY JOSSN
 MEXQS SWDSG VICOJ
 HAXCM ONTIDQ TAGXB
 GCDEQ AECHC ISHLN
 VRVAQ MBERB KSLWW

HRHDB TWLQI APRTI
 KYOIU LIRTL AMALF
 WOLKJ RQWPT RGDQS
 JWLIN TCKVT LBBJM
 ALKDJ VLLJR PKGKO
 NVTUC PNIKF AFOEV
 IISGE WRNKW IVIFC
 HGXVW KQIVL LOOEX
 VYREQ IAJLQ LWRQT
 IXWTF CTVCN ILLWQ
 CIHOP QJAGI QCDPS
 TORXJ APVIC COICB
 INZNY JWVRA NMBFI
 XBUAI BBTPI WPRJR
 BYBYE GKGWI ALLKL

PROBLEM 31

Following are three messages suspected to be enciphered at some point on the same page of additive (not necessarily level starting). Can they be made into a depth?

8978 9813 8802 2411 1387 4809 7092 1834 7736 7013 4083 8186 2246 etc.
 2091 2846 3986 8019 3468 6013 7738 4081 6613 2879 8934 8199 3768 etc.
 7768 0124 4879 0811 4036 8739 3681 6911 7083 3681 8224 2571 7698 etc.

PROBLEM 32

Following are several messages sent on one day:

1. YGMKX BESDF GBKOD GAWZD UIMLK etc.
2. FDHCJ NEGPB NVDSZ HZJDE AWDJL etc.
3. ARZDZ HMKWB DTEHI CJNDH AWZJV SMKOL etc.
4. QBNVE SZIYK EEBMF UDKHW DDIAL etc.

A message on a different day begins:

PXDAN RUJUV XSADV YUAYO VWZRQ etc.

PROBLEM 33

Following are three isomorphs in a fractionating system. Without spending any great deal of time attempting to reconstruct the elements, can you give a reasonable hypothesis as to the manner in which the cipher differs? (The next problem offers an opportunity for more complete reconstruction.)

EAXGCZKIADRSMNZIES

XYCULKHEYBNRFPKEXR

DXBAMLIWXROQPGLWDQ

PROBLEM 34

In a system similar to the above, it will be noted that the three isologs are not isomorphic. However, the messages should enable you to recover certain of the enciphering elements.

1. ANOHK RACSY LHCJP HUECQ RXMIC OVUSL IFZON
2. ALQUD RZDFY EIKBY IHRTO EJIUG HPQSE QXVOL
3. ECJYH ZTOAK LYNOP HZEPM GQQIP NQZSK TURJC

~~TOP SECRET CANOE~~

PROBLEM 35

The following are known to be enciphered indicators. Theoretically, they should show a 3-digit line number (the starting point of additive) checked in some way. Is there any property which would yield to solution of the indicators and possible overlapping?

2037	3201
2065	3245
2905	4565
4746	7458
1253	1969
4088	6424
0189	0297
3752	5896
5474	8602
0791	1243

PROBLEM 36

The following isologic beginnings imply what type of encipherment? (In your reasoning, you will probably determine the actual plain text).

SEOGVIQKKAOCX
 ZIMHLLVRGHRYP
 WNNHSPPGMFXAW
 TGOEZHQGLZWWV
 XJONTJRH FARUY
 VMCKUHNEJHQYZ
 SEMJWMUENGQVR
 RMFJREUCMYQAX

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

PROBLEM 37

What can you say about the following groups?

CVBNM GFDSA MZXCV ERTYU

IASDF XCVBN BVCXZ RTYUI

KLASD

PROBLEM 38

Following is the beginning of a message, and a resend the next day. A property can be noted and with sufficient background on a particular phase of communications an even more specific phenomena can be explained.

A. EQEU5 DEQBK 8DA5S

8FUXY WUJTU EFQBK

B. OQ7LG D7PBC V34G9

8FIMY WURHI ENPOC

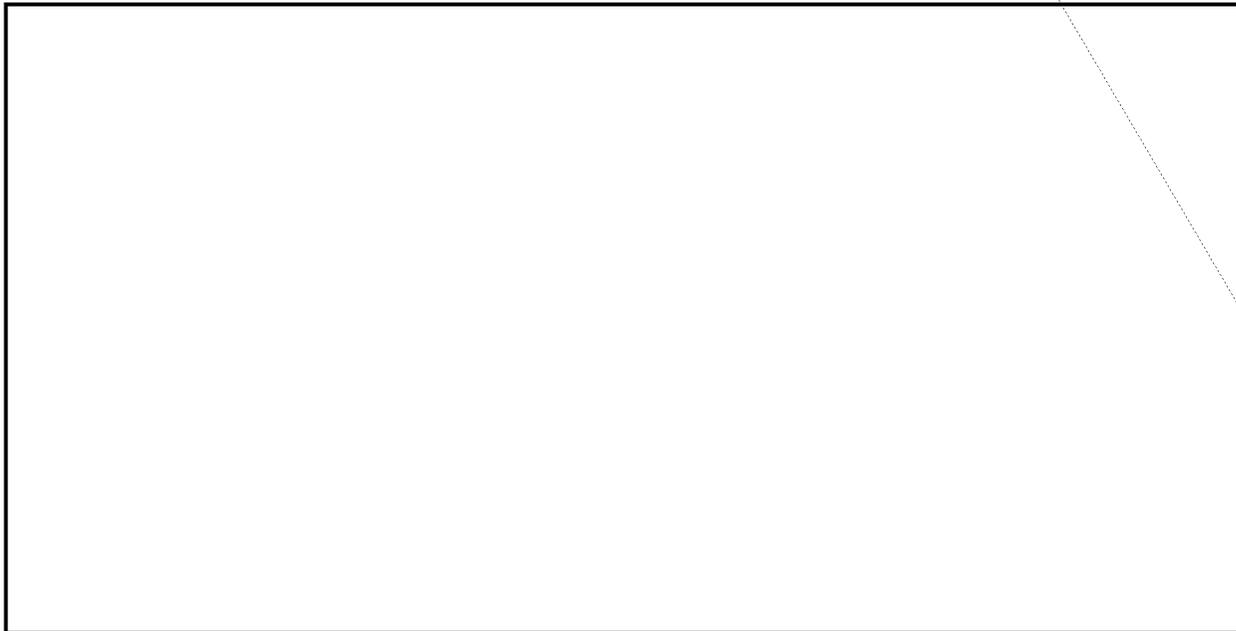
~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

COMMENTS ON FOREGOING PROBLEMS

PL 86-36/50 USC 3605
EO 3.3(h) (2)

PROBLEM 1



PROBLEM 2

One of the more common methods of indicator encipherment involves the subtraction of one group from another. In this case the second group subtracted from the fourth in sequent messages yields the interesting series.

53901
55902
69903
63905
75906
79907

At first blush it might appear that the last three digits of this difference in themselves form the only startling phenomena, and perhaps imply the starting point or pad name of successive encipherments. However, the progression of the first two digits when noted and analyzed, shows that the two digit date must be subtracted from the fourth group (with carrying) before the second group is applied (without carrying) to form a uniform series.

4th Group	4th Group Less date	2nd Group	Indicator
55079	54079	02178	52901
75319	72319	20417	52902
20132	13132	61239	52903 etc.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

PROBLEM 3

This is typical of the specialized problems which are obvious to those experienced in certain phases of the work, and not necessarily meaningful to others. The limitations of the first six columns are such that there is a point in the alphabet beyond which no cipher letter appears -- in the first column this "absence" area is R to Z, in the second column T to Z, etc. From the positive viewpoint, the highest letter used in these columns is Q, S, U, W, Y, (and Z) respectively. In terms of numbers, the limitations 17, 19, 21, 23, 25 and 26 would suggest Hagelin indicators to anyone who has been exposed to the machine.

PROBLEM 4



PROBLEM 5

A simple example of a FIBONACCI series, (this type of key might be used by an agent for example, who can remember a short stretch of key and generate a much longer series from it), in this case, the first and second digits are summed to create the eighth, the second and third to create the ninth, etc.

-17-

PL 86-36/50 USC 3605 •
EO 3.3(h) (2)

~~TOP SECRET CANOE~~

A more complex Fibonacci series might be:

12955263499144723990

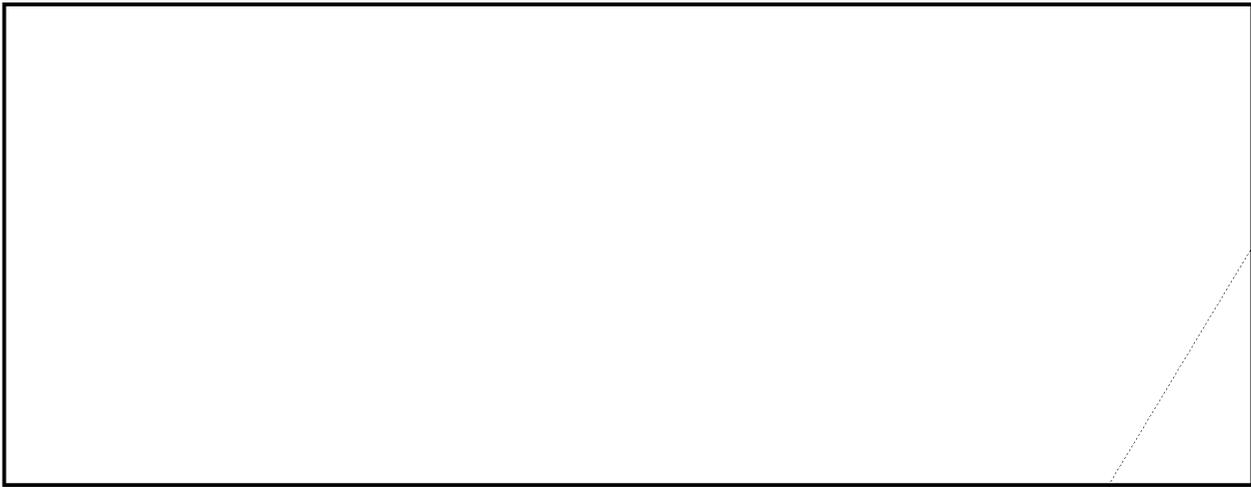
Can you analyze it?

In actual cases, such Fibonacci usage as has been determined has been oftentimes much more complex; sometimes the user will go through several steps of combination of different series, using a final version which exhibits no properties, yet is based on two or more series (unused) which do have properties.

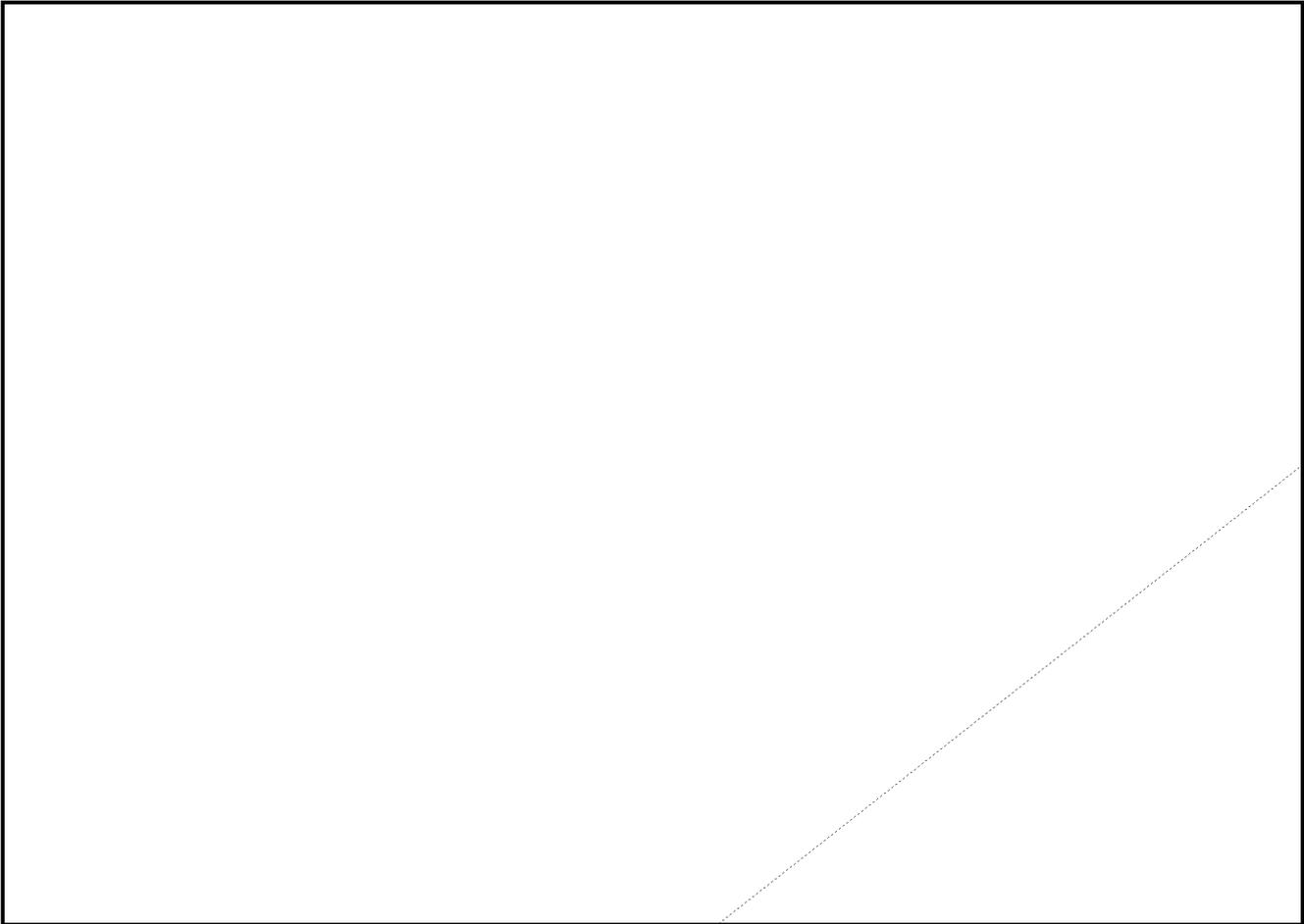
PL 86-36/50 USC 3605
EO 3.3(h)(2)

PROBLEM 6



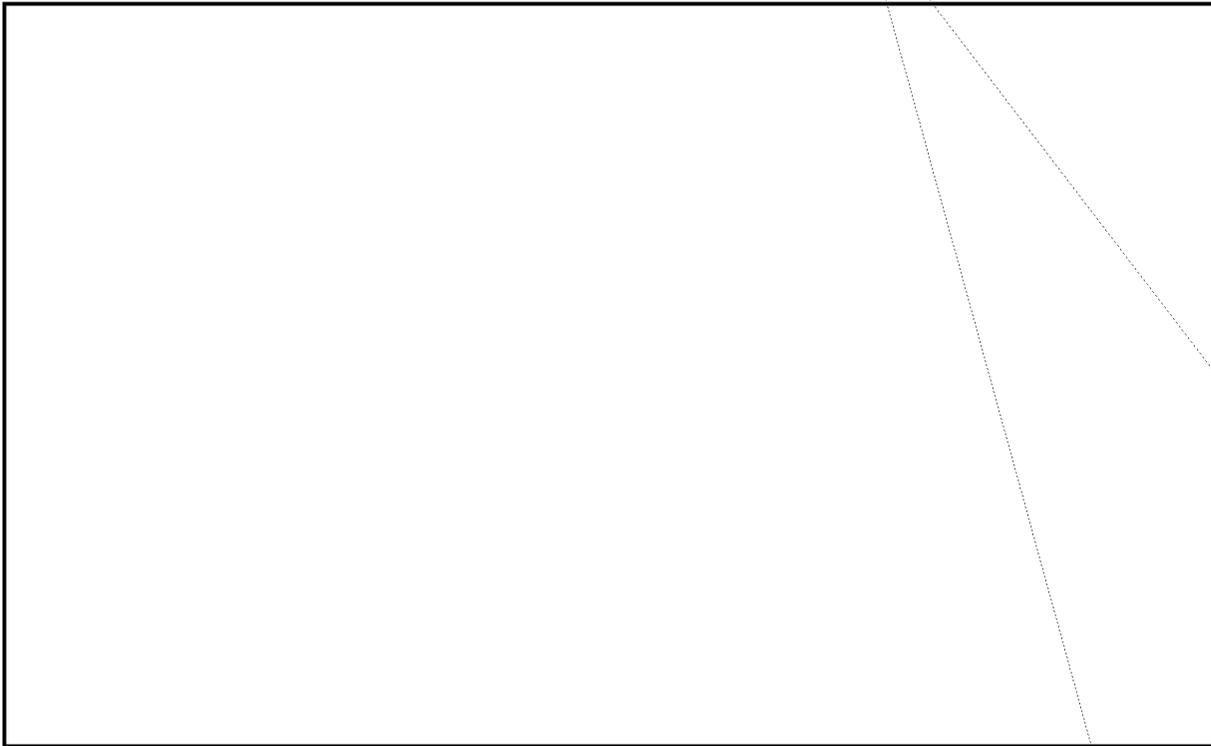


PROBLEM 7

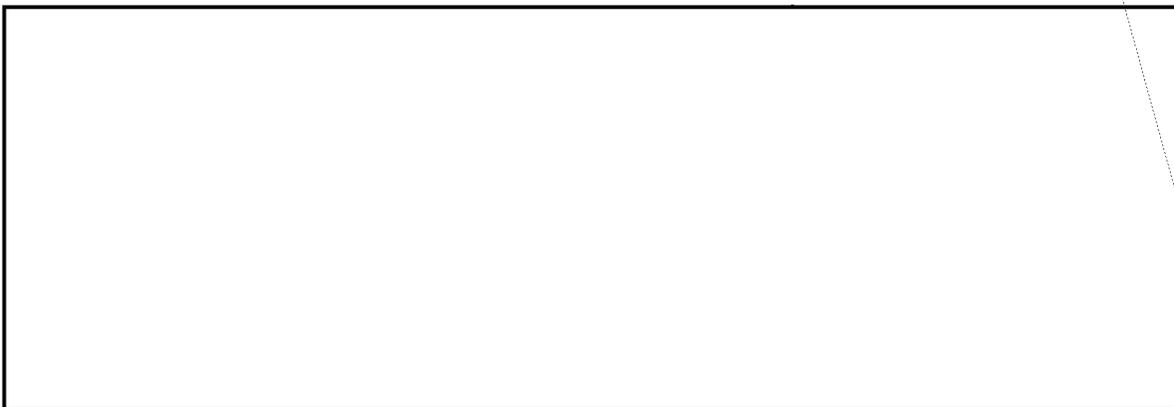


PL 86-36/50 USC 3605
EO 3.3(h) (2)

PROBLEM 8



PROBLEM 9



PROBLEM 10

The difference between the two ciphers given is:

000005599884400344678 etc.

Those experienced with conventions of plain numbers in some monome-dimome systems would spot this typical difference -- in many such systems the number "1" is indicated in plain as a double digit "11", "2" as "22", etc. (Some systems use a triple check - 111, 222, etc.)

When a number in one message falls over a number in a message in depth, the difference is characteristic. Of course, by itself, this will not "read" the depth -- other tools are necessary for ultimate solution, but an understanding of the basic problem may be obtained.

PROBLEM 11

This is a simplified example of the indicator usage of the Japanese Military Attache system used early in the war.

The critical messages to note are:

AB	CR	(BA)	(ZT)...	(KP)	AB	CS	(OL)
AB	ZL	(BX)	(JS)...	(YQ)	AC	RZ	(OK)
AC	CN	(DG)	(CH)...	(XT)	AB	KZ	(RD)
AD	OV	(ML)	(EE)...	(NG)	AD	OV	(LE)

Among the considerations would be the possibility that a diagraphic page designation is made at the beginning of the message (with possibly a different diagraph being used as a control) and also that the ending point of key is checked by an indicator similarly enciphered by a different control, placed at the end of the message. Perhaps row and column coordinates are included in the indicator as well.

Thus the AD OV - AD OV might imply a message ended on the same page as it began, and the control happened by chance to be the same diagraph. (Which is control and which cipher remains to be seen). The AB R - AB CS occurrence might lead to the hypothesis that here the ending was on a consecutive page from the beginning, the control being AB and the enciphered pages CR and CS. This might imply normal alphabets were used to encipher the page designation. If the chain AB ZL - AC RZ, AC CN - AB KZ is checked the following relative solution might be obtained. (Only "page" encipherment can be thus quickly confirmed, if the indicator is "PP RC" the row-column digraph will probably "come out in the wash".)

Control	AB	Control	AC
Key	AA	Key	SO
Starting Page	YK	Ending Page	YK
Cipher	ZL	Cipher	RZ
Control	AC	Control	AB
Key	SO	Key	AA
Starting Page	JY	Ending Page	JY
Cipher	CN	Cipher	KZ

(It is of course appreciated that ZL from RZ gives the same difference as KZ from CN).

In the actual system involved, the solution of indicator enabled the complete reading of the system (which involved an underlying digraphic code chart) and, more important the solution of the simple version using normal alphabets enabled the more complex solution of subsequent periods using mixed components which by themselves could have offered great obstacles.

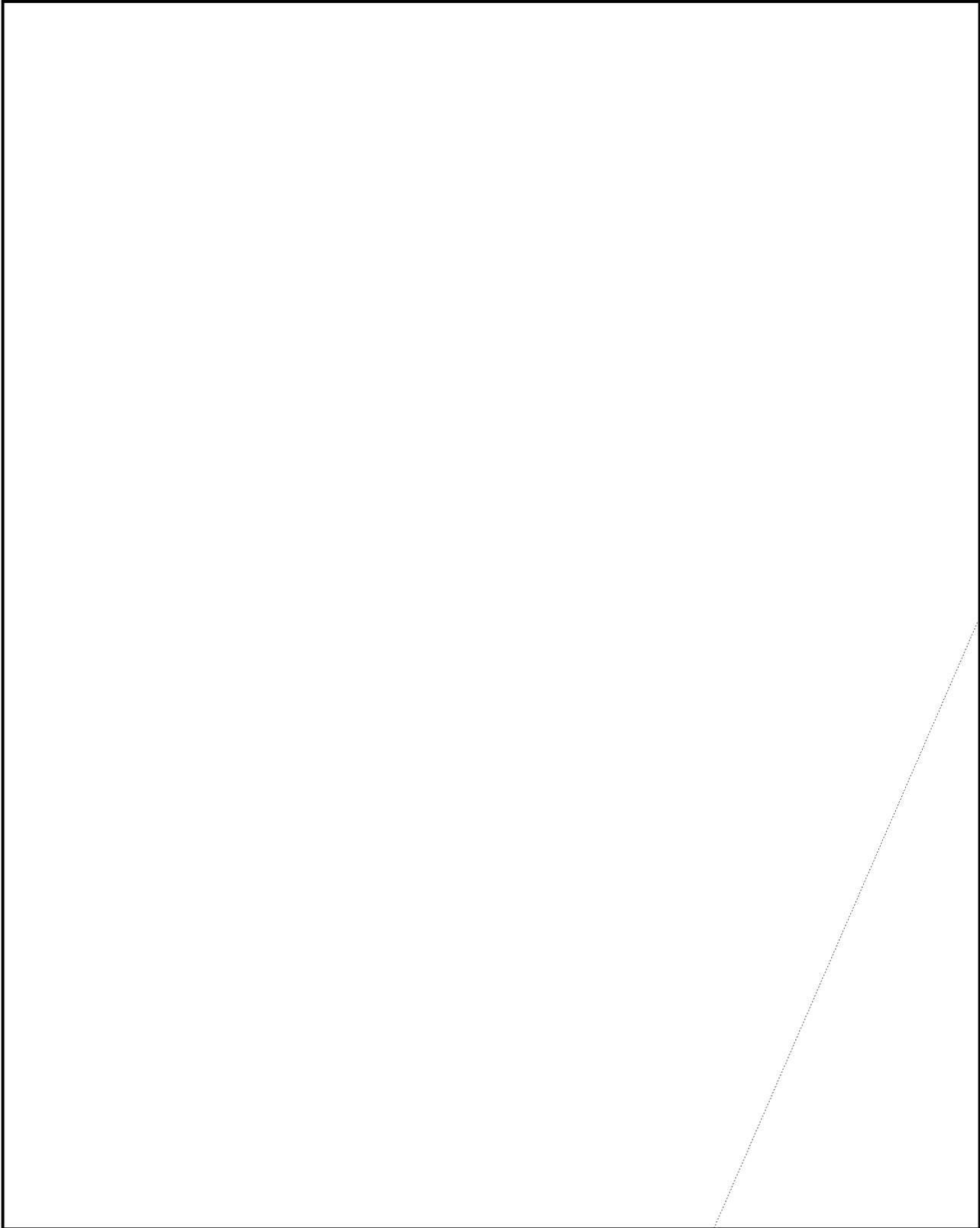
The importance of continuity, and getting into the simpler versions before they become impossibly complex, cannot be over-emphasized.

PROBLEM 12



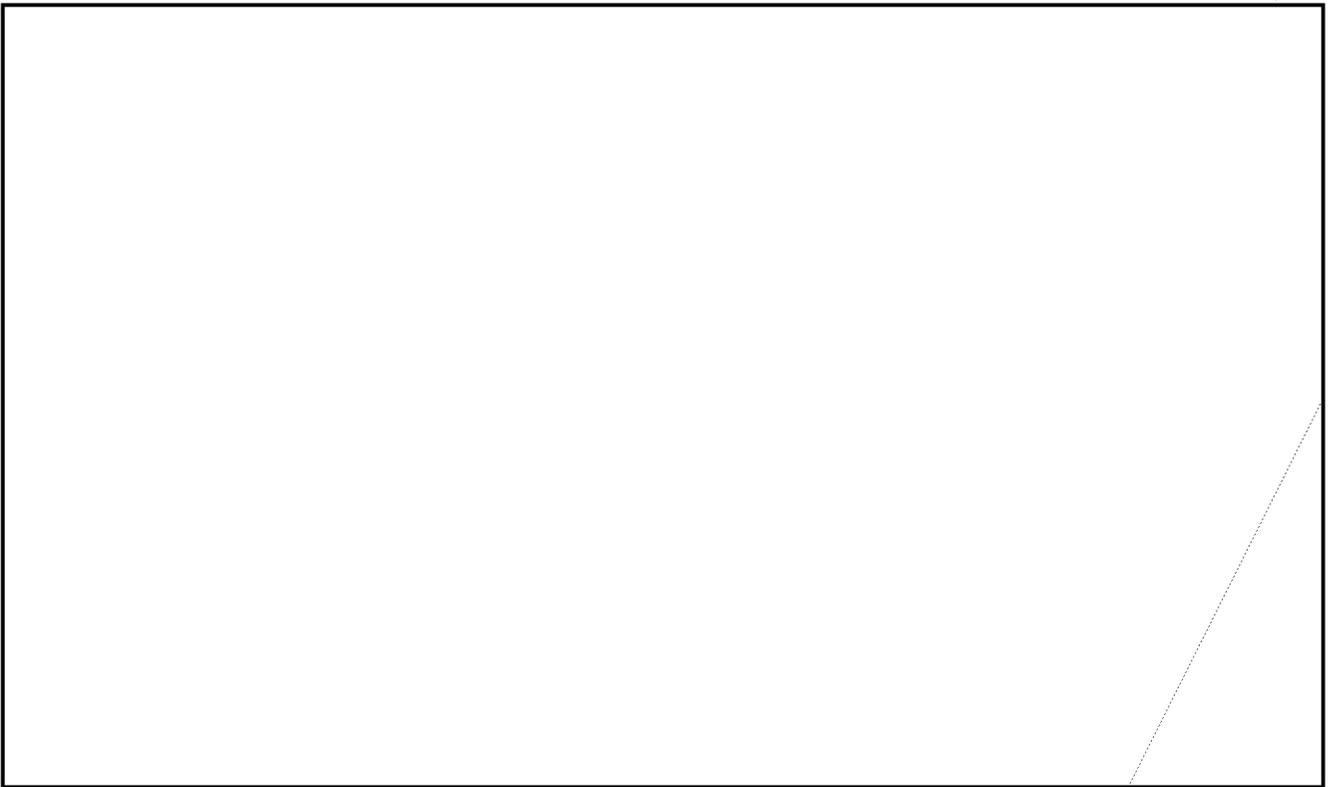
PROBLEM 13



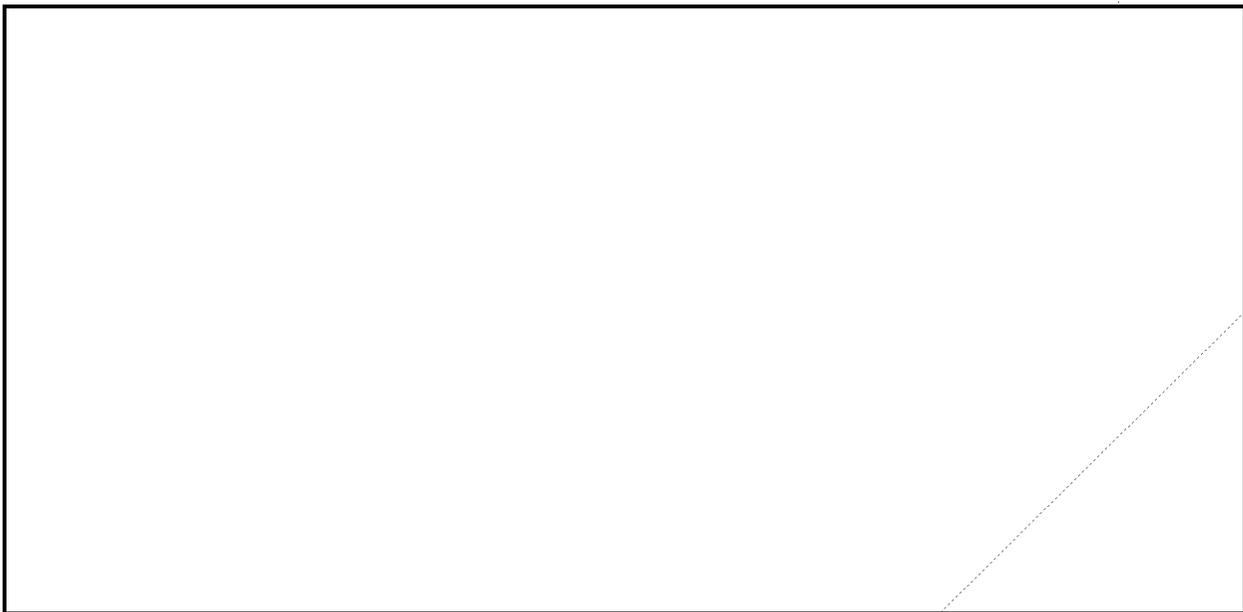


~~TOP SECRET CANOE~~

PROBLEM 14



PROBLEM 15



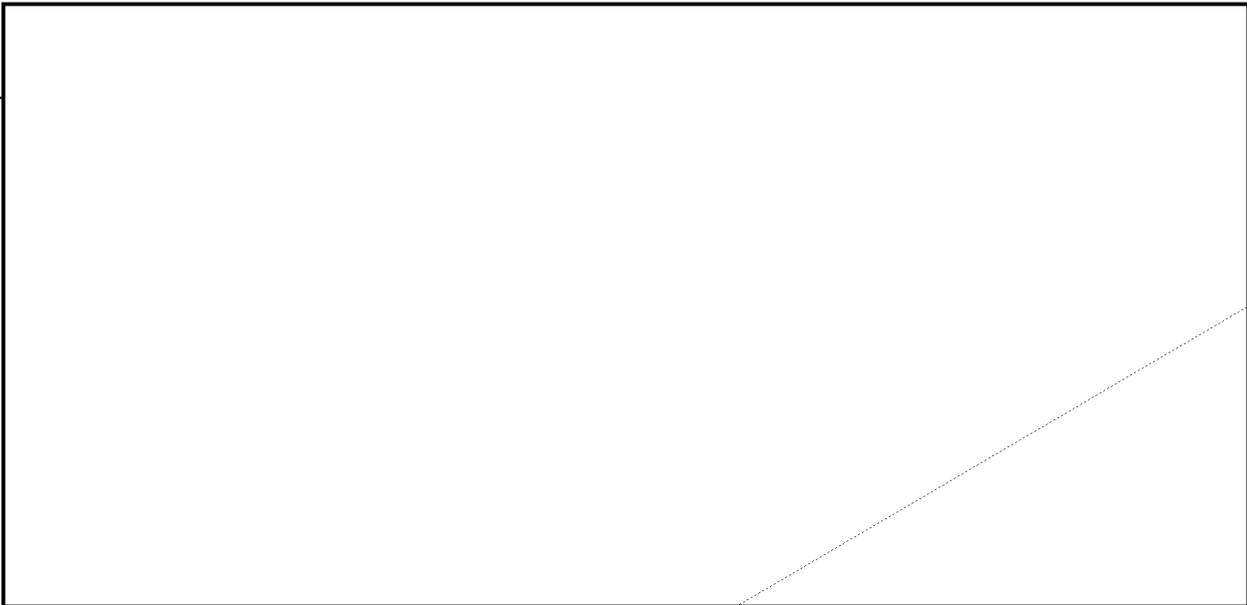
-24-

PL 86-36/50 USC 3605
EO 3.3(h)(2)

~~TOP SECRET CANOE~~

It will be noted that the relationship between the first digits' of the first two groups listed is constant -- 0 to 9, 1 to 8, 2 to 4, etc. This is a decimation of the actual sequence used on each wheel. Knowing the first two keys are in sequent order, the true sequence 1528043976 is obtained even more simply. The reader can certainly work out the rules of motion from this point.

PROBLEM 16



PL 86-36/50 USC 3605
EO 3.3(h)(2)

PROBLEM 17

This problem is not too simple to analyze. Possibly few readers will spot the cycle of 5, but (discounting the first few letters, identically enciphered before a mistake caused the shifting of one message relationship) there is a completely isomorphic representation of 5 alphabets here.

Thus, starting with the 9th letter, indexing the lower message in terms of the upper, on a cycle of 5 (with a minimum of garbles) shows:

Upper
Beat

	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
1		C	D	R	M		H	F		K	N	A		L	Q	S	T		W		Y					
2		C	P	I	N		H	M		L	M	D		E	Q	R	T	S	B	U		W	X			
3	B	C	T		H		J	A	K	L	R		P	M	Q	D	S		O					Y		
4		C	A		D	F	G		H	J	L			O	Q	S	R		T					Y		
5	O	L	B	D		S		G	H	J	K	A	M				C	Q	R	U	V	W		Y		

If one takes the trouble to solve these messages (as a 5 wide polyalphabetic substitution) one will note that the same 5 alphabets are used in each, but one of them 'dropped a stitch'. Many tricks can be used in recovery, as one quickly gets the impression that the sequences are based on keywords (accounting for the largely undisturbed relationships in certain parts of the alphabet).

EO 3.3(h)(2)
PL 86-36/50 USC 3605

PROBLEM 18

This is based on a German system, which used a dictionary code, sending page and line number of the desired word (using a standard pocket dictionary). Instead of sending figures, however, the letters DURCHWALKE were substituted for 1-0, with N used as a separator between page and line and between successive combinations. Unnecessary digits were omitted (page 1 line 1 sent NDNDN, for example).

In the problem given, instead of using a keyword (with only 11 letters appearing in the text) the maker has used a simple substitution with variants, so that each digit can be portrayed by two or three letters at different times. The use of the variants is not random, however. One notes that every few letters either a V or K is present -- with never more than three intervening letters.

Also the order KVKVKVK is almost invariable. If these two letters are the separators, an eleven-wide box is suggested, and a lucky guess as to the order (based on the 11-22 relationship of K to V) would pay off. At worst, the limitations afforded by the fact that not all digits appear as beginning page or line numbers would lead to a partial solution.

PROBLEM 19

The property to be noted here is one of distribution -- within the first groups (the left hand column of 5-digit additive) there are exactly four 0's, four 1's, four 2's, etc. The same property holds for each of the other four columns.

~~TOP SECRET CANOE~~

PROBLEM 20



PROBLEM 21

This illustrates an extended monoalphabetic substitution, wherein the key is constant for 10 letters, then changes to a different key. Within these stretches everything is monoalphabetic, so off-set hits occur, but disappear when the 'border' is reached and reappear only after both off-sets get into the same 'territory' again. The irregular interval between partial hits (WIZVJTGLNIYN and WIZHQWTNIYN) is an example of a very simple thing which can be temporarily perplexing when one knows the overall messages do not involve either monoalphabetic or single-position cyclic keys.

PL 86-36/50 USC 3605
EO 3.3(h) (2)

PROBLEM 22

This is based on the properties of the original Japanese machines (Red) which preceded Purple, wherein vowels were substituted for vowels, and consonants for consonants (through a rather complex substitution process). The result at first blush bears a resemblance to transposition, but the flatness of course precludes such a theory.

PROBLEM 23

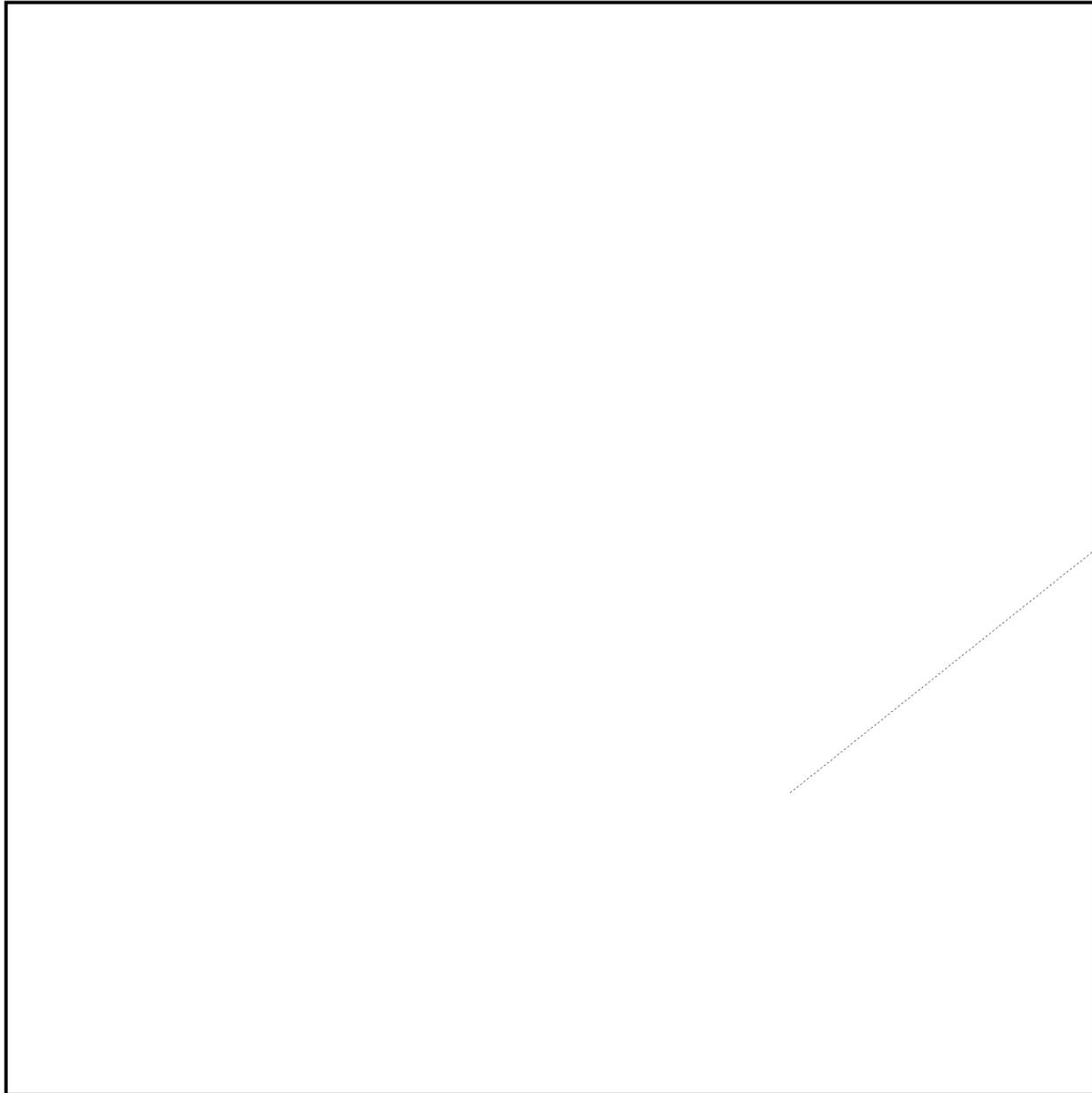
Those familiar with Enigma might be expected to quickly spot the word NUMBER as a cliché, due to the non-crashing features of such reciprocal systems, where a letter can not be enciphered as itself. Overall counts of such traffic (which includes certain strip systems as well as machines) should show a reverse curve of the normal frequency - expectations of plain text -- E would be low in the cipher, for instance.

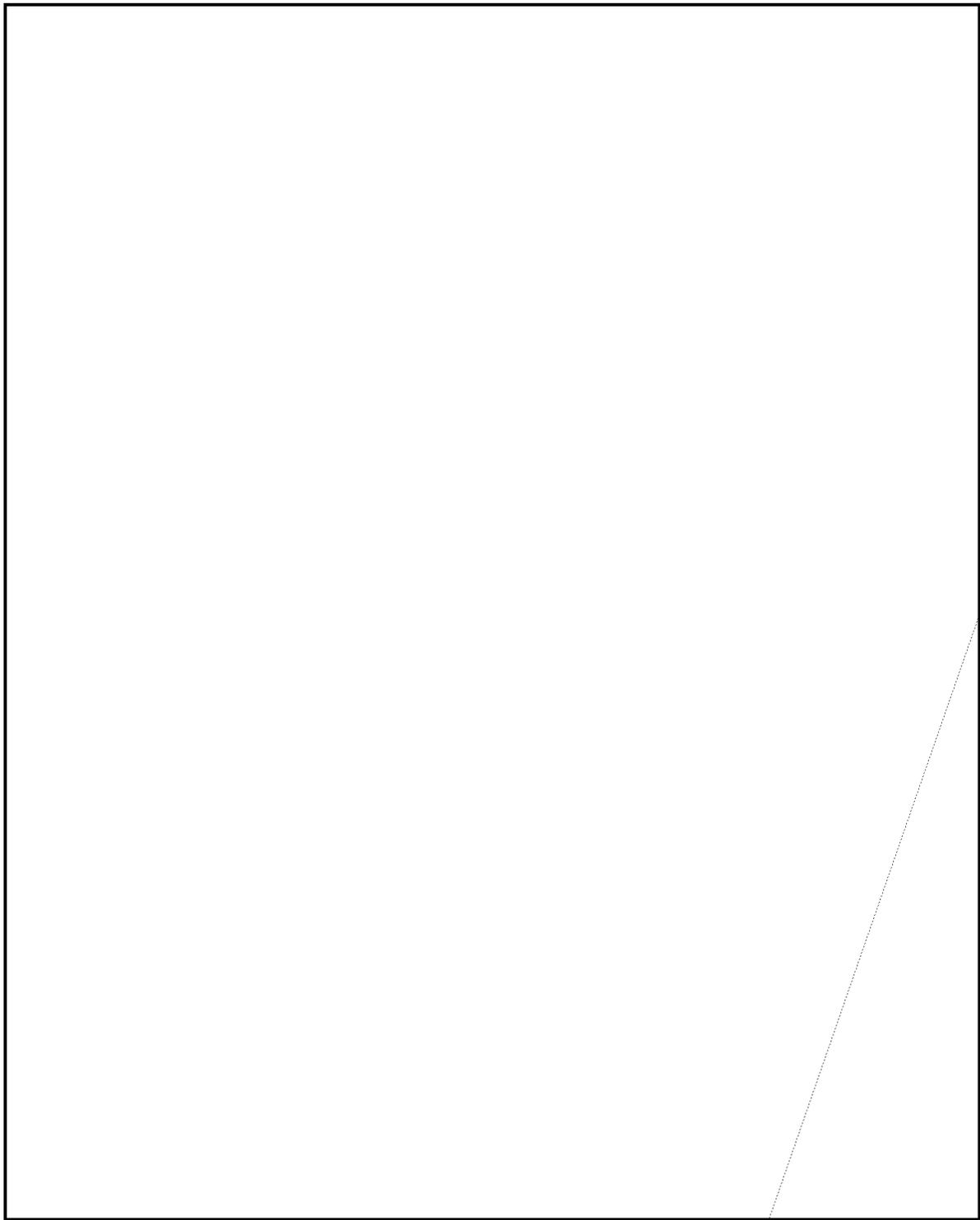
PROBLEM 24

~~TOP SECRET CANOE~~



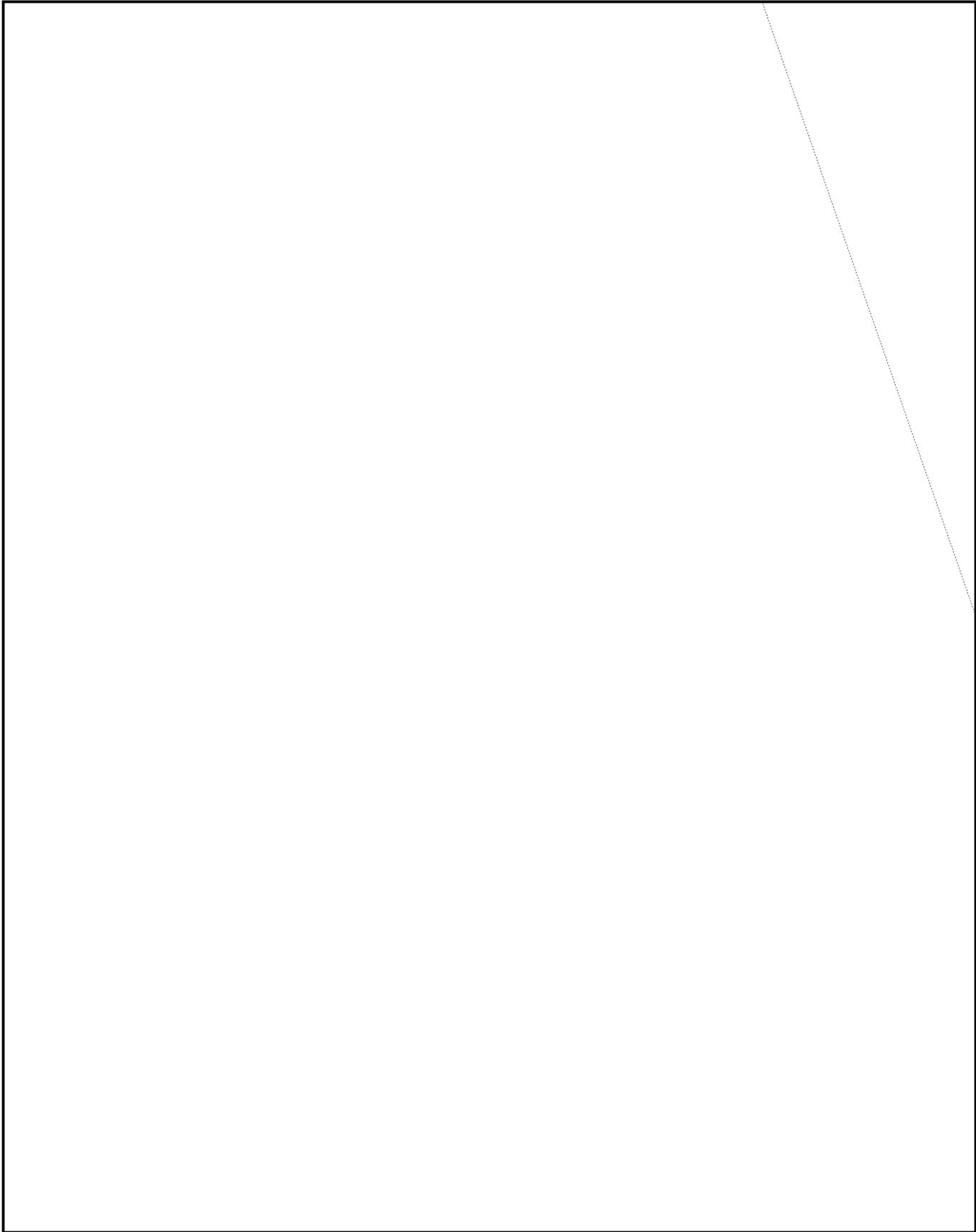
PROBLEM 25



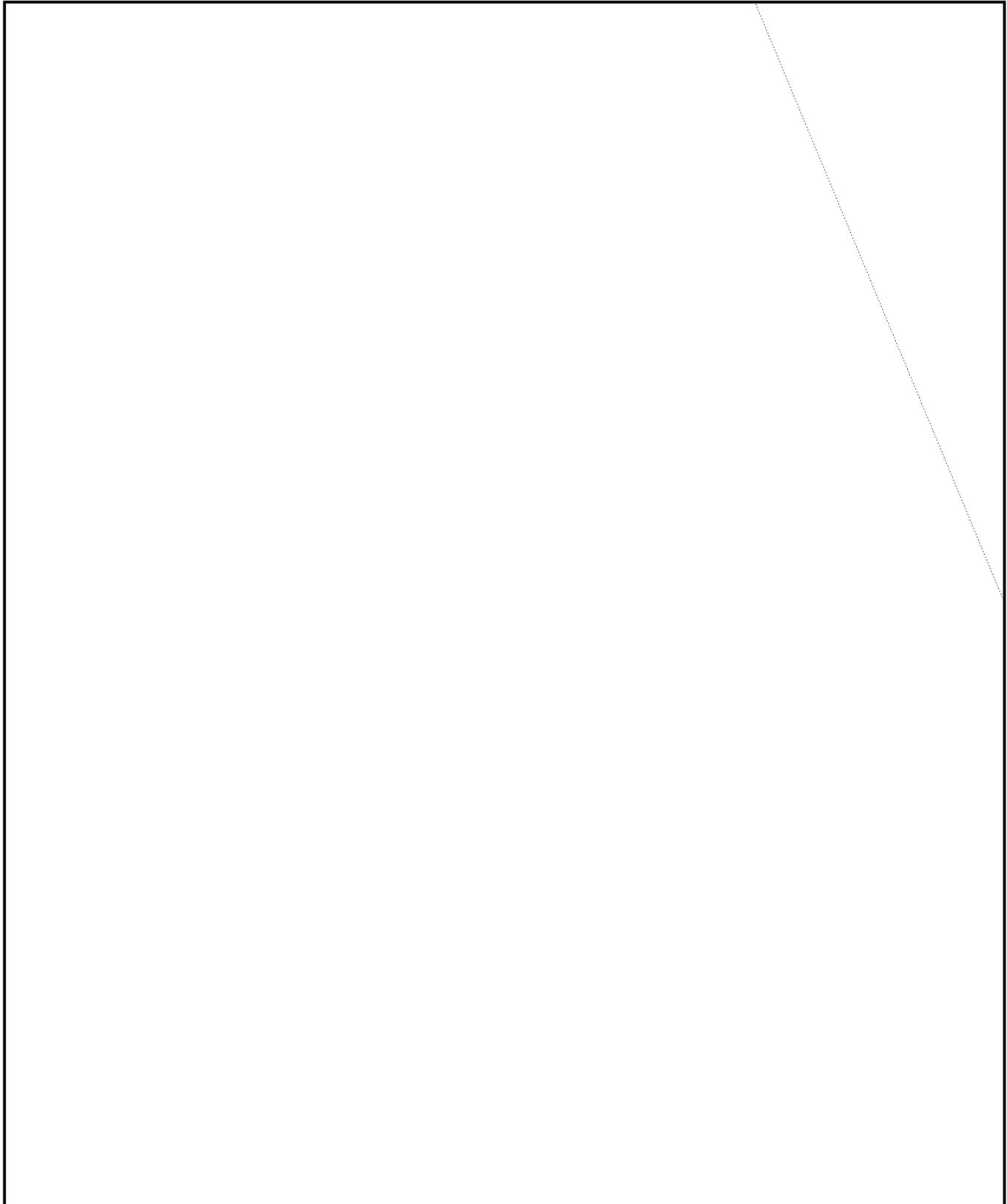


EO 3.3(h) (2)
PL 86-36/50 USC 3605

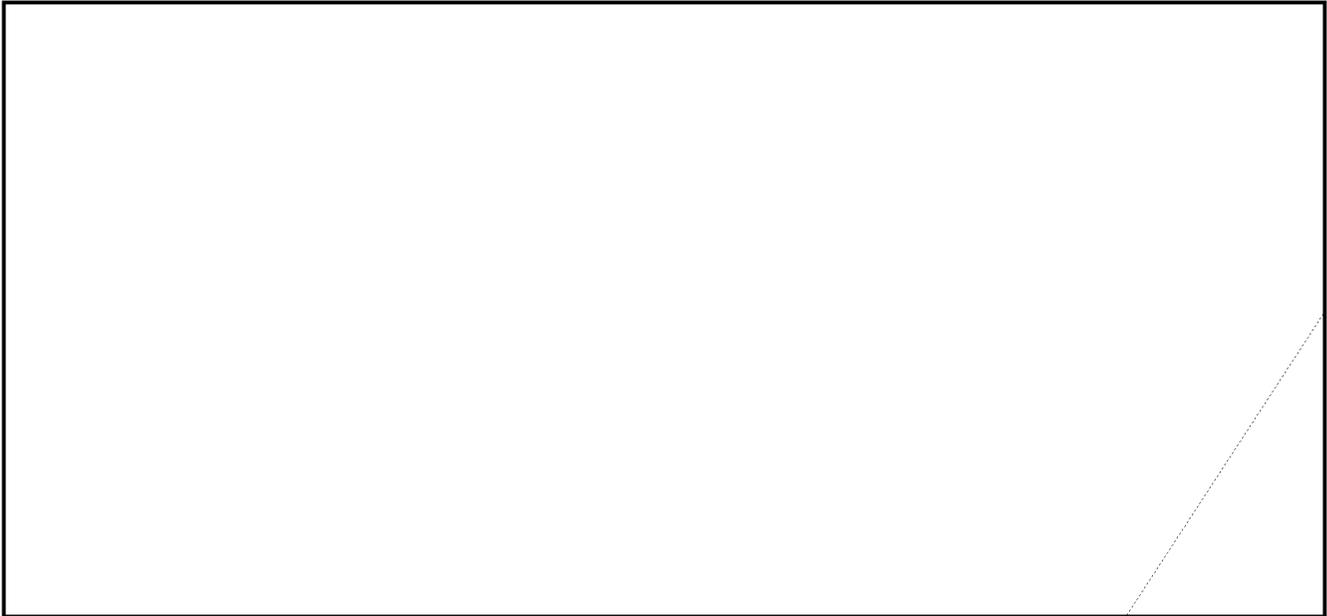
EO 3.3(h)(2)
PL 86-36/50 USC 3605



EO 3.3(h)(2)
PL 86-36/50 USC 3605



PROBLEM 27

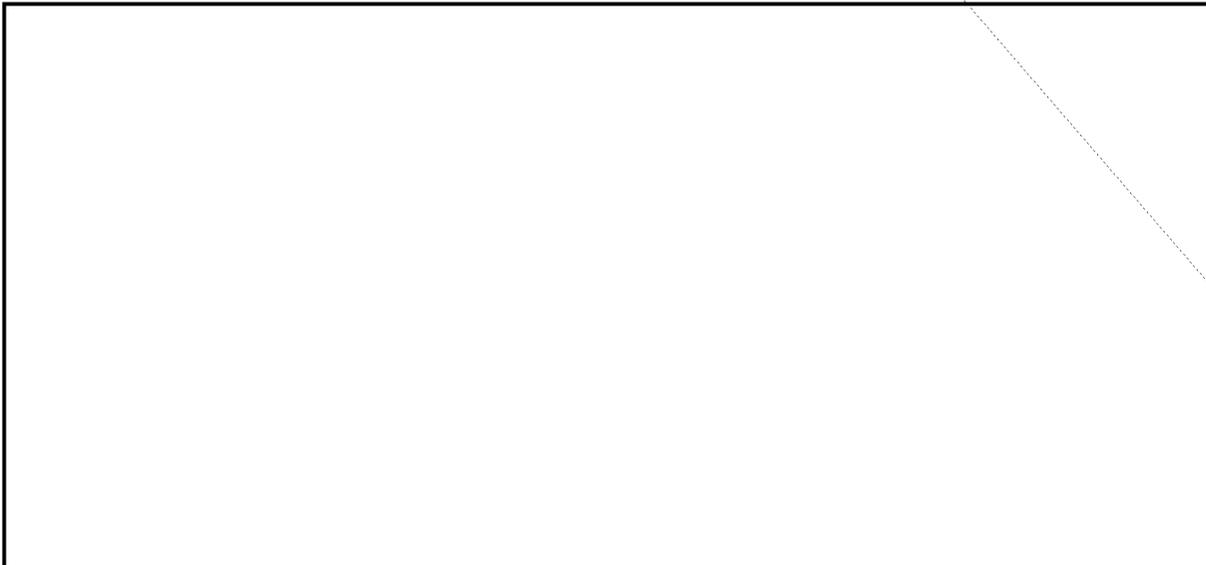


PROBLEM 28

This will probably be quickly spotted as a literal transposition, but perhaps not all readers will as quickly notice the properties which make solution simple. With the exception of a few letters (which differ between the messages, and imply a different word appearing within the two versions) the first message can be broken into segments of 3 or 4 letters, each segment then being matched with an identical segment in the second message. Assuming almost identical text, but different column as transposition keys, the plain is easily recoverable.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

PROBLEM 29



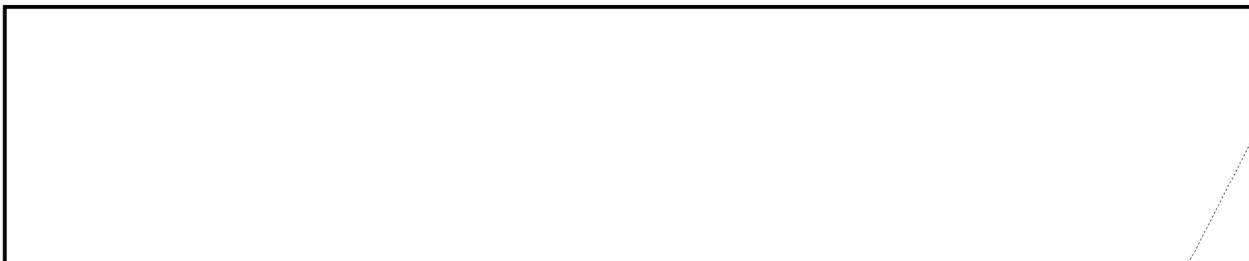
(Notice 9021 - 9220 and 6743 - 6942)

EO 3.3(h) (2)
PL 86-36/50 USC 3605

PROBLEM 30



PROBLEM 31



PROBLEM 32

First of all, this example must be studied on the cut of 4-letter groups.

Consider:

- 1. YGMK XBES DFGB KODG
- 2. FDHC JNEG
- 3. ARZD ZHMK WBDT EHC JNDH

PL 86-36/50 USC 3605
EO 3.3(h) (2)

Note that there is a close relationship (never more than 2 letters removed) between these messages at this point. Other such relationships show no evidence of additive, as "hits" and "near misses" come at all points (but stay on the beat of 4). It is seen that relationships fall into classes of 2 and 3 letters at a time in alphabetical order, and the clusters are:

A-C, G-I, J-L, M-O, P-R, ST, UV, WX, and YZ

If one assumes such a conversion table (with variants) as:

O12 etc.
ADG
BEH
CFI

The texts begin:

1. 9243 8016 1120 etc.
2. 1120 3412
3. 0591 9243
4. 5047 1692

One can solve the next days message on the square

O12 etc.
RUX
SVY
TWZ

which yields:

9243 8016 1120 etc.

PROBLEM 33

In order for the true isomorphs to show through, there should be either a constant method of enciphering the elements of fractionation (i.e. the substitution on rows and/or columns would be constant, but different between messages) or, if constantly changing (as by running keys, moving commutators, etc.) the keys or motion must be the same (or isomorphic in the case of keys). In other words, different settings plus different motion of at least one commutator would probably not cause true isomorphism, but different settings and the same motion might. Disregarding plain text and frequency relationships, no motion and the same motion are indistinguishable in their cipher isomorphic phenomena. With enough data, a relative square could be obtained in the type of problem given if rows are constant and columns are isomorphic, or vice versa.

One could also build up a distorted type of square if, without being identical, the rows and/or columns are slides of each other (12345 as coordinates of one message going to 23451 in the other). Random isomorphism on both sides simultaneously (12345 equivalent to 15243, for example) would be much more difficult to untangle.

It is seen on the problem given that all 3 messages cannot be treated simultaneously as being constant on the same element; for the chains built up would be too large. (X,C,L,E,D,M,F,P etc would all have to be in the same row or column!) However, indexing and chaining the relationships of messages 1 to 2, 1 to 3, and 2 to 3 yields:

1-2	1-3	2-3
CXLIE	ROED	XYD
AY	XAGBN	RQCB
GU	PMC	UA
KZH	ZL	LKM
DB	KIW	HI
NPRS	SQ	ON
FM		EW
		FPG

This implies that CXLIE might all be on the same row, or the same column, or perhaps diagonally related if the coordinates are slide between messages. By the same token XAGBN, and independently RQCB are related in some fashion. A square can be made which will satisfy all these conditions. However, if we are fortunate enough to have a simple slide of coordinates (or identity) in all cases of, a much simpler solution is possible. In such a case, going back to the messages, E is next to X, X is next to C, C is next to L, etc. (Or at worst the relationships are on an adjacent diagonal).

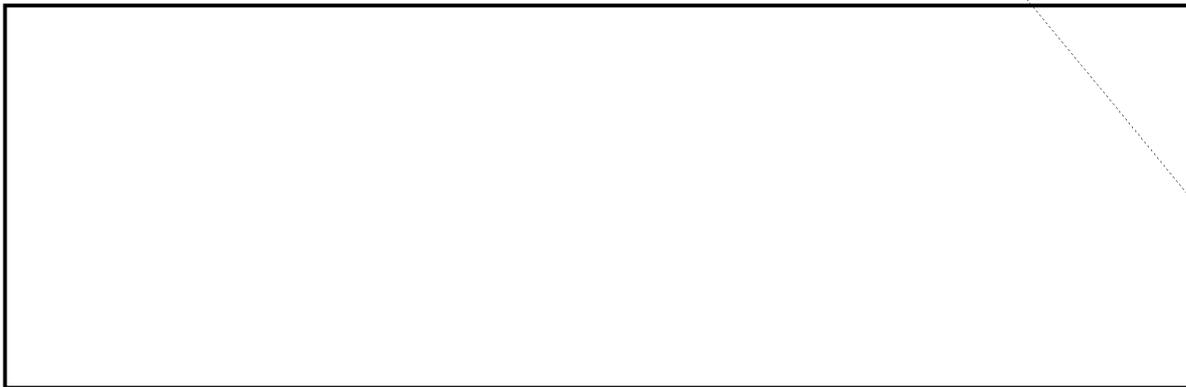
In this case, we must be careful how we associate the letters, chaining them exactly:

IEXCL	EDRO	YXD
AY	NGAXB	CERQ
GU	CMP	UA
ZKH	ZL	KIM
DB	KIW	HI
SRNP	SQ	EW
MF		NO
		FPG

The square falls into place almost automatically now.

PL 86-36/50 USC 3605
EO 3.3(h) (2)

PROBLEM 34





PROBLEM 35

PL 86-36/50 USC 3605
EO 3.3(h) (2)



PROBLEM 37



PROBLEM 38



PROBLEM 36

Readers of Jules Verne will recognize this simple polyalphabetic cipher, using digital key -- only 10 possible ciphers for any plain letter, of course. The lowest form (counting on a normal alphabet) in each column should represent plain plus 0 or 1 usually, and the cliché stands out like the proverbial sore thumb.

PL 86-36/50 USC 3605
EQ 3.3(h)(2)