Some Principles of Cryptographic Security

BY BRIGADIER JOHN H. TILTMAN

~~*Top Secret Umbra*~~

The author derives some general principles of cryptographic security as seen from the two opposite points of view of the designer of a cipher system and of the cryptanalyst. He illustrates the principles by examples from his own experience, emphasizing the weaknesses of design and usage which have led to the solution of a number of systems.

I have attempted in the following paper to derive some general principles of cryptographic security, looking at it from the two opposite points of view of the designer of a cipher system and the cryptanalyst. I have found it impossible to arrange these principles in any logical order and have decided to express them in the form of disconnected aphorisms and to illustrate them from my own experience. Much of what I have to say will seem rather obvious, and I do not imagine that any of it will be of value to the designer of a cipher system today, but I hope that some of it may serve to stimulate the imagination of cryptanalysts facing complex but potentially vulnerable systems (such as are still used in many countries). In any case, the principles should not be taken too seriously. They should be regarded as a loose framework for the classification of weaknesses of design and usage which have led to the solution of a number of systems in the analysis of which I have taken part.

Except in the rather special case of the German on-line teleprinter machine known to us as "TUNNY," I have omitted altogether reference to machines and modern computer methods of which I have no experience (e.g., Hagelin systems, on which I have never worked, and the ENIGMA machine on which I worked very little and then only on the commercial model without the additional security attachments belonging to its military usage).

A. A cipher system has to be a compromise between security and practicability. It should be designed specifically for the task it has to perform. Anyone can produce a secure cipher, e.g., one-time pads, but OTP becomes impractical when the system has to be used for frequent intercommunication among a number of holders.

B. The responsibility for the security of a system has to be taken completely out of the hands of the cipher operator, who should virtually be told how to encrypt each message. Further, a system has to be proof as far as possible against attempts by holders to circumvent the instructions through laziness, i.e., the instructions should take account of this possibility.

C. A system is as strong as its weakest link. Cryptanalysts make their living out of the sloppy thinking and enthusiastic over-ingenuity of designers of cipher systems. When the security of a system is assessed in advance, the possible damage due to compromise of part of the cryptographic materials, e.g., the codebook, has to be taken into account.

D. All transposition systems are dangerous. If they are overcomplicated, they breed mistakes leading to [redacted] and generally they are vulnerable to unpredictable special cases.

E. The usage of a system should be periodically monitored to ensure that it is not overloaded. In some cases, as frequently in the case of field ciphers and authentication systems, long-term security is not essential—a reasonable minimum time period can be assessed, after which the information will be of no use to an enemy.

F. Many a system has been ruined by reliance for security on variant substitution units. They are generally used quite irregularly, or even worse, sometimes the issuing authority has been known to instruct the holders to use them in regular cyclic order.

[redacted]

I. An otherwise secure system may be ruined by an inadequate indicating system.

J. It may need only [redacted] to ruin the security of an otherwise sound system.

K. One-time pads do not have to be absolutely random, just unpredictable. Extreme examples of predictable pads are [redacted] generation. Cryptanalysts have frequently wasted a great

deal of time trying to read messages [redacted] on the strength of nonrandom key bias and have got out of their effort no more than they have put in. But there are shades of nonrandomness, e.g., [redacted] where many messages were read [redacted] by making use of optimum key values at regular intervals. Running key produced by substitution from passages of book text is a special case; it really provides a [redacted] as sense can be made both in the key and intermediate text.

L. Ciphers have to be specially designed for transmission of [redacted] reports. Generally speaking, adequate security can be economically achieved by the use of OTP, a separate pad for each reporter, of which each of the recipients (more often than not one only) holds a copy. Here there is no intercommunication between holders to be catered for.

The following examples of (a) cipher designs and (b) successful solutions, in which I have tried to place the emphasis on the weaknesses which have led to solution, are loosely related to the principles stated above by a letter in square brackets referring to the appropriate paragraph.

I shall be grateful for any comment or criticism which might make this attempt at classification of system defects more useful. Many other examples could be cited in a later issue of the *Journal* if the endeavor in this form is considered to be worthwhile.

As examples of systems aiming at a high degree of security, but exhibiting grave weaknesses, I give pride of place to [redacted] I have described this system rather fully because, although it was the subject of an excellent wrap-up report, I feel that not enough emphasis was placed on the flaws which led to its complete solution. It has not previously been described in the *Journal*.

[redacted]

Before the introduction of the system, the commercial firms had been accustomed to use large commercial codebooks containing code equivalents for a very large number of Chinese-Japanese characters, compounds of characters and phrases, etc., and it must have been a severe blow to them when they were forced to draft their telegrams in syllabic form.

The Roman equivalents for the kana syllables which had to be used for the plain-language components of their telegrams were:

a	*i*	*u*	*e*	*o*
ka	*ki*	*ku*	*ke*	*ko*
sa	*si*	*su*	*se*	*so*
ta	*ti*	*tu*	*te*	*to*
na	*ni*	*nu*	*ne*	*no*
ha	*hi*	*hu*	*he*	*ho*
ma	*mi*	*mu*	*me*	*mo*
ya		*yu*		*yo*
ra	*ri*	*ru*	*re*	*ro*
wa				
n				

To these were added the ten digits and —, " and °, 58 plain-language units in all. " was used for "nigori," i.e., the sign which converts *k, s, t* and *h* to *g, z, d* and *b*. ° was used for "han nigori," which converts *h* to *p*. For beginning and ending of parentheses " was used doubled.

For the cipher units the syllables were conventionally converted to digraphs which appeared in the cryptographic materials in the following order:

AA II UU EE OO KA KI KU KE KO
SA SI SU SE SO TA TI TU TE TO
NA NI NU NE NO HA HI HU HE HO
MA MI MU ME MO YA YU YO RA RI
RU RE RO WA WE WI WO WN QC QD
QF QG QL QP QV QX QB QZ

UO was used as a null to fill the final group of a message where necessary.

For the sake of clarity throughout this description, the plain-language units are printed in italics and the cipher units in capitals.

The cryptographic materials consisted of:

(a) Thirty grilles 11 × 11, i.e., 121 cells of which 21 were blank, and

(b) a substitution rectangle 20 × 58. Of the 20 columns of this rectangle six are reproduced in Table A. These are sufficient to explain the substitution of the top three lines of the example in Table B.

Each of the grilles was designated by a 3-kana name, e.g., *i ra ku* (Nr. 16), *e mi tu* (Nr. 17), *o ro to* (Nr. 18).

To produce the intermediate text for encryption, the operator numbered the paragraphs of the plain text "*ichi*" (= 1), "*ni*" (= 2), "*san*" (= 3), etc., and shuffled them.

As a grille can accommodate only 100 units, in the case of larger messages (i.e., most messages) the successive 100-unit sections, although transmitted as one continuous message, were encrypted in different grilles, normally successive grilles in the cyclic order in which they came in the cryptographic materials.

To encrypt a message, the operator selected one of the grilles and, leaving the top three permitted squares in the righthand column unfilled for later insertion of a nontextual indicator, wrote the first 97 units of the intermediate text from left to right and line by line into the remaining 97 permitted cells. He then substituted cipher units for plain-language units by use of the 20 × 58 substitution rectangle, of which six selected columns are shown in Table A, wrote the nontextual indicator downwards into the top three permitted cells of the righthand column and took out the columns of cipher units (including the indicator) from right to left to form the first 100 cipher digraphs of the message.

TABLE A

	KI KU KE	KO SA SI	SU SE SO	TA TI TU	HU HE HO	WI WO WN
AA	*o*	*nu*	*ti*	*yu*	*e*	*ru*
II	*ta*	*ra*	*na*	*u*	*ku*	4
UU	*ku*	8	*se*	*me*	—	*ni*
EE	*hu*	*re*	*ni*	—	*u*	—
OO	"	*he*	*hu*	7	*yo*	*ma*
KA	*ni*	*tu*	*ha*	*si*	*su*	2
KI	*si*	*ti*	*ya*	4	*ni*	*ti*
KU	*n*	*u*	*ri*	*he*	7	*se*
KE	*to*	*i*	—	*n*	*ta*	·
KO	2	*hi*	*i*	*a*	*ha*	*na*
SA	*mi*	Ø	*ra*	*ke*	*nu*	*n*
SI	6	*so*	*nu*	*o*	*yu*	*ho*
SU	7	*su*	8	*tu*	2	*yu*
SE	*sa*	*ni*	*hu*	*wa*	*me*	*i*
SO	*ya*	°	*ro*	*ku*	*ro*	7
TA	3	*e*	*mi*	*re*	*mu*	*wa*
TI	*wa*	*o*	*mo*	*ya*	*to*	*tu*
TU	*a*	*me*	*ru*	*e*	*no*	*he*
TE	*se*	*ho*	*sa*	2	·	*ta*
TO	*su*	*ke*	4	*ne*	1	*no*
NA	*ki*	*no*	*a*	*te*	*ho*	*u*
NI	*ru*	*n*	3	*ta*	*so*	*hi*
NU	*i*	*sa*	*no*	*ka*	*hu*	*mo*
NE	*te*	7	*ne*	·	*ri*	*yo*
NO	*ne*	*ki*	2	3	*tu*	9
HA	*ro*	*ru*	*tu*	*na*	*na*	*so*
HI	*hi*	*yu*	*e*	9	*ki*	*ne*
HU	*re*	2	1	*i*	8	*ke*
HE	*ri*	"	Ø	*so*	*re*	*me*

	KI KU KE	KO SA SI	SU SE SO	TA TI TU	HU HE HO	WI WO WN
HO	—	*ma*	*su*	*yo*	*n*	*ha*
MA	*ra*	4	*yo*	*ni*	*ne*	1
MI	*yu*	3	*re*	1	6	*hu*
MU	4	*yo*	*te*	*hi*	*mi*	*nu*
ME	*mu*	9	*yu*	*no*	*ra*	"
MO	*e*	*ri*	*to*	*se*	4	5
YA	*mo*	*ro*	*mu*	*ru*	*i*	*o*
YU	Ø	*ko*	5	*to*	*ku*	*ra*
YO	*ti*	*si*	6	*mu*	*te*	*re*
RA	*so*	*ne*	*me*	*ri*	*ru*	*e*
RI	*ha*	*ya*	*ka*	*su*	*si*	6
RU	*he*	*mi*	*ko*	*ho*	3	*sa*
RE	*me*	*ha*	*wa*	*ki*	5	Ø
RO	*ke*	*ka*	*si*	*ko*	*ma*	*mu*
WA	*na*	*te*	*hi*	6	*ti*	*ya*
WE	*ma*	*a*	9	*ti*	*o*	*mi*
WI	1	6	*ku*	*nu*	*se*	8
WO	*ka*	5	*n*	*ha*	"	*te*
WN	*yo*	*mu*	*ke*	Ø	*mo*	*ku*
QC	*ko*	*wa*	7	*ma*	Ø	*ki*
QD	*tu*	*se*	*ta*	5	*hi*	*si*
QF	9	*ta*	*o*	"	*he*	*ka*
QG	8	1	"	*hu*	9	3
QL	*nu*	*to*	*ma*	*ro*	*ya*	*ri*
QP	*no*	*mo*	*ki*	8	*ku*	*a*
QV	*ho*	—	*su*	*sa*	*a*	*ko*
QX	5	*hu*	*u*	*ra*	*sa*	*su*
QB	*u*	*na*	*he*	*mi*	*wa*	*ro*
QZ	·	*ku*	·	*mo*	*ke*	*to*

This table shows 6 selected columns of the 20 in the substitution rectangle. Columns headed AA II UU, EE OO KA, TE TO NA, NI NU NE, NO HA HI, MA MI MU, ME MO YA, YU YO RA, RI RU RE, RO WA WE, QC QD QF, QG QL QP, QV QX QB and QZ are here omitted in order to save space.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

[redacted]

Fortunately for the sanity of the cryptanalysts, the columns were not taken out in transposed order!

One important practice has not so far been mentioned. This was the custom, so universal that it must have been insisted on in the instructions, of placing at the beginning of each block of 97 plain-language units the number of the part. Thus, the first three units of intermediate text of the first blocks of messages invariably read *sono* 1 (i.e., Part 1), of the second blocks *sono* 2, etc. This was quite independent of the shuffling of paragraphs and was totally unnecessary; [redacted] The shuffling of paragraphs, which, I suppose, was suggested by the general practice of [redacted] in Japanese systems back to about 1935, was also unnecessary and neither helped nor hindered the cryptanalysts.

[redacted]

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

My research section at G.C.H.Q. and a party at ASA worked concurrently on the [redacted] traffic and exchanged results regularly.

At an early stage of the investigation, study of a small number of [redacted] and partially [redacted] messages strongly suggested that transposition was involved, with grilles of about 10 columns in width. It was clear from the general flatness of the cipher texts that some form of substitution was also present.

The indicators, i.e., [redacted] were studied continuously as new traffic arrived, and in July 1944 the indicators had been grouped into a cycle of 30 classes, each class containing a number of variants, later determined to be 20. The analysts tested all the indicators believed to be equivalents (i.e., all those falling into one of the 30 classes) in order according to the corresponding [redacted] The following is part of the table produced for class 17:

1	2	3	[redacted]		
RA	MA	RU	AA	II	UU
SO	KA	RI	EE	OO	KA
MO	SA	QD	KI	KU	KE
TA	RU	KA	KO	SA	SI
HI	TA	HA	SU	SE	SO
TU	QE	SU	TA	TI	TU
YA	OO	MA	TE	TO	NA
QC	KA	SU	NI	NU	NE
KA	WA	RU	NO	NA	HI

[redacted]

[K] [redacted] was the German one-time pad system used from long before World War II until the collapse of Germany in 1945 for their most secret diplomatic communications. Pads were made up of 100 single sheets, each containing 48 5-digit groups arranged in eight lines of six groups each. The sheets were used once only. Messages or parts of messages were converted to digits by means of a one-part 5-digit code and recipherered by addition starting at the top lefthand corners of successive sheets from the current pad, the sheets being given consecutive tetranomes for indicating purposes. The codebook was

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

captured during the war, but had already been extensively reconstructed before the initial break into [redacted] The Germans clearly attached no importance to the compromise of the book, as they relied on the one-time usage to give absolute security (see Fig. 1).

The sheets were printed by means of a mechanical device consisting of a framework accommodating according to the pad format 240 printing wheels, each having 10 digits equally spaced on the periphery. Two copies of each sheet were printed from the device in one operation and then the wheels turned before printing the next sheet. The sheets were then shuffled, numbered consecutively and made up into pads of 100 sheets. (More than one system of numbering was used at different periods and for different purposes; I have selected the simplest.)

Two chances of reading messages at an early date were missed. G.C and C.S. possessed a file dated 1932 describing an early prototype of the printing mechanism developed by a British engineering firm and stating that examples of it had been sold to the German Government, but its use for producing one-time pads was not realized until messages began to be readable in early 1945. In July 1940, 3,600 pad sheets became available to ASA in Washington as a result of the arrest of a suspected German agent. These were analyzed by IBM, but no significant excess of 5-digit repetitions was observed, and the work was put aside for the time being in favor of more profitable undertakings.

In 1943 when the double additive of [redacted] (another high-grade German diplomatic system) had been reconstructed and some of the ASA staff which had accomplished this solution had become available, the study of the pads was reopened. [redacted] By late 1944 the sheets of the compromise pads had been placed in printing order and successful solution of current intercept had been started.

I have made up an idealized example to show the vulnerable feature of the method of generation (see Table E). The column of tetranomes at the left in Table E represents the final numbers of the pad sheets after they were shuffled and made up into pads. The 1st, 2nd, 3rd, 7th, 15th and 28th groups of 25 pads in the original printing order are shown here. At the head of each column of pentanomes will be seen the digits 1 through 5 in mixed order; this was known as the dependence order. Each of the 240 printing wheels carried a "stop," shown here as a bar between two vertically consecutive digits. The

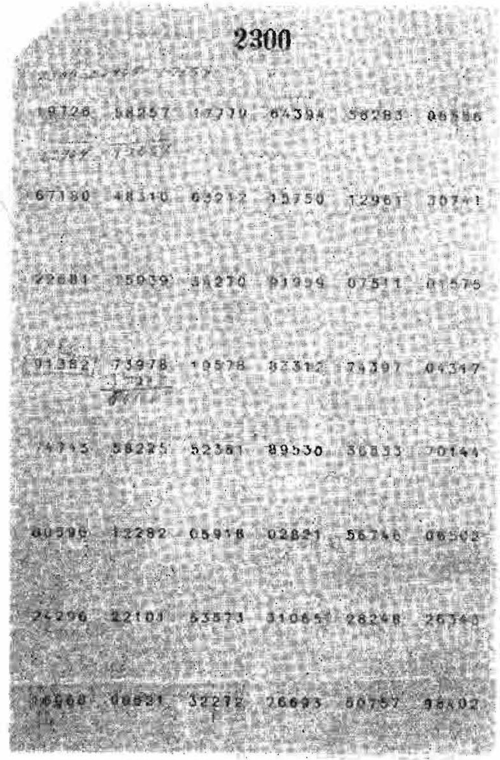


Fig. 1 —A Page from the World War II German High-Level One-Time Pad System [redacted]

TABLE E: [redacted]

	1	2	3	7	15	28
	21453	25143	42531	15342	52314	42135
4072	50102	76663	82725	72014	19608	22615
4123	54102	64199	86782	27366	19688	97548
4125	98785	94099	86787	97368	06811	70457
4290	82254	40280	55690	65957	78123	35767
4333	25391	80837	90411	55957	90344	35367
4012	66838	20936	68373	05540	94060	34067
4127	01936	08512	23268	85445	95960	43836
4171	47936	13475	11956	40701	63775	06290
4150	79520	13775	04809	13232	52592	09100
4200	33317	55301	78834	34823	51532	51974
4283	10669	39624	37145	78189	27406	68622
4173	14669	77158	32142	21694	27486	82583
4122	58043	61043	32147	96076	89217	17419
4301	92042	91243	46520	66078	46629	20741
4011	85175	42869	45581	56078	38848	20341
4000	26704	86990	80093	09317	10161	95055
4211	61281	24587	58718	82960	04353	94855
4070	07358	04486	93676	47555	75074	73268
4317	49358	04786	61469	17451	73994	36138
4059	73896	10332	24354	37742	72770	49997
4231	30990	58615	18205	75203	71790	41607
4176	34990	33171	07932	20839	97535	08576
4099	18557	75004	07937	93124	69402	52420
4042	52339	69228	02930	64686	69482	67780

effect of this was that after the printing of two copies of the sheet, the wheels moved on one space, except that for each group the wheels remained unmoved after a stop in those wheels lower in the dependence order; e.g., in column 1 of the table having operating order 21453 there is a stop after the first digit in the second wheel of group 1 and the other four wheels do not move. [redacted] It is easy to see that the sheets can now be rearranged in the original printing order. By use of this mechanism 100,000 sheets can be printed without ever producing a [redacted] (except in those not too uncommon cases where a particular digit occurs more than once on a wheel).

As I have said, the Germans presumably attached no importance to the sanctity of the code or the intermediate text, and it was found possible to reconstruct pads by applying probable groups of the code (e.g., a large proportion of messages started with the word "GEHEIM"—secret). There were several large "families" of pads printed in a single operation, named by us COPPER, SILVER, etc.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

There were many instances of temporary sticking of wheels, but these were a minor obstacle to solution.

I had no hand in the original diagnosis, but I and my research section went to work on the material as soon as we heard of ASA's break and I made the initial entry into the pads in use in Tokyo.

[B] In the early days of the war in Europe the British general fleet system consisted of a code reciphered by long additives. By early 1941 it became apparent that the system was heavily overloaded, and I was asked to produce a secure replacement. My final solution was the S. S. Frame. This consisted of a plastic grille containing 100 4-digit-wide windows randomly spaced. This could be superimposed over an additive sheet in use for one day, and one day only. The sheet carried (a) 48 lines of 68 digits each, (b) setting squares at top and bottom providing 100 possible settings of the grille over the sheet and (c) a conversion table providing two mixed sequences of the digits 00 through 99 for indicating purposes. The additive sheets were bound in books containing an additive series for each day of the month and different setting squares and conversion squares for each day. Each of the 1700 holders was given a list of tetranomes to be used once only in turn for successive messages. The tetranome was substituted on two cuts by use of the two mixed sequences of the conversion table and the resulting 4-digit group used for setting the sheet under the grille and for defining the window from which the first additive tetranome had to be taken.

In retrospect I realize that a better solution of the indicating system would have been to provide a book of additive tetranomes with separate starting positions for each holder. However, it is clear from Ticom documents that the German cryptanalysts who had had considerable success in reading messages in the preceding cipher and had reconstructed the whole S. S. Frame system for the first month of its use before the introduction of a new code [C], read no messages thereafter.

Soon after the introduction of the system, it was reported to me that at Portsmouth Dockyard, the largest holder, it was the practice at the beginning of each day to back-index the conversion table for the day, so that if a cipher operator didn't wish to move the additive sheet between successive messages, he could derive the appropriate indicator from the setting, which was the converse of my intention, i.e., to set the frame from the next random tetranome and *not vice versa*!

Table F is part of an actual additive sheet showing the arrangement of the daily changing setting sequences and conversion tables.

Table G shows the top three lines of 4-digit additives as they appear in the grille windows with the sheet set at the position 23.

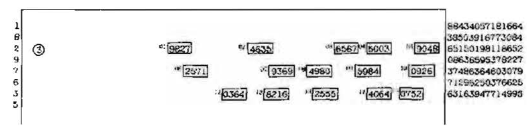
[D] My article "A Cryptologic Fairy Tale" in the Spring 1962 edition of the *NSA Technical Journal*, and "Double Transposition—A Special Case" in the Fall 1972 edition, cover some of the defects of transposition systems.

TABLE F: PART OF AN ACTUAL ADDITIVE SHEET OF THE S.S. FRAME CIPHER SYSTEM OF THE BRITISH GENERAL FLEET IN WORLD WAR II


KEY SQUARE — TABLE GROUPS

1- 0963 54 8 217 — 008975981272067464326581770915463759624 36
8- 5 0 6198 2743 — 2359901165850234287067464326581709154 63'
2- 31 0 7 4956 28 — 4098272364958536134287067466170915463' 6
9- 50 273 94 6 18 — 5430427595623649585361342870674643 2' .543
7- 630 8 452 7 9 1 — 3738126134287067464326581709154 69 57856
6- 1 07 5 692 48 3 — 308005758536134287067464326581 7 .7258580
3- 01 6 53 9 278 4 — 3218702358045674647587101996 7 .769645359
5- 6 2587 490 13 — 5584126795924543566854357 8 .95853613428
0- 1 94 8 05 632 7 — 8966288516584351472585 80 .1709915403759
4- 2 51 870 9 43 6 — 6427733986854357856347 .173564729161758
943012528851472585 60 .161758465938278 86
939962321769045359 .593627613475110 0956
870684559562364 9 .536134287067464326588
S.P. 2357 (107) — 619073112870 67 .068168457936653389147 01
'Y' RECODING TABLE NO. 107 — 851020175846 .816795924543566854357 8563
for use with NAVAL CODE — 1013138824 .584351472581583580456746475
2nd DAY — 76392754 .874885334523217696453597 43221
003212 .4758562364958536134287067990065
3562 .596243173504722464588679410881684
CONVERSION TABLE — 72 .701325467475831710716774368167 95440
081115785634789557639170445794368584 35
670764612248580456746475871019967488 5334
49819967488533452321769645359743189161758
91708230875956236495853613428706746432056
85316746432658170915463759624317356472213
8 217 — 46986175846593627613475956236495853013428
2743 — 48476432658170915463759624317356472662714
956 28 — 68697895576391704457942386368584351472585
94 6 18 — 39792094410688650601527674647567101996748
8 452 7 9 1 — 86758910175846593627613475956236134793649
07 5 692 48 3 — 45831347595623649585361342870674643265817
01 6 53 9 278 4 — 87702009842315213063974495853613428706746
6 2587 490 13 — 49121170265487104649333505076285361342870
0- 1 94 8 05 632 7 — 79557394509950418342870674643265817091546
4- 2 51 870 9 43 6 — 95010457170445794368858435147254485804567

TABLE G



EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

My article "Addendum to a Cryptologic Fairy Tale" in the Winter 1973 edition describes a system which comes very near to being a secure and practical transposition system. [redacted]

[G] The Japanese military attaché system used throughout World War II consisted of a digraphic code reciphered by means of long literal additives. Rigorous [redacted] was employed, but starting-point indicators were not free key. [redacted]

[H] To the best of my knowledge, the Japanese services were the first to practice [redacted] I can remember it as far back as 1936. Starting in December 1937, the Japanese army gradually introduced 4-digit codes reciphered by use of additives 10,000 groups long, i. e., 100 pages of 100 groups each. Starting and ending point indicators were enciphered by tetranomes controlled by dinomes in the first and last textual groups. The starting points were chosen by the operators, resulting in overloading at certain positions. [redacted] was employed, but very commonly only the final auxiliary verb was pushed back to the beginning, with the result that the stereotyped matter, address, serial numbers, signature, etc., appeared quite close to the beginning.

[J] The German 12-wheel machine "TUNNY" was reconstructed entirely from the key provided by the solution of the [redacted]

[redacted] Without this I believe the 12 unique wheel cycles could not have been derived during the war. Even in the case of this [redacted] it would not have been possible to get the wheel cycles if, during the earliest period of the machine's use, the key tapes had not been biased in favor of perforations. Refer to my article "The 'Tunny' Machine and Its Solution," Spring 1961 *NSA Technical Journal* and its sequel by Dr. Campaigne in the Fall 1962 *Journal*, "Reading TUNNY."

[K] During the years 1931 through 1934, I was almost entirely occupied with the study of KOMINTERN cipher systems, in all of which the cryptographic materials consisted of (a) a code or dictionary, (b) an alphabet consisting of a mixed sequence of dinomes to correspond to the letters of the alphabet (in whatever language was employed) used for converting running text to digits and (c) a book or books from which to generate digital key. The progress of this investigation is described in my article "The Development of the Additive" in the Fall 1963 number of the *NSA Technical Journal.* I have thought it worthwhile to repeat here the description of the most complicated of the systems solved. Complicated it certainly was, and yet we read virtually all of the messages.

The system was used on the London-Berlin link starting in February 1934. *Langenscheidt's Pocket English-German Dictionary,* with an elaborate supplement, was used as the code. The alphabet was changed six times a month. The key source book was made up (two identical copies—one for each end of the link) by cutting up the following five books into paragraphs, which were then completely shuffled and numbered consecutively:

(i) *Albatross Book of Living Verse;*
(ii) *The Merry Stories Omnibus,* an anthology of jokes;
(iii) *Taps,* an American anthology of war poetry;
(iv) *Poems of Sentiment,* by Ella Wheeler Wilcox, American Edition;
(v) Dickens' *Pickwick Papers,* Everyman edition.

An indicator giving the number of the alphabet and the number of the paragraph (the paragraphs were never used twice) was reciphered by addition of the sum of the first two textual groups and placed for London messages in the A3 position, for Berlin messages in the A1 position. Stereotyped preambles were buried in the text.

The method of generation of the alphabets is described in the Fall 1963 edition of the *Journal,* which contains a general description of the solution of KOMINTERN systems, pages 1 through 10 and 15 through 22.

[K] I remember an early example of the solution of the problem of producing strictly one-time perforated tape. A Canadian engineer working for a British intelligence organization in New York who knew nothing at all about cryptography produced in 1942 an on-line machine called TELEKRYPTON. He generated his tapes by pouring a mixture of metal and glass balls through a hopper, the metal balls alone passing current and perforating 5-level tape. He analyzed the result and saw that it was biased, owing to the heavier weight of the metal balls, and then changed the respective sizes of the balls to compensate for the extra weight of the metal.

[L] I was in Finland in March 1940 for the last two weeks of their war with Russia. The Finns had had much success in solving Russian military additive systems but were puzzled by the communications of Russian submarines operating in the Baltic. I was able to explain that they were using [redacted]

[L] [redacted] But this did not prevent solution, owing to the stereotyped nature of the texts. This is a case where separate one-time pads for each station would have been completely secure and a much simpler system to operate.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Non - Responsive [redacted]