

File M-138  
Patent Application

8

July 6, 1935

**MEMORANDUM FOR: Research and Development Division (THRU: W.P. & T. Div.)**

1. In accordance with provisions of Par. 4c, AR 850-50, there is attached a draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.

2. It is understood that the Navy Department has pending an application for patent on their first type of strip cipher device, and are filing an application covering their second type. They are apparently satisfied to standardize, for the Naval Service, our Type M-138, and are planning to purchase 100 or 200 devices identical with ours, except as to name plate.

3. It is recommended that the attached draft be forwarded to the Signal Corps Patents Section for use in the preparation of detailed specifications and drawings. In view of the existence of similarities between our Type M-138 and the Navy types, it is probable that patent of only limited scope can be obtained. Nevertheless, the improvements devised by me, consisting in the use of metal channel ways, a slidable guide rule, and a construction which permits of setting up the text alternately at the left side and right side of the assembly, make our type of device a very much more practical instrument than any of those heretofore devised.

4. Since these improvements arose from my own studies, it is requested that application be made in my name as inventor.

William F. Friedman,  
Signal Intelligence Section.

COPY FOR: Mr. Friedman.

85

D R A F T

July 5, 1935

This invention relates to cryptographic devices and has for its object the provision of a hand-operated device capable of affording a relatively high degree of security without involving the use of complicated mechanisms.

Another object is to provide a device useful in cryptographic and cryptanalytic investigations requiring the use of sliding alphabets.

*two figures.*

The invention is explained in connection with <sup>Figure 1,</sup> ~~which~~ is a front and side elevation of <sup>one embodiment of</sup> the device; ~~and figure 2, which shows the device as assembled for use.~~ <sup>Figure 2 is a front and side elevation of a second embodiment of the device.</sup> ~~in this embodiment~~

Referring to figure 1, the device consists of a base, 1, on which are horizontally fastened a series of cylindrical rods, 2, forming a set of channel ways, 3, into which paper strips, <sup>4,</sup> may be inserted and slid from ~~one side to the~~ <sup>left to right or vice versa.</sup> ~~other.~~ In the specific embodiment disclosed herein the device comprises 25 such

channel ways, set off in groups of fives, but the device is by no means limited to this number. ~~of channel ways.~~ The number chosen in this embodiment is merely a convenient number, and it may be increased or decreased <sup>within certain limits</sup> in other embod-

iments without materially departing from the basic nature of the device. A rule, <sup>or reading guide,</sup> 5, ~~called the reading guide,~~ attached to a reading guide slide, 6, can be slid to the left or right on a reading guide slide rail, 7. End bars, 8 and 9, serve

as stops against which the reading guide 5 can be brought at the end of its travel to the left or right. To the back of the base 1 is fastened a hinged supporting frame, 6, which can be pulled out to support the device in a slanting position as it rests upon a table, desk, or other plane surface. Or, if the operator prefers to lay the device flat upon the table, the rubber feet, 7, at the four corners of the bottom of base 1 will support the device and keep it from sliding about on the table.

~~Reference is now made to figure 2, to show one of the uses of the device~~

*As stated above,*  
 Into the channel ways 3 there are inserted strips of paper, 4, hereinafter called alphabet strips, upon which appear sequences of letters of the alphabet, each sequence being repeated on the strip, and the letters being equidistant from one another throughout. The purpose of the duplication of sequence will appear presently. The letters on the alphabet strips, 4, may be in normal order or in disarranged order; if the latter, the various alphabets may or may not be different. Assuming, however, different alphabets are being used, each strip bears an identifying mark such as a number, 7, so that the alphabet strips may be inserted into the channel ways C according to some preagreed key. For example, in figure 2 is shown a set of 25 channel ways into which <sup>25 different</sup> alphabet strips 4 have been inserted according to the following key, reading from the

top downwards

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

If another embodiment of the device should include more than 25 channel ways, additional alphabet strips may be inserted, according to a longer key.

Having inserted the alphabet strips into the channel ways in key order, the device is now ready for use either to encipher a plain language message or to decipher a cryptogram which has been enciphered by means of the device, alphabets, and key shown in figure 1. Suppose this plain-text message is to be enciphered:

ACCORDING TO AN OFFICIAL REPORT FROM MILITARY AUTHORITIES . . .

Moving the reading guide 5 to the left, and bringing it against the left end bar 6, the operator proceeds to align, in a column immediately to the right of the reading guide, the first 25 letters of the message. This is most conveniently done by placing the eraser end of a pencil upon the successive desired letters as found on the successive alphabet strips<sup>4</sup> from the top downwards, and pulling or pushing the alphabet strips<sub>^</sub> toward the reading guide so that each strip stops with the proper letter just to the right of the<sup>right hand</sup> edge of the reading

5  
 guide. ~~Figure 3 shows the 21 letters ACCORDING TO AN OFFICIAL aligned as indicated; the operator is about to align the first letter of the next word, REPORT. When the alphabet strips are being aligned on the left hand side of the device, as in the above procedure, the operator confines his search for letters to the left-hand half of the duplicated sequence on each alphabet strip.~~

When all 25 alphabetstrips have been aligned as indicated, there is disclosed a multiplicity of columns of letters to the right of the plain-text column of letters thus aligned. All these columns of letters, except one, are columns of cipher letters, each column representing a cipher equivalent of the plain-text column. The single exception is the column which is the 25th removed from the plain-text column set up by the operator, and is merely a repetition of that plain-text column. One of these cipher columns is selected at random and is recorded in 5-letter groups. The reading guide 5 is useful in this operation,

since by placing it alongside the column selected, reading of the cipher column

is facilitated. *Suppose that the reading guide 5 is moved so that its left-hand edge aligns to a column of cipher text. The letter position in Figure 3, and aligned on the column of cipher letters selected at random from among the available columns. The column reads as follows:*

~~QWERTY UIOPASDFGHJKLZXCVBNM~~

These letters are recorded and constitute the cipher letters for the first 25 plain-text letters.

The reading guide **5** is now moved to the extreme right of the device, up against the right end bar **9**; the next 25 letters of the plain text are aligned against the left edge of the reading guide **5**. Again a set of columns of cipher letters are disclosed to the left of the reading guide. *again a set of 25 cipher letters representing the second set of plain-text letters*

One of these columns is selected at random and is recorded. If the message contains more than 50 letters the foregoing procedure is repeated until the entire message has been enciphered. There is no need to indicate to the recipient of the message which column is selected for the cipher equivalent of each set of 25 plain-text letters, as will be noted presently.

To decipher the message, having the alphabets and the key according to which they have been arranged, the operator merely proceeds as in encipherment, *in their channel ways* aligning the alphabet strips *cipher* so that the first 25 letters of the cryptogram are in one column. He then examines all the other 25 columns of letters, looking for one which contains intelligible text throughout its extent from top to bottom. There will be one and only one such column, and this will be the plain-text equivalent of the column of cipher text set up on the device. The reading guide **5** is useful in this search for the plain-text column, as it can readily be moved to scan the

successive columns from left to right, or from right to left. The plain-text column thus found is recorded in word lengths and the operator proceeds to set up the next 25 cipher letters on the right-hand side of the device. Again he looks for a plain-text column and records it when found. He continues this process until the message has been completely deciphered.

The many uses of this device, with variable alphabets, in cryptographic or cryptanalytic studies will be apparent to all skilled in the art and nothing further need be said on this score except that there has existed for many years a hitherto unfulfilled need for a simple device of this type, suitable for the insertion of sliding alphabets.

Although in the figures accompanying this description a device is shown in which cylindrical rods are riveted to a base, at regular intervals from one another to form the channel ways into which the alphabet strips are inserted, it should be understood that any other means may be employed to form the channel ways. For example, a series of elongated metal strips known in the trade as "card holders", used ordinarily to hold narrow strips of paper bearing names of mail-box owners in apartment houses, etc., may be used to form the channel ways; these card holders may be riveted to the

move  
down  
at  
and  
to  
place  
insert  
\*

base, or spot welded to it, or attached in any other suitable manner. Or, the channel <sup>ways</sup> may be formed by milling grooves in the base itself, which may be made of molded bakelite, for example. In such case the grooves are made by a rotating cutter which undercuts at the two edges, forming a channel <sup>way</sup> such as is commonly found in slide-rules. Figure 2 shows such a construction in the form of a piece of bakelite or similar material <sup>13,</sup> <sub>11</sub> in which five such channel <sup>ways</sup> have been cut.

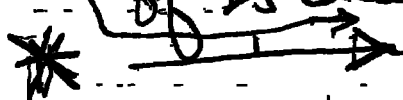
In Figure 3 there is shown another embodiment of the invention, in which instead of having all the channel <sup>ways</sup> on a single base, the latter is merely made in the form of a flat surface onto which <sup>five</sup> ~~has been cut up into~~ sections of channel ways <sup>may be rested and temporarily fixed, so</sup> that rearrangements of sections can be made. Each of these sections bears an identifying symbol, <sup>with the case the letters A, B, C, D, E</sup> according to subsidiary keys. In this embodiment Figure 3 shows six sections of five channels each, the sections being numbered being set into position ~~on base~~ <sup>at the bottom</sup> of the box 14, according to a key consisting of the numbers 1 to 6 in some preagreed order, say



ment, the method of operation would be as follows: First, the sections are <sup>temporarily</sup> fastened to the base in the ~~alphabetical order~~ <sup>alphabetical order</sup> from A to E, reading downward. Then the 25 alphabet strips would be inserted in the <sup>25 consecutive</sup> channels according to the <sup>predetermined</sup> numerical key already referred to above. Thus, section A would comprise, in the case of the numerical key given in connection with figure 1, the <sup>numbered</sup> alphabet strips 14, 16, 9, 6, and 22; section B would comprise the alphabet strips numbered 25, 23, 5, 12, and 24, and so on. To encipher a given message, there would then be a subsidiary or special key, also arranged for in advance, <sup>by means of an indicator in the message,</sup> which would direct that the sections be <sup>now</sup> placed into ~~different~~ <sup>a mixed order,</sup> say E-D-A-C-B, as shown in Figure 3. The encipherment of a message would then proceed exactly as before. In another message, the ~~indicator~~ <sup>indicator</sup> for the sectional arrangement might be different, say one calling for

In figure 3 the sections of channel ways comprise equal numbers of channel ways, but this is of course not an essential feature. Sections consisting of 1, 2, 3, ... ~~channel ways~~ up to say 7 or 8, are perfectly possible, and would give increased cryptographic security by rearrangement.

the sequence of sections D-A-C-E-B. Thus, with five sections there could be 120 different arrangements of sections on the base, even though only one set of 25 alphabet strips is employed. The purpose of this is of course to increase the keying possibilities of the device, without going to the trouble of making a complete rearrangement of all 25 alphabet strips in the set of 25 channel ways.



\* 1. A cryptographic device consisting of a base upon which is provided a plurality of channel ways in which ~~slidable~~ strips of ~~paper~~ character-bearing material ~~sequences~~ may be inserted and slid into alignment.

2. [same as 1] plus "the channel ways being open at both ends."

3. [same as 1] plus "and a slidable transversely guide rule for making excursions across the channel ways."

4. A cryptographic device consisting of a base with a hinged support rest attached to the

reverse surface of the base; a plurality of members fixed to the obverse surface of the base at equidistant intervals to form a plurality of channel ways for the insertion of <sup>character-bearing</sup> strips bearing alphabetic sequences; solid members fixed at opposite ends of the channel ways and resting upon the members forming the channel ways; and a guide rule attached to a sleeve permitting the guide rule to be slid transversely across the channel ways.

5. A cryptographic device consisting of a base; ~~into which are fitted~~ a plurality of <sup>slidably</sup> grooved members providing channel ways for the insertion of character-bearing strips, said grooved members <sup>bearing distinguishing symbols to differentiate one from another and</sup> containing one or more said channel ways; means for temporarily fixing said members to the base in <sup>linear</sup> juxtaposition to afford series of juxtaposed channel ways; end members attached to said base transversely to the direction in which the channel ways extend and raised above the <sup>ends of the</sup> channel ways so as to provide stops against which an instrument is brought at the end of its travel in setting up letters for enciphering and deciphering; and a slidable guide

rule movable transversely across the channel ways.

6. A cryptographic device of the character specified in claim 5, in which said grooved members contain ~~ing~~ equal numbers of channel ways.

7. A cryptographic device of the character specified in claim 5, in which said grooved members contain unequal numbers of channel ways.

Fig. 2

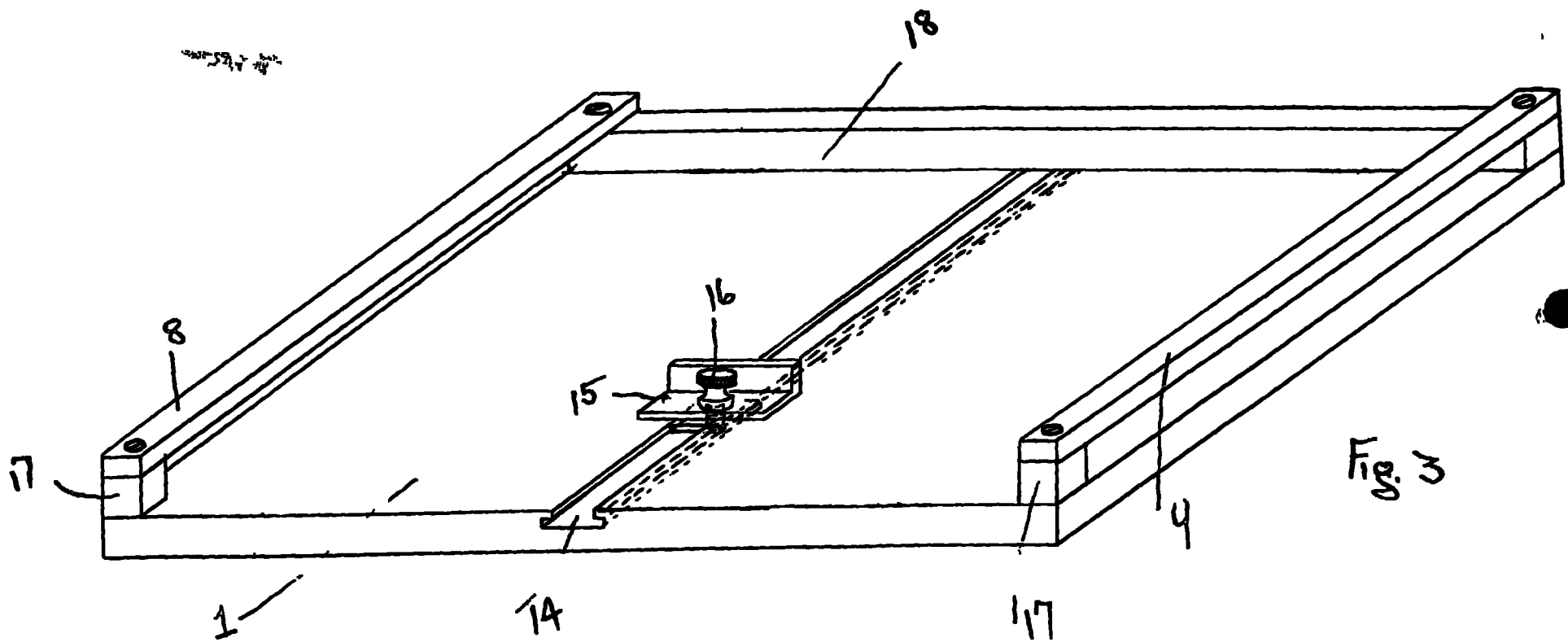
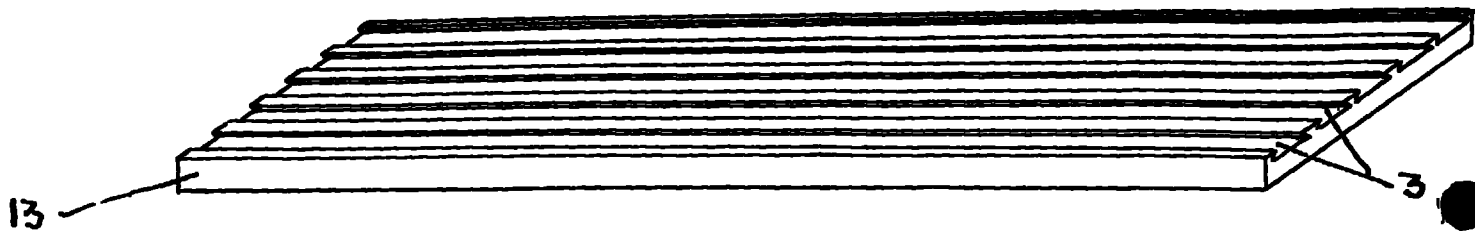


Fig. 3

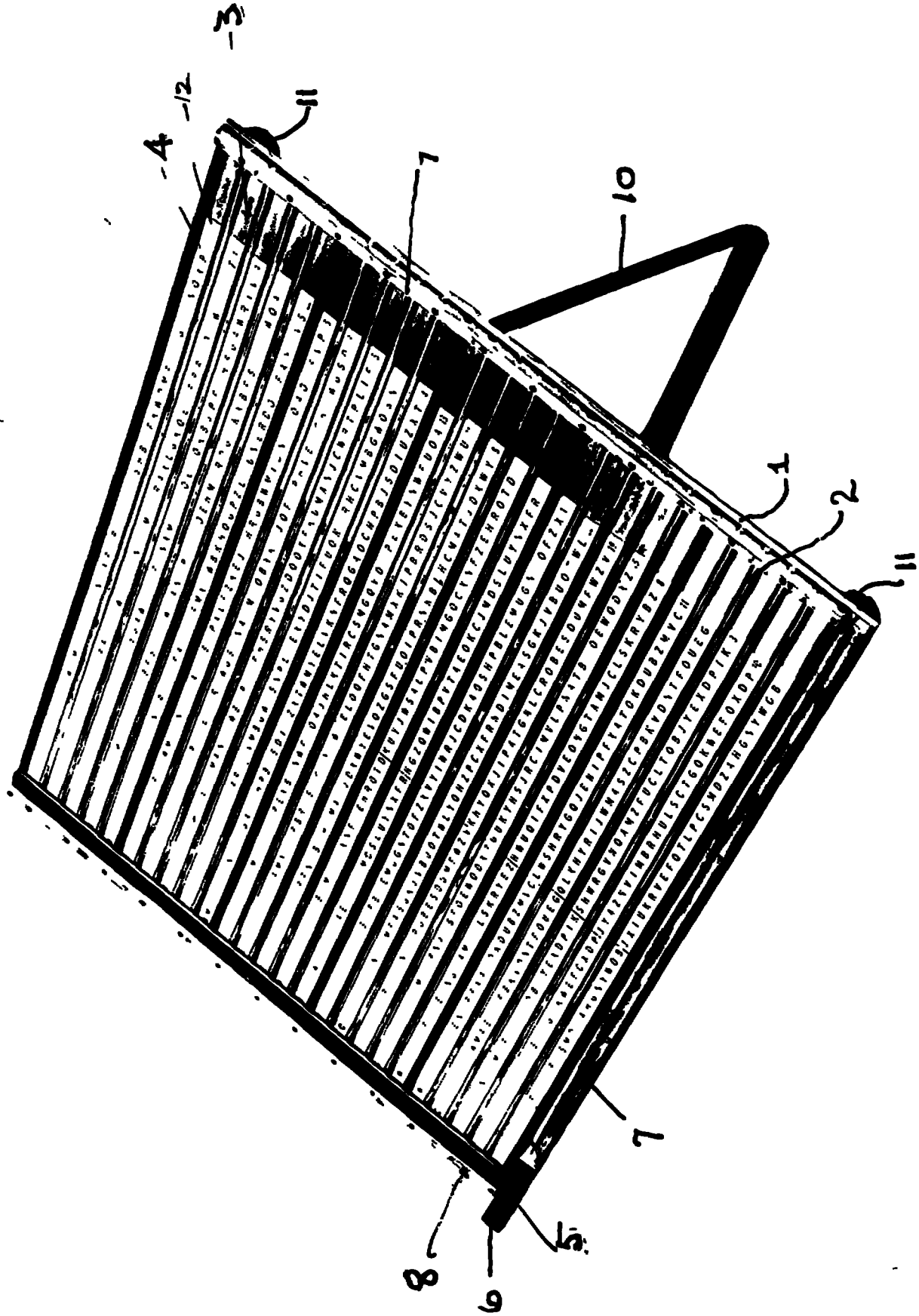


Fig. 1

R LVC SHBVFKWDMEO	ANQXPZRJUYCTSHBVFKWDMEOIGLANQXPZH
NHZMJIRAXLG	CFPBSODWYUVTNHZMJIRAXLGKQECFPBSODWYUVT 16
EYNXMT	EUQKB JPFZHS GAWRIV EYNXMTDLOCUGKB JPFZHS GAWRIV 9
NUP	DEHMYRDGVKXBFSLZJWOA NUPCTLOEHMYRDGVKXBFSLZJWOA 6
NXJWBKHO GPZLC	RDOIFAYTVS NXJWBKHO GPZLC UNERDOIFAYTVS 2
XLFZKEJURGB	DNYTGAOCSVP XLFZKEJURGBW MIDNYTGAOCSVP 25
NAYMZOBXKTJOFUPHVE	IWGS D NAYMZOBXKTJOFUPHVELCRIWGS D 2
HSRYV GZDOOXEK	IJCWBTPLIFHSRYV GZDOOXEKUMANJCWBTPLIF 3
PLZEXYDJTIFUOKARHC	EWOS NPLZEXYDJTIFUOKARHC VMBGWOS N 12
WMYELVKNFRGGAOCHPBJSDI	IWMYELVKNFRGGAOCHPBJSDIUZXTM
JHLRTIRCSNGQVDZPEXBYN	DAJHLRTIRCSNGQVDZPEXBYNWFUOA 11
ELOQFN	AMXKIPBRDSJCVYZWU ELOQFHTGNAMXKIPBRDSJCVYZWU 11
EVOZGSFUO	IKBLHCMATJDXWY EVOZGSFUOIPRNKBLHCMATJDXWY 11
KJY WSA LPVBINGCCXNFZ	OTDRUYJWSALPVBINGCCXNFZEHROTD 1
HGZOWIBPVTAEOKCJMDSLG	FRHGZOWIBPVTAEOKCJMDSLUYNXFR 7
VYIWRJCDKAOSHPLMBG	ZXVYIWRJCDKAOSHPLMBGHTOFZX 17
YQHZPCSE	MEASGKJVBUTWL YQHZPCXFRNDIMEASGKJVBUTWL 2
KHYOXJIPAT	EROBESDUMFWZV KHYOXJIPATGNLCROBESDUMFWZV 10
GUKYNS	MVLPNATBFOEWODXZ GUKYNSJRCIMVLPNATBFOEWODXZ 15
HWUOIFXPDVGO	AMJCLSKRYBZ HWUOIFXPDVEONGTAMJCLSKRYBZ 1
	LWSHRYGOJENIPFXATOKDUBZMVC LWSHRYGOJENIPFXATOKDUBZMVC 11
	OLXHYRIJWMA SZCPBKVDNTFOUEG OLXHYRIJWMA SZCPBKVDNTFOUEG 2
	SHWRGVNGAMZFUCLTOBJYEXDPIK SHWRGVNGAMZFUCLTOBJYEXDPIK 31
	JYAZNVI MBRHULSCTGOKWEFOXDP JYAZNVI MBRHULSCTGOKWEFOXDP 10
	JXIUKRVEFQTLPCSNZAHGNYWOB JXIUKRVEFQTLPCSNZAHGNYWOB 4

R J U Y C T S H B V F K W D M E O	GLANQXPZRJUYCTS	VFKWDMEOIGLANQXPZ14
N H Z M J I R A X L G	Q E C F P B S O D W Y U V T N	M J I R A X L G K Q E C F P B S O D W Y U V T 16
E Y N X M T	L O C U Q K B J P F Z H S G A	I V E Y N X M T D L O C U Q K B J P F Z H S G A W R I V 9
N U P	T I O E H M Y R D G V K X B F	Z J W O A N U P C T I O E H M Y R D G V K X B F S L Z J W Q 6
M X J W B K H Q G P Z L C	N E R D O I F A Y T V S M X J	K H O G P Z L C U N E R D O I F A Y T V S 2
X L F Z K E J U H R G B	M I D N Y T Q A O C S V P X L	K E J U H R G B W M I D N Y T Q A O C S V P 25
N A Y M Z O B X K T J O F U P H V E	C R I W G S D N A Y M Z O B X	J Q F U P H V E L C R I W G S D 3
H S R Y V G Z D Q O X E K	M A N J C W B T P L I F H S R	G Z D Q O X E K U M A N J C W T P L I F 5
P L Z E X Y D J T I F U Q K A R H C	M B G W O S N P L Z E X Y D J	F U Q K A R H C V M B G W O N I
W M Y E L V K N F R Q G A O C H P B J S D I	Z X T W M Y E L V K N F R O G	C H P B J S D I U Z X T 4
J H L K T I R C S M G O V D Z P E X B Y N	F U O A J H L K T I R C S M G	D Z P E X B Y N W F U O A 13
E L O O F H	G N A M X K I P B R D S J C V	W U E L O O F H T G N A M X K I P P R C S J C V Y Z W U 21
E V Q Z G S F U O	P R N K B L H C M A T J D X W	V Q Z G S F U O I P R N K B L H C M A T J D X W Y 18
K U Y J W S A L P V B I M G O C X N F Z	H R O T D K U Y J W S A L P V	M G O C X N F Z E H R O T D 1
H G Z Q W I B P V T A E O K C J M D S L U	N X F R H G Z Q W I B P V T A	K C J M D S L U Y N X F R 7
V Y I W R J C D K A Q S H P B L E M U G	T O F Z X V Y I W R J C D K A	H P B L E M U G N T O F Z X 17
Y Q H Z P C X F	N D I M E A S G K J V B U O T	Y Q H Z P C X F R N D I M E A S G K J V B U O T W L 20
K H Y O X J I P A T	N L C R O B E S D U M F W Z V	Y Q X J I P A T G N L C R O B E D U M F W Z V 19
G U K Y H S	R C I M V L P N A T B F O E W	X Z G U K Y H S J R C I M V L P N A T B F O E W O D X Z 15
H W U Q I F X P D V E O	G T A M J C L S K R Y B Z H W	I F X P D V E O N G T A M J C L S K R Y B Z 8
Q L	L W S H R Y G Q J E N I P	A T O K D U B Z M V C L W S H R Y G Q J E N I P F X A T O K D U B Z M V C 11
S H W R G V N Q A M Z F U C L T O	H Y R I J W M A S Z C P B K V	T F O U E G Q L X H Y R I J W M A S Z C P B K V D N T F O U E G
J Y A Z N V I M B R H U L S C T G O K W E F	J Y E X D P I K S H W R G V N	M Z F U C L T O B J Y E X D P I K 3
J X I U K R V E F Q T L P C S M D Z A H G	X D P J Y A Z N V I M B R H U	E T G O K W E F O X D P 10
	W O B J X I U K R V E F Q T	C S M D Z A H G N Y W O B 4



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

C T S H B V F K W D M E O I G L A N Q X P Z 14  
 R D G V K X B F S L Z J W Q A 6  
 R D O I F A Y T V S 22  
 R G B W M I D N Y T O A O C S V P 25  
 D 23  
 Q O X E K U M A N J C W B T P L I F 51  
 J T I F U Q K A R H C V M B G W O S N 12  
 X T 24  
 13  
 C V Y Z W U 21  
 N K B L H C M A T J D X W Y 18  
 X N F Z E H R O T D 1  
 U Y N X F R 7  
 C D K A O S H P B L E M U G N T O F Z X 17  
 G N L C R O B E S D U M F W Z V 19  
 E W Q D X Z 15

X P D V E O N G  
 O L X H  
 F U C L T O B J  
 G O K W E F O X  
 M D Z A H C N Y

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

[REDACTED]	RJUYCTSHBVFRWDM	GLANQXPZIRJ	CTSHBVFRWDMEOISLANQXPZ 14
[REDACTED]	NHZMJIRAXLGKQECFPBSODWYUVT	BSODWYUVT 16	
[REDACTED]	EYNXMTDLOCUCQKBJPFZHS GAWRI	PFZHS GAWRI	
[REDACTED]	NUPCTIOEHMYRNDGKXBFSLZ 3	ANUPCTIOEH	RDGVKXBFSLZJWQA 6
[REDACTED]	MXJWBKHOQPZLCUNERDOIFAYTVS 11	BKHOGPZLCU	RDOIFAYTVS 22
[REDACTED]	XLFZKEJUHRCBWMIDNYTQ	SVPZLFZKEJ	RCBWMIDNYTQAOC SVP 25
[REDACTED]	NAYMZOBXKTJOFUPHVELCRIWGS	UPHVELCRIW	D 23
[REDACTED]	HSRYVGGZDOOXEKUMAHJC	PLIFHSRYVG	GOOXEKUMAHJCWBTP LIF 5
[REDACTED]	PLZEXYDJTIFUQKARHC	GWOSHPLZEX	JTIFUQKARHCYMBGWOSH 12
[REDACTED]	WMYELVKNFRGGAOCHPBJSDIUZX	AOCHPBJSDI	XTM
[REDACTED]	JHLKTI RCSMGQVDZPEXBYNWFOA	ZPEXBYNWFU	13
[REDACTED]	ELOOFHTGNAMKKIPBRDSJCVYZW	NAMXKIPBRD	CVYZW 24
[REDACTED]	EVQZGSFUOIPRNBKBLHC MATJD	EVQZGSFUOI	NKBLHC MATJDXWY 18
[REDACTED]	KUYJWSALPVBINGOCXNPFZEHROTDR	WSALPVBING	XNPFZEHROTDR 1
[REDACTED]	HGZOWIBPVTAEOKCJMDSLUYNXFR	VTAEOKCJMD	UYNXFR 7
[REDACTED]	VYIWRJCDKRAQSHPBLE	NTOPZXVYIW	CDKRAQSHPBLEMUGNT OF ZX 17
[REDACTED]	YQHZPCXFRNDIMEASGKJVBUOTWL	KJVBUOTWLB	
[REDACTED]	KHYOXJIPATGNLCROBESDU	ZV KHYOXJIP	GNLCROBESDUMFWZV 19
[REDACTED]	GUKYHSJRCINVLPHNATBFOEWODXZ	CINVLPHNATB	EWODXZ 15
[REDACTED]	HWUOIFXPDVEONGTAMJCLSKRYBZ	PDVEONGTAM	LSKRYBZ 8
[REDACTED]	LWSHRYGOJENIPFXATOK	ZMVC LWSHRY	JENIPFXATOKDUBZMVC 11
[REDACTED]	OLXHYRIJWNASZCPBKVE	QUEGOLXHYR	WNASZCPBKVDNTFOUEG 2
[REDACTED]	SHWRCVNGANZFUCLTOBJYEXD	SHWRCVNGAM	UCLTOBJYEXDPIK 3
[REDACTED]	JYAZNVIMBRHULSCTGOKWFOXD	ZNVIMBRHUL	TGOKWFOXD 10
[REDACTED]	JXIKRVEFOTLPSCMDZAHGNYW	IURRVEFOTL	SMDZAHGNYWOB 4

[ R ]	S H B V F K W D M E O I G L A N O X P Z R J U Y C T S H B V F K W D M O I G L A N O X I Z 14
[ E Y N X M T D L O C U Q K B J P F ]	N H Z M J I R A X L G K Q E C T P B S O D W Y U V T N H Z M J I R A X I G K Q E C P B S O D W Y U V T 1
[ N U P C T I O E H M Y R D G ]	A W R I V E Y N X M T D L O C U Q K B J P F Z H S G A W R I V 9 1
	F S L Z J W Q A N U P C T I O E H M Y R D G V K A B F S L Z J W Q A 5
	J W B K H Q G P Z L C U N E R D O I F A Y T V S M X J W B K H Q G P Z L C U N F R D O I F A Y T V S 2
	L F Z K E J U H R G B W M I D N Y T O A O C S V P X I F Z K E J U H H C R W A I D N Y T O A O C 1 P 2
[ N A Y ]	X K T J Q F U P H V E L C R I W G S D N A Y M Z O B X K T J O F U P H V E L C R I V G S D 7 1
	R Y V G Z D O O X E K U M A N J C W B T P L I F H S R Y V C Z D O O X E K U M A T J C V R T P L I F 5
[ P L Z ]	J T I F U O K A R H C V M B G W O S N P L Z E X Y D J T I F U O K A R H C V M B C W O S N 12
[ W M Y E L V K ]	G A O C H P B J S D I U Z X T W M Y E L V K N F R O G A O C H P B J S D I U Z X T 24
[ J H L K T I ]	G O V D Z P E X B Y N W F U O A J H L K T I R C S M G O V D Z P E X B Y W F U O A 13
[ E L O Q F H T G N A M X K I P B R ]	V Y Z W U E L O Q F H T G N A M X K I P B R D S J C V Y 7 W U 2 1
[ E V Q Z S F U O I P R N K B L H C M A ]	W Y E V Q Z G S F U O I P R N K B L H C M A T J D X W Y 18
[ K U Y J W ]	V B I M G O C X N F Z E H R O T D K U Y J W S A L P V B I M G O C X N F Z E H R O T D 1
[ H G Z Q W I ]	A E O K C J M D S L U Y N X F R H G Z Q W I B P V T A E O K C J M D S L U Y N X F R 7
[ V Y I W R ]	A Q S H P B L E M U G N T O F Z X V Y I W R J C D K A O S H P B L E M U G N T O F Z X 17
[ Y Q H Z P C X F R N D I M E A S G K ]	T W L Y Q H Z P C X F R N D I M E A S G K J V B U O T W L 20
[ K H Y Q X J I P A T G N L C R O B E S D U ]	V K H Y Q X J I P A T G N L C R O B E S D U M F W Z V 19
[ G U K Y H S J R C I M V L P N A T ]	W O D X Z G U K Y H S J R C I M V L P N A T B F O E W O D X 7 15
	W U Q I F X P D V E O N G T A M J C L S K R Y B Z H W U O I F X P D V E O N G T A M J C L S K R Y B Z 8
[ L W S H R Y G Q ]	P F X A T O K D U B Z M V C L W S H R Y G Q J E N I P F X A T O K D U B Z M V C 11
	L X H Y R I J W M A S Z C P B D N T F O U E G O L X H Y R I J W M A S Z C P B K V D N T F O U E G
	H W R G V N Q A M Z F U C I Y E X D P I K S H W R G V N Q A M Z F U C L T O B J Y E X D P I K 3
	A Z N V I M B R H U L S C T G O K W E F O X D P 10
	I U K R V E F O Y L P C S M D Z A H G N Y W O B 4

RJU	CTSHRVFKWDMEO	ANQXPZ	RJUYCTSHRVFKWDMEOIGLANQXPZH
	NHZNJIRAXLGN	CFPBSODWYUVT	NHZNJIRAXLGXOECFPBSODWYUVT 16
EYNXMTDLOCUQKBJPFZ	SGAWRIV	EYNXMTD	CUOKBJPFZKSGAWRIV 5
NUPCTIOENMYRQGV	XBFLZJWQA	HUPC	QEHMYRQGVKXBFLZJWQA 6
	MXJWBKHHGPPZLC		RDOIFAYTVS
	XLFZKEJUHRGB		MXJWBKHHGPPZLCUNERDOIFAYTVS 21
HAYM	OBXKTJOFUPHVEL		DHYTOAOCSP
	HSRYVGGZDOOXEK		XLFZKEJUHRGBWMIONHYTOAOCSP 25
	YDJTIFUOKARHC		IWGS
PLZE	ROGAOCHPBJSDI		NAYMZOBXKTJOFUPHVELCRIWGS 25
WMYELVKN	JHLKTI		NJCWBTPLI
	SMGOVDZPEXBYN		FHSRYVGGZDOOXEKUNANJCWBTPLI 5
ELOOFHTGNAMXKIPBRD	JCVYZWU		GWOSH
	DXWYEVOZGSPUO		PLZEXYDJTIFUOKARHCVMGWSN 12
EVOZGSPUOIPRNKBLHCHMAT	LVPBINGOCXNFZ		TWMYELVKNFRGOACHPBJSDIUZZY 21
	VTAEOKCJMDSL		QA
NGZOWIB	DKAOSHPPBLEMUG		JHLKTI
YVYIWRJ	UOTWLYGHZPCXZ		RCSMGQVDZPEXBYNWFUOA 13
YGHZPCXFRNDIMEASGRJV	WZV		AMXKIPBRDS
KHYQXJIPATGNLCROBESDUM	OEWDGXZGUKYHS		JCVYZWU
GUKYHSJRCIMVLPNAT	HWD		DXWYEVOZGSPUO 18
	NIPFXATOKDUBZ		OTD
LWSHRYGQJ	BKVDHTFOUEGOL		KUYJWSALPVBINGOCXNFZEHR 11
OLXHYRIJWMAZZE	GVNOAMZFUCLYO		FR
	RHULSCTGOKWEP		HGZOWIBPVTAEOKCJMDSL 11
JYAZNVI	FOTLPCSMZAHG		FZ
JXUKR			VYIWRJCDKAOSHPPBLEMUGNT 17
			IMEASGKJVB
			UOTWLM
			ROBESDUM
			FWZV 11
			IMVLPNAT
			BFOEWDGX 11
			ANJCLSKRYBZ
			HWD 11
			FXPDVEONGTAMJCLSKRYBZ 9
			LWSHRYGOJEN
			IPFXATOKDUBZ 11
			RIJWMAZZCPBKVDHTFOUEG 2
			EXDPI
			KSHWRGVNOAMZFUCLYOB 11
			JYAZNVIMBRHULSCTGOKWEP 11
			FXDP 11
			OB
			JXUKRVEFOTLPCSMZAHGNV 11

RJUYCTSHBVKWDMEDI GLANQXPZRJUYCTSHBVKWDM E  
 NHZMJIRAXLGNQECFPBSODWYCVNHZMJIRAXLGKOE C  
 EYNXMTDLOCUQKB JPFZHS GAWRIV EYNXMTDLOCUOK  
 NUPCTIOEHMYRDG VKXB FSLZJWQA NUPCTIOEHMYRDG VKXB FSLZ J  
 MXJWBKHO GPZLCUNERDOIFAYTVS MX  
 XLFZKEJUHRGBWMIDNYTQAOCSPV XLFZKEJUHRGBWMIDNYTQA  
 NAYMZOBXKTJQFUPHVELCRIWGS DNAYMZOBXKTJ  
 HSRVVGZDQO XEKUMANJCBWBTPLIF HSRVVGZDQO XEKUMANJCW  
 PLZEXYDJTIFUOKARHC VMBGWOSN PLZEXYDJTIFUOKARHC V  
 WMYELVKNFROGAOCHPBJS DIUZX TWMYELVKNFR  
 JHLKTI RC SMGOVDZPEXBYNWFUOAJHLKTI RC SMGO  
 ELOQFHTGNAMXKIPBRDSJCVYZWUELOQFH  
 EVQZGSFUOIPRNKBLHC MATJDXWY EVQZGSFUOIPRNKBLHC MATJDX  
 KUYJWSALPVBIMGOCXNFZEHROTD KU  
 HGZQWIBPVTAEOKCJMD SLUYNXFR HGZQWI  
 VYIWRJCDKAOSH PBLEMUGNT OFZX VYIWRJCDKAOSH PBLE M  
 YQHZPCXFRNDIMEASGKJVBUOTWL YQHZPCXFRNDIMEA  
 KHYOXJIPATGNLCROBESDUMFWZV KHYOXJIPATGNLCROBESDUM  
 GUKYHSJRCIMVLPNATBFOEWQDXZ GUKYHS  
 HWUQIFXP DVEONGTAMJCLSKRYBZ HWUQI  
 LWSHRYGOJENIPFXATOKDUBZMVC LWSHRYGOJENIPFXATOKD  
 QLXHYRIJWMASZCPBKVDNTFOUEG QLXHYRIJWMASZCPBKVDN  
 SHWRGVNOAMZFUCLTOBJYEXDP KSHWRGVNQAMZFUCLTOBJYEXDP  
 JYAZNVIMBRHULSCTGQKWEFOXDPJ  
 JXIUKRVEFQTLPCSM DZAHGNYWOB JXIUKRVEFQTLPCSM DZAHGNYWOB

ANQXPZ 14

ODWYUVT 15

ZHS GAWRIV 9

HOGPZLCUNERDOIFAYTVS 22

P 25

HVELCRIWGS D 23

IF 5

OS N 12

CHPBJS D I U Z X T 24

EXBYNWFUOA 13

MXKIPBRDSJCVYZWU 21

ALPVBIMGOCXNFZEHROTD 1

AEOKCJMD SLUYNXFR 7

OFZX 17

VBUOTWL 0

19

MVLPNATBFOEWQDXZ 15

VEONGTAMJCLSKRYBZ 8

VC 11

EG 2

VIM

RJUYCTSHBVFKWDMEOIGLANQXPZR	CTSHBVFKWDMEOI	ANQXPZ 14
NHZMJIRAXLGKQECFPBSODWYUVT	MJIRAXLGKQECFP	ODWYUVT 16
EYNXMTDLOCUOKBJPFZHS GAWH	YNXMTDLOCUOKBJ	ZHS GAWRIV 9
NUPCTIOEHMYRDGVKXBFSLZJWQANUPCTIOE	RDGVKXBFSLZJWQ	HQGPZLCUNERDOIFAYTV 5 22
[REDACTED] MXJWBKHKQGPZLC	RDOIFAYTVSMXJW	P 25
XLFZKEJUHRGBWMIDNYTQAOCVFXLFZKE	RGBWMIDNYTQAOC	HVELCRIWGS 5 D 23
[REDACTED] NAYMZOBXKTJOFUPHVELCRI	D NAYMZOBXKTJOF	IF 5
HSRYVGZDQOXEKUMANJCVBTPLIFHSRYV	QOXEKUMANJCVBT	OSN 12
PLZEXYDJTIFUQKARHCVMBGWOSNPLZE	JTIFUQKARHCVMB	CHPBJSDIUZXT 24
[REDACTED] WMYELVKNFROGAOCHPBJS	XTWMYELVKNFROG	EXBYNWFUOA 13
[REDACTED] JHLKTIRCSMGQVDZPEXBYNWF	JHLKTIRCSMGQVD	MXKIFBRDSJCVYZWU 21
[REDACTED] ELOOFHTGNAMXKIPBR	CVYZWUELOOFHTG	ALPVBIMGQCXNFZEHROTD 1
EVOZGSFUOIPRNBKBLHCMATJDXWYEVOZGSFUO	NKBLHCMATJDXWY	AEOKCJMDSLUYNXFR 7
[REDACTED] KJYJWSALPVBIM	XNFZEHROTDKUYJ	OFZX 17
[REDACTED] HGZOWIBPVTAEOKCJM	UYNXFRHGZOWIBP	VBUIWL 20
VYIWRJCDKAQSHPBLEMUGNTOFZXVYI	CDKAQSHPBLEMUG	19
YQHZPCXFRNDIMEASGKJVBUOTWL	ZPCXFRNDIMEASG	MVLPNATBFOEWQDXZ 15
KHYQXJIPATGNLCROBESDUMFWZVKHYQXJI	GNLCROBESDUMFW	VEONGTAMJCLSKRYBZ 9
[REDACTED] GUKYHSJRCIMVLPNAT	EWQDXZGUKYHSJR	VC 11
[REDACTED] HWUOIFXPDVEONGTA	LSKRYBZHWUOIFX	EG 2
LVSHRYGOJENIPFXATOKDUBZMVC LVSHR	JENIPFXATOKDUB	VIMBRHULSCTGOKWFOXPJYA
OLXHYRIJWMASZCPBKVDNTFOUEGOLXHY	WMASZCPBKVDNTF	SMDZAHGNYWOB 4
SHWRGVNQAMZFUCLTOBJYEXDPIKSHWRGVNQA	UCLTOBJYEXDPIK	
[REDACTED] JYAZNVIMBRHU	TGOKWFOXPJYA	
JXIUKRVEFOTLPCSMZAHGNYWOB JXIUKRVEFOT	SMDZAHGNYWOB 4	