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

1 orig
2 cc

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 crypt-

analytic investigations requiring the use of sliding alphabets.

two figures.

The invention is explained in connection with ~~which~~ Figure 1, ~~which~~ is a front

one embodiment of

and side elevation of the device; ~~and figure 2, which shows the device as~~

~~assembled for use.~~ *Figure 2 is a front and side elevation of a second embodi-
ment of the device. 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

4,

ways, 3, into which paper strips may be inserted and slid from ~~one side to the~~

left to right or vice versa.

~~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

within certain limits

merely a convenient number, and it may be increased or decreased in other embod-

iments without materially departing from the basic nature of the device. A rule,

or reading guide,

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, may be in normal order or in

disarranged order; if the latter, the various alphabets may or may not be differ-

ent. Assuming, however, different alphabets are being used, each strip bears

an identifying mark such as a number, 2, 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 *25 different* 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 con-

veniently done by placing the eraser end of a pencil upon the successive desired

letters as found on the successive alphabet strips from the top downwards, and

pulling or pushing the alphabet strips *in their channel ways* toward the reading guide so that each

strip stops with the proper letter just to the right of the *right hand* 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 alphabets strips have been aligned as indicated, there is dis-

closed 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 Ѕⅅ 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

~~Figure 4 shows the reading guide, which has moved away from its~~

its right-hand edge aligns the column of cipher text. The letter

~~position in Figure 3) and aligned on the column of cipher letters selected at~~

the entire column ~~reappears.~~

~~random from among the available columns.~~ The column reads as follows:

~~QRJGT   LDEG   CWHYJ   HPVW   TVBCF~~

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

One of these columns is selected at random and *again a set of 25 cipher letters representing the second set of* 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 so that the first 25 *cipher* 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

plain - text letters

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 con-

tinues 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 rivéted 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

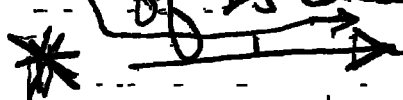be used to form the channel ways; these card holders may be riveted to the

base, or spot welded to it, or attached in any other suitable manner. Or, the channel ways may be formed by milling grooves in the base 1 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 way 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 13, in which five such channel ways have been cuts.

In Figure 3 there is shown another embodiment of the invention, in which instead of having all the channel ways on a single base, the latter is merely made in the form of a flat surface onto which five has been cut up into sections of channel ways may be rested and temporarily fixed, so that rearrangements of sections can be made Each of these sections bears an identifying symbol, in this case the letters A, B, C, D, E according to subsidiary keys. In this embodi-

Figure 3 shows six sections of five channels each, the sections being numbered being set into position on the bottom 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 *temporarily* fastened to the base in the ~~of their identifying symbols, that is, in this case,~~ alphabetical order, from A to E, reading downward. Then the 25 alphabet strips would be inserted in the *25 consecutive* channel ways according to the *predetermined* numerical key already referred to *in connection with figure 1.* above. Thus, section A would comprise, in the case of the numerical key given in connection with figure 1, the alphabet strips *numbered* 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 specific key, also arranged for in advance *by means of an indicator in the message,* ~~which would direct that~~ the sections be ^ now placed into ~~different~~ ~~order from that~~ the ~~fall~~ in a mixed order, 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 ~~the~~ indicator for the sectional arrangement might be different, say one calling for

In figure 3 the sections channel ways comprise equal number 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 and to impart uniqueness to successive messages, 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 character-bearing material may be mounted and slid into alignment.

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

3. [same as 1] plus ", and a slidable guide rule for making excursions transversely 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 character-bearing 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; a plurality of grooved members providing channel ways for the insertion of slidable character-bearing strips, said grooved members bearing distinguishing symbols to differentiate one from another and containing one or more said channel ways, means for temporarily fixing said members to the base in linear 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 ends of the 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 containing 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.
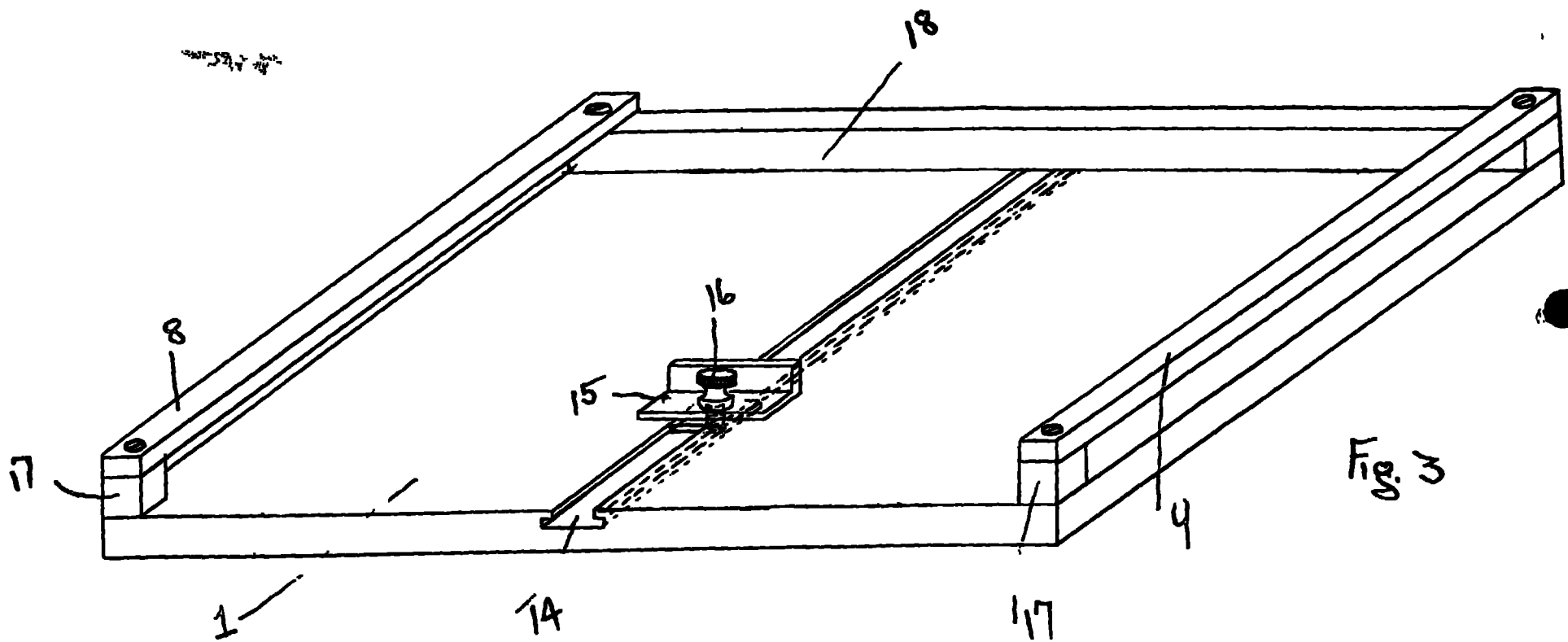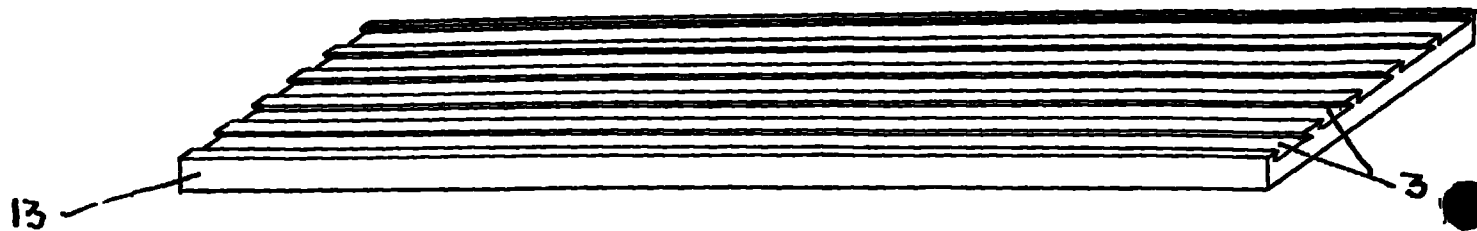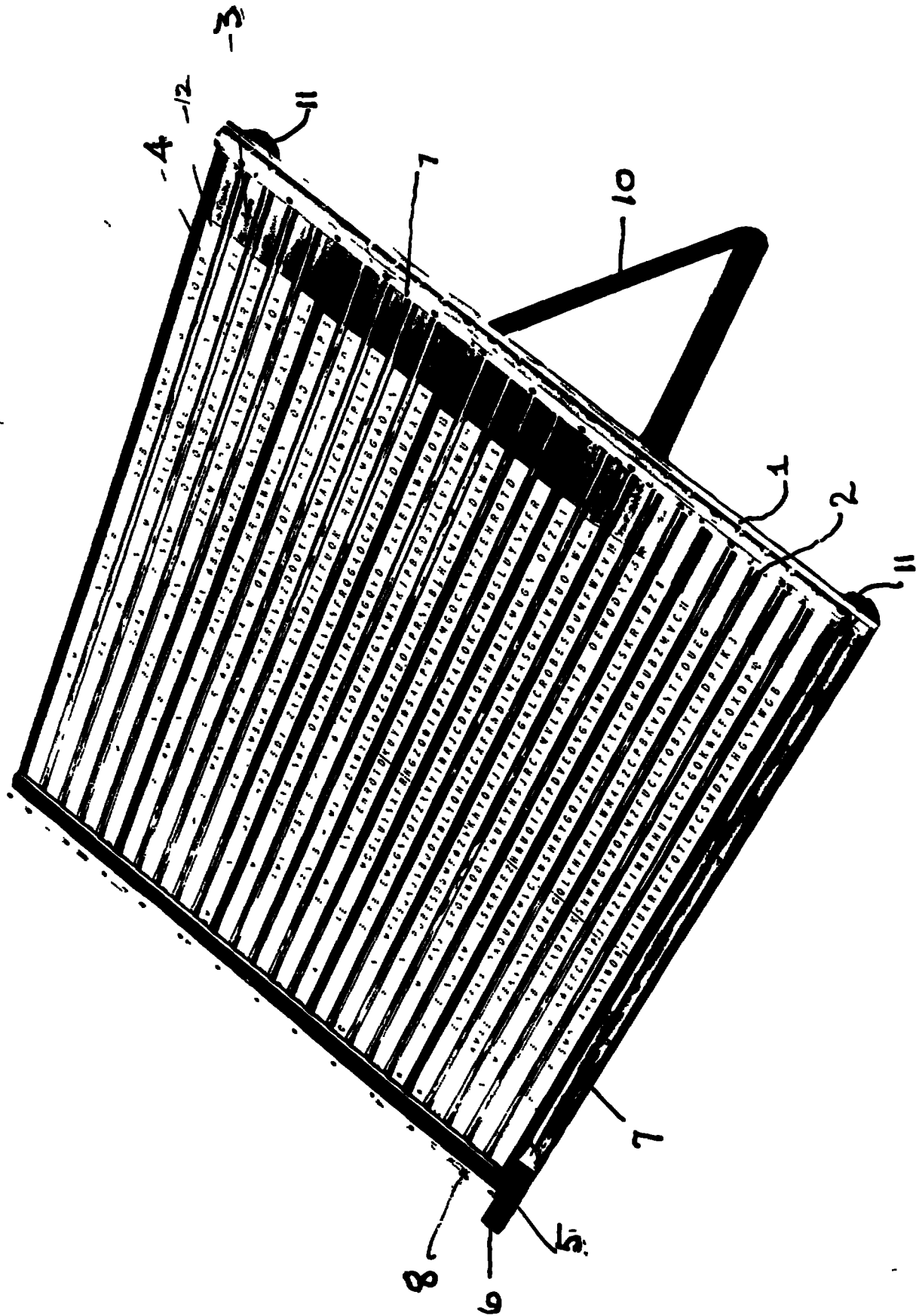
Fig. 2

13

3

18

16

15

8

17

1

14

4

1,17

Fig. 3

Fig. 1

Fig.3

```
R J U Y C T S H B V F K W D M E O        G L A N Q X P Z R J U Y C T S      V F K W D M E O I G L A N Q X P Z 14
            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 Q 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 Q 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 Q 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 1
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 Q 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 Q 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 Q F H          G N A M X K I P B R D S J C V      W U E L O Q F H T G N A M X K I P P R E S J C V Y Z W U 21
              L 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 Q 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
                                         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
                        Q L              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
  S H W R G V N Q A M Z F U C L T O      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 Y A Z N V I M B R H U L S C T G Q K W E F  X D P J Y A Z N V I M B R H U   C T G Q K W E F O X D P 10
  J X I U K R V E F Q T L P C S M D Z A H G  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
```

H

D

Fig 4

```
          R J U Y C T S H B V F K W D M E O I G L A N O X P Z R | C T S H B V F K W D M E O I G L A N O X P Z 14
    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      R D G V K X B F S L Z J W Q A 6
          M X 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      R D O I F A Y T V S 22
          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      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 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 Q F U P H V E L C R I      D 23
          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      Q O X E K U M A N J C W B T P L I F 5
          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      J T I F U Q K A R H C V M B G W O S N 12
    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      X T 24
    J H L K T I R C S M G Q 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 Q V D Z P E X B Y N W F      13
      E L O Q 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 Q F H T G N A M X K I P B R      C V Y Z W U 21
          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      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 E H R O T D K U Y J W S A L P V B I M      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 Y N X F R H G Z Q W I B P V T A E O K C J      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 N T O F Z X V Y I      C D K A Q 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 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 V K H Y Q X J      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 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 T      E W Q D X Z 15
XPDVEONG  A M J C L S K R Y B Z H W U Q I F X P D V E O N G T    M J C L S K R Y B Z
          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      H R Y G Q J E N I P F X A T O K D U B Z M V C 11
QLXH      R I J W M A S Z C P B K V D N T F Q U E G Q L X      A S Z C P B K V D N T F Q U E G 2
FUCLTOBJ  E X D P I K S H W R G V N Q A M Z F U C L T O
GQKWEFOX  P J J Y A Z N V I M B R H U L S C T G Q K W
MDZAH NY  O B J X I U K R V E F Q T L P C S M D Z A
```

```
                              RJUYCTSHBVFKWDM        GLANQXPZ|RJ      CTSHBVFKWDMEOIGLANQXPZ 14
NHZMJIRAXLGKQECFPBSODWYUVT|NHZMJIRAXLGKQE€          BSODWYUVT 16
EYNXMTDLOCUQKBJPFZHSGAWRIV|EYNXMTDLOCUOK           PFZHSGAWRI
              NUPCTIOEHMYRDGVKXBFSLZJ              ANUPCTIOEH       RDGVKXBFSLZJWQA 6
       MXJWBKHQGPZLCUNERDOIFAYTVSM                 BKHQGPZLCU       RDOIFAYTVS 22
                XLFZKEJUHRGBWMIDNYTQ               SVP|XLFZKEJ      RGBWMIDNYTQAOCSVF 25
NAYMZOBXKTJQFUPHVELCRIWGSD|NAYMZOBXKT              UPHVELCRIW       D 23
              HSRYVGZDQOXEKUMANJC                 PLIF|HSRYVG      OOXEKUMANJCWBTPLIF 5
               PLZEXYDJTIFUQKARHC                 GWOSN|PLZEX      JTIFUQKARHCVMBGWOSN 12
WMYELVKNFRQGAOCHPBJSDIUZXT|WMYELVKNF              AOCHPBJSDI       XT 24
JHLKTIRCSMGQVDZPEXBYNWFUOA|JHLKTIRCSMG            ZPEXBYNWFU       13
ELOOFHTGNAMXKIPBRDSJCVYZWU|ELOOF                  NAMXKIPBRD       CVYZWU 21
       EVOZGSFUOIPRNKBLHCMATJD                    EVOZGSFUOI       NKBLHCMATJDXWY 18
  KUYJWSALPVBINGQCXNFZEHROTDK                     WSALPVBING       XNFZEHROTD 1
HGZOWIBPVTAEOKCJMDSLUYNXFR|HGZOW                  VTAEOKCJMD       UYNXFR 7
                VYIWRJCDKAQSHPBLE                 NTOFZX|VYIW      CDKAQSHPBLEMUGNTOFZX 17
YQHZPCXFRNDIMEASGKJVBUOTWL|YQHZPCXFRNDIME         KJVBUOTWL 20
          KHYQXJIPATGNLCROBESDU                   ZV|KHYQXJIP      GNLCROBESDUNFWZV 19
  GUKYHSJRCIMVLPNATBFOEWODXZ|GUKYA                CIMVLPNATB       EWODXZ 15
  HWUQIFXPDVEONGTAMJCLSKRYBZ|HWUC                 PDVEONGTAM       LSKRYBZ 8
              LWSHRYGOJENIPFXATOK                 ZMVC|LWSHRY      JENIPFXATOKDUBZMVC 11
              QLXHYRIJWMASZCPBKVD                 QUEG|QLXHYR      WMASZCPBKVDNTFOUEG 2
          SHWRGVNQAMZFUCLTOBJYEXD                 SHWRGVNQAM       UCLTOBJYEXDPIK 3
     JYAZNVIMBRHULSCTGQKWEFOXDR                   ZNVIMBRHUL       TGOKWEFOXDP 10
     JXIUKRVEFQTLPCSMDZAHGNYWQ                    IUKRVEFQTL       SMDZAHGNYWOB 4
```

```
R J
EYNXMTDLOCUQKBJPF
NUPCTIOEHMYRDG
NAY
PLZ
WMYELVK
JHLKTI
ELOQFHTGNAMXKIPBF
EVQ    SFUOIPRNKBLHCMA
KUYJW
HGZQWI
VYIWR
YQHZ CXFRNDIMEASGKJ
KHYQXJIPATGNLCROBESDU
GUKV        IMVLPNAT
LWSHRYGQ
```

```
SHBVFKWDMEOIGLANQXPZ|RJUYCT|SHBVFKWDM OIGLANQXIZ|14
NHZMJIRAXLGKQECFPBSODWYUVT|NHZMJIRAXIGKQEC PBSODWYUVT|1
AWRIV|EYNXMTDLOCUQKBJPFZHSGAWRIV|9
FSLZJWQA|NUPCTIOEHMYRDGVK BFSLZJWQA|6
JWBKHQGPZLCUNERDOIFAYTVS|MXJWBKHQGPZLCUNFRDOIFAYTVS|2
LFZKEJUHRGBWMIDNYTQAOCSVP|XIFZKEJUHHCBWNIDNYIQAOC VP2
XKTJQFUPHVELCRIWGSD|NAYMZOBXKTJQFUPHVELCRIVGSD|23
RYVGZDQOXEKUMANJCWBTPLIF|HSRYVCZDQOXEKUMAFJCVRTPLIFS
JTIFUQKARHCVMBGWOSN|PLZEXYDJTIFUQKARHCVMBCWOSN|12
GAOCHPBJSDIUZXT|WMYELVKNFROGAOCHPBJSDIUZXT|24
GQVDZPEXBYNWFUOA|JHLKTIRCSMGQVDZPEXBY WFUOA|13
VYZWU|ELOQFHTGNAMXKIPBRDSJCVY7WU|21
WY|EVQZGSFUOIPRNKBLHCMATJDXWY|18
VBIMGQCXNFZEHROTD|KUYJWSALPVBIMGQCXNFZEHROTD|1
AEOKCJMDSLUYNXFR|HGZQWIBPVTAEOKCJMDSLUYNXFR|7
AQSHPBLEMUGNTOFZX|VYIWRJCDKAQSHPBLEMUGNTOFZX|17
TWL|YQHZPCXFRNDIMEASGKJVBUOTWL|20
VKHYQXJIPATGNLCROBESDUMFWZV|19
WQDXZGUKYHSJRCIMVLPNATBFOEWODX|15
WUQIFXPDVEONGTAMJCLSKRYBZ|HWUQIFXPDVEONGTAMJCLSKRYBZ|8
PFXATOKDUBZMVC|LWSHRYGQJENIPFXATOKDUBZMVC|11
LXHYRIJWMASZCPB|DNTFOUEGQLXHYRIJWMASZCPBKVDNTFOUEG
HWRGVNQAMZFUCL|YEXDPIK|SHWRGVNQAMZFUCLTOBJYEXDPIK|3
AZNVIMBRHUL|FOXDPJYAZNVIMBRHULSCTGQKWEFOXDP|10
IUKRVEFQ|WOBJXIUKRVEFQTLPCSMDZAHGNYWOB|4
```

RJU	CTSHBVFKWDMEO	ANOXPZ RJUYCTSHBVFKWDMEOIGLANQXPZ 14	
	NHZMJIRAXLGK	CFPBSODWYUVT NHZMJIRAXLGXQECFPBSODWYUVT 16	
EYNXMTDLOCUQKBJPFZ	SGAWRIV EYNXMTD	CUOKBJPFZ HSGAWRIV S	
NUPCTIOEHMYRDGV	XBFSLZJWQA NUPC	OEHMYRDGVK XBFSLZJWQA 6	
	MXJWBKHQGPZLCB	RDOIFAYTVS MXJWBKHQGPZLCUNERDOIFAYTVS 22	
	XLFZKEJUHRGB	DNYTQAOCSVP XLFZKEJUHRGBWMIDNYTQAOCSVP 23	
NAYM	OBXKTJQFUPHVEL	IWGSD NAYMZOBXKTJQFUPHVELCRIWGSD 23	
	HSRYVGZDQOXEK	NJCWBTPLIF HSRYVGZDQOXEKUMANJCWBTPLIF S	
PLZE	YDJTIFUOKARHC	GWOSN PLZEXYDJTIFUOKARHCVMBGWOSN 12	
WMYELVKN	RQGAOCHPBJSDI	TWMYELVKNFRQGAOCHPBJSDIUZXT 24	
JHLKTIR	SMGQVDZFEXBYN	OA JHLKTIRCSMGQVDZFEXBYNWFUOA 13	
ELOQFHTGNAMXKIPBRD	JCVYZWU ELOQFH	AMXKIPBRDSJCVYZWU 21	
EVQZGSFUOIPRNKBLHCMAT	DXWY EVQZGSFUQ	NKBLHCMATJDXWY 18	
KUYJWS	LPVBIMGQCXNFZ	OTD KUYJWSALPVBIMGQCXNFZEHROTO 1	
NGZQWIB	VTAEOKCJMDSLU	FR HGZQWIBPVTAEOKCJMDSLUYNXFR 7	
VYIWRJ	DKAQSHPBLEMUG	FZX VYIWRJCDKAQSHPBLEMUGNTOFZX 17	
YQHZFCXFRNDIMEASGKJV	UOTWL YQHZPCXF	IMEASGKJVBUOTWL 20	
KHYQXJIPATGNLCROBESDUM	WZV KHYQXJIFAT	CROBESDUMFWZV 13	
GUKYHSJRCIMVLPNATX	OEWQDXZ GUKYHS	IMVLPNATBFOEWQDXZ 15	
	HWUQIFXPDVEO	AMJCLSKRYBZ HWUQIFXPDVEONGTAMJCLSKRYBZ 8	
LWSHRYGQ	HIPFXATQKDUBZ	LWSHRYGQJENIPFXATQKDUBZMVC 11	
OLXHYRIJWMASZG	BKVDNTFOUEGQL	RIJWMASZCPBKVDNTFOUEG 2	
SH	GVNQAMZFUCLTO	EXDPIK SHWRGVNQAMZFUCLTOBJYEXDPIK 3	
JYAZNVI	RHULSCTGQKWEF	IJYAZNVINBRHULSCTGQKWEFOXDPU	
JXIUKR	FQTLPCSMDZAHG	UB JXIUKRVEFQTLPCSMDZAHGNYWOB 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 J U Y C T S H B V F K W D M E      A N Q X P Z 14
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        O D W Y U V T 16
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            Z H S G A W R I V 9
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 H M Y R D G V K X B F S L Z J
M X 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                                 H Q G P Z L C U N E R D O I F A Y T V S 22
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 J U H R G B W M I D N Y T Q A    P 25
N A Y M Z O B 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                H V E L C R I W G S D 23
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 G Z D Q O X E K U M A N J C W      I F 5
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 X Y D J T I F U Q K A R H C V        O S N 12
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                  C H P B J S D I U Z X T 24
J H L K T I R C S M G Q 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 Q              E X B Y N W F U O A 13
E L O Q 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 Q F H                          M X K I P B R D S J C V Y Z W U 21
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 I P R N K B L H C M A T J D X
K U Y J W S A L P V B I M G Q C X N F Z E H R O T D | K U                                  A L P V B I M G Q 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 Y N X F R | H G Z Q W I                          A E O 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 N T O F Z X | V Y I W R J C D K A Q S H P B L E M   O F Z X 17
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         V B U O T W L 0
K H Y O X J I P A T G N L C R O B E S D U M F W Z V | K H Y O X J I P A T G N L C R O B E S D U M    19
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                          M V L P N A T B F O E W Q D X Z 15
H 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 Q I                            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 J E N I 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    V C 11
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 | Q L X H Y R I J W M A S Z C P B K V D N    E G 2
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 | S H W R G V N Q A M Z F U C L T O B J Y E X D P
J Y A Z N V I M B R H U L S C T G Q K W E F O X D P | J                                    V I M B R
J X I U K R V E F Q T L P C S M D Z A H G N Y W O B | J X I U K R V E F Q T L P C S M D Z A H G N Y W O B
```

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	C T S H B V F K W D M E O I	A N Q X P Z 14
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	M J I R A X L G K Q E C F P	O D W Y U V T 16
E Y N X M T D L O C U Q K B J P F Z H S G A W R	Y N X M T D L O C U Q K B J	Z H S G A W R I V 9
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	R D G V K X B F S L Z J W O	
M X J W B K H Q G P Z L C	R D O I F A Y T V S M X J W	H Q G P Z L C U N E R D O I F A Y T V S 22
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	R G B W M I D N Y T Q A O C	P 25
N A Y M Z O B X K T J O F U P H V E L C R I	D N A Y M Z O B X K T J O F	H V E L C R I W G S D 23
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	Q O X E K U M A N J C W B T	I F 5
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	J T I F U Q K A R H C V M B	O S N 12
W M Y E L V K N F R Q G A O C H P B J S D	X T W M Y E L V K N F R Q G	C H P B J S D I U Z X T 24
J H L K T I R C S M G Q V D Z P E X B Y N W F	J H L K T I R C S M G Q V D	E X B Y N W F U O A 13
E L O O F H T G N A M X K I P B R	C V Y Z W U E L O Q F H T G	M X K I P B R D S J C V Y Z W U 21
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	N K B L H C M A T J D X W Y	
K J Y J W S A L P V B I M	X N F Z E H R O T D K U Y J	A L P V B I M G Q 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	U Y N X F R H G Z Q W I B P	A E O 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 N T O F Z X V Y I	C D K A Q S H P B L E M U G	O F Z X 17
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	Z P C X F R N D I M E A S G	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 M F W Z V K H Y Q X J I	G N L C R O B E S D U M F W	19
G U K Y H S J R C I M V L P N A T	E W Q D X Z G U K Y H S J R	M V L P N A T B F O E W Q D X Z 15
H W U Q I F X P D V E O N G T A	L S K R Y B Z H W U Q I F X	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 J E N I P F X A T O K D U B Z M V C L W S H R	J E N I P F X A T O K D U B	V C 11
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 Q L X H Y	W M A S Z C P B K V D N T F	E G 2
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 S H W R G V N Q A	U C L T O B J Y E X D P I K	
J Y A Z N V I M B R H U	T G Q K W E F O X D P J Y A	V I M B R H U L S C T G Q K W E F O X D P 10
J X I U K R V E F Q T L P C S M D Z A H G N Y W O B J X I U K R V E F Q T	S M D Z A H G N Y W O B 4	