

~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland



MARCH 1974



**DRAGON
SEEDS**

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

Dragon Seeds is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

Dragon Seeds is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Publisher

DONALD E. MCCOWN, CHIEF B4

Managing Editor
Minnie M. Kenny

Executive Editor
Robert S. Benjamin

Rewrite Editor
Jane E. Dunn

Special Interest Editor
Ray F. Lynch

Feature Editor
Robert F. Kreinheder

Education Editor
Marian I. Reed

Composition

Louella M. Ertter

PRESS CORPS

B11	Carolyn Y. Brown	B42	Peggy Barnhill
B2	George S. Patterson	B43	Mary Ann Laslo
B31	Jack Spencer	B61	<input type="text"/>
B32	Jean Gilligan	B62	Edmund J. Guest
B33	Louis Ambrosia	B63	William Eley
B41	James W. Schmidt	B65	Philip J. Gallagher

~~TOP SECRET UMBRA~~



VOL 3
NR 1

MARCH 1974

TABLE OF CONTENTS

GURUJI: A Natural History of GUPPIES...Virginia Jenkins	1
GUPPIES: Alphabetical Guide.....	4
Categorical Guide.....	8
Cryptosystem Guide.....	11
The Open Door: A Peebles to People Message.....	
..... Sally Peebles	20
B Signals Lab Capabilities and Mission.....Robert Earles	24
Return of the Exiles.....	25
Seedlings.....	26
Ask the Dragon Lady.....	29
Contributors.....	30
Index of Previous Issues.....	31

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

WHAT OTHERS TAUGHT
I ALSO TEACH.

THE KNOWLEDGE OF CONSTANCY
I CALL ENLIGHTENMENT AND SAY
THAT NOT TO KNOW IT
IS BLINDNESS THAT WORKS EVIL.

至
聖
先
師



BE DONE WITH ROTE LEARNING
AND ITS ATTENDANT VEXATIONS!

BY THIS I KNOW THE BENEFIT
OF SOMETHING DONE BY QUIET BEING;
IN ALL THE WORLD BUT FEW CAN KNOW
ACCOMPLISHMENT APART FROM WORK,
INSTRUCTION WHEN NO WORDS ARE USED.

---Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ALWAC III

A NATURAL HISTORY OF GUPPIES

Virginia Jenkins, E13

The GUPPIES on RYE are a collection of over one hundred computer programs, designed and for the most part written by cryptanalyst programmers, to handle many of the standard cryptanalytic tasks performed daily throughout the Agency. The name "GUPPY" comes from the initials of General Utility Programs. This article tells in brief how general cryptanalytic programs, cryptanalyst programmers and remote-operated computers grew up together at NSA.

ROGUE, ROB ROY AND RYE

The GUPPIES were born (but were not yet named) with ROGUE,¹ NSA's first remote-operated computer system, in 1956.² Open-shop programming--programming of their own work by local analysts--started at about the same time. It seems to have been realized rather early that cryptanalysts who could program their own jobs had a valuable tool in their tool boxes, and that the best desk-side aid for any cryptanalyst was a computer program he could run himself from his working area. ROGUE provided both possibilities. It boasted four outstations.

The tradition grew, and so did the number of users, open-shoppers, and programs. The five outstations of ROB ROY,³ which succeeded ROGUE in 1960, were busy and productive. ROB ROY was popular in spite of long waits for input, one-job-at-a-time processing, and paper tape as the only mode of output.

1. Remotely-Operated General Use Equipment. The computer was the ALWAC IIIE.

2. ROGUE in fact was one of the first in the country. Monograph #2 in the NSA Technical Literature Series, HISTORY OF NSA GENERAL-PURPOSE ELECTRONIC DIGITAL COMPUTERS, by Samuel S. Snyder, tells the story. Some of the information in this article is based on that monograph.

3. The computer, originally designed as an editing computer, was named BOGART after the city editor of the New York SUN. The name ROB ROY was not an acronym, but popular ingenuity explained it as one: "Remotely Operated BOGART--Remotely Operated by You."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The outstation looked like a modified government gray desk. Paper tape was output through a hole in the bottom righthand drawer, and hard copy was produced off-line by reading the paper tape through a Flexwriter. I counted about 80 general and special-purpose programs in a ROB ROY manual I came across recently, many of them with familiar names like BAYOU, HUSK, STET, and DIANA.

In 1963, ROB ROY was replaced by RYE.⁴ The extent to which analysts had come to depend on doing their cryptanalysis by computer can be measured by the large number of programs--now for the first time called "GUPPIES"--programmed for the new remotely-operated system, and by the numerous outstations used. At present, RYE outstations number more than 150. Indeed, the demands for service have at times outweighed RYE's ability to fill them. As a result, many GUPPY programs have been rewritten for other computers, notably for DCS,⁵ starting in 1966.

From very early, and increasingly as time went on, the cryptanalyst programmers designed their programs to be both "General" and "Utility."

The "Utility" portion of the GUPPY name stems from the fact that many of these programs are computerized versions of the day-to-day standard cryptanalytic tasks performed all over the Agency. Some in fact were, and are, versions of pre-computer specialized equipment, like GEEWHIZZER which was originally the name of an Electro-Mechanagrammer. All cryptanalysts, whether they work manual or machine cryptosystems, are generally concerned with substitution, transposition, or some combination of the two. And all cryptanalysts need worksheets, frequency counts, statistics, decrypts, and indexes; they need to drag cribs and to test keys in order to do their jobs. These are like electricity and water "utilities" to the cryptanalysts, and many are handled by the GUPPY programs.

Flexible parameters make the GUPPY programs "General." One cryptosystem differs from another primarily in the crypto-variables (figures, cipher alphabets, and keys) associated with it, its character set, and the underlying language. Most GUPPIES are not limited either in the kind of data they accept or the way they handle it. Almost all of them contain a generalized parameter-handler routine that allows the user to tailor a program to his specific needs.

4. RYE is not an acronym. Two computers--UNIVAC 490 and UNIVAC 494--have been used on this system.

5. Direct-Coupled System, using IBM hardware.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

For example, the GUPPY programs will accept a character set 2 through 64 long; data can be prepared on paper tape or cards, or on a variety of equipment (ASR-35, CXCO, FLEX). Options abound for specifying arithmetic (additive, subtractive, minuend, Baudot), widths, graph sizes, sort fields, and data arrangement. Thresholds can often be changed, specialized log weights input, and instructions for formatting of printout given.

Descriptions of the GUPPY programs are published in the GUPPY Manuel available from Mrs. Linda Sweeney, C4, phone 3829s. This publication is available to any interested cryptanalyst. In addition, the use of RYE and of the GUPPY programs is taught in three courses conducted by the Cryptanalysis Department of the NCSch. They are: General Cryptanalysis (CA-100), Practical Diagnosis (CA-260), and Rye Operations for Cryptanalytic Applications (CA-090). The latter course is a new one; the pilot class was held in March 1973.

In G Group, Mr. J. D. Tankersley is always available to give assistance on RYE both to cryptanalysts and to open-shoppers. In his office, 3A111 (phone 4727s), he maintains a file of all the GUPPY program assemblies and a library of punched paper tapes of plain text and weights for some of the G Group languages. He also serves as GUPPY trouble shooter and is the person to call if a program seems to be in trouble.

Instructors in the Cryptanalysis Department are also glad to assist cryptanalysts in using RYE in any way they can. The phone number of 8025/36; the room number in FANX II is A2A32B.

* * * *

TRANSLATION, PLEASE?

SAVILLE DER DAGO
TOUSEND BUZES IN ARO
NOCHOE DEM IST TROUXS
SUMMIT COUZIN
SUMMIT DOUXS

Vince Las Casas, B6

(See answer on page 28)

3

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

An Alphabetical Guide to the GUPPIES

- * [PROGRAMS WHICH PUNCH TAPES AS WELL AS PRINT ARE MARKED WITH AN ASTERISK.] *
- + [BAUDOT PROGRAMS OR ONES WITH BAUDOT OPTIONS ARE MARKED WITH A PLUS SIGN.] +
- ASKIT: Predicts or evaluates results of polyalphabetic depth search based on Kappa test.
- +BALK: Prints worksheet, 3 to 100 characters per line.
- *BAYOU: Prints monographic and digraphic frequency counts, log and category weights for chained, disjointed or transposition digraphs.
- +*BDELT: Makes Baudot horizontal or intermessage difference streams.
- +BEE: Prints binary 5-level differences and statistics.
- BIGSTET: Standard diagnostic STET tests on option, some with thresholds, but handles more data, widths, intervals and prints columnar counts.
- BISEC: Key recovery and decryption via generatrices and scores, for monoalphabetic in fixed-length-section cipher.
- BREN: Route and grille transposition decrypt, span < 450.
- +BUNK: Key drag and difference stream, Baudot arithmetic.
- CALC: Desk calculator functions: +, -, x, /, exponentiation, square root, number base change.
- CASANOVA: Periodic polyalphabetic intermessage depth search, individual or all monographic column pairs on a width.
- CHICKADEE: Diagnoses and exploits stagger bust.
- COLLEEN: Mono-, di-, and trigraphic columnar counts and statistics on a width.
- COPPERHEAD: Polyalphabetic polygraphic depth search.
- CRAZYQUILT: Transposition bust exploitation.
- CROSSUM: Cross-product sums and repeat rates at all slides for all pairs of N frequency distributions.
- DELPHI: Key recovery and decryption, periodic polyalphabetic, related or unrelated alphabets.
- +*DELT: Horizontal or intermessage differences or sums, modular or Baudot arithmetic.

~~TOP SECRET UMBRA~~

+*DELTBDELT: 


DIANA: Digraphic counts and statistics.

*DØBE: Uniliteral (1 for 1) substitution decrypt or conversion.

*DØBE2: Biliteral (2 for 1) substitution decrypt or conversion.

DOODLE: Formatted worksheets, specified hits underlined. Hat and crenelated diagrams.

+DOPESHEET: Probabilistic worksheet for polyalphabetic depth reading.

EPICTETUS: Enciphered indicator search.

+FINKSBURG: Diagnostics on levels of 5-level streams.

FLUSH: Aperiodic polyalphabetic depth search.

FREQWIDTH: Prints formatted worksheet, with count below each group.

GEEWHIZZER: Anagrams columnar and grille transposition.

+*GEORGE: General purpose encipher/decipher of transposition, monoalphabetic and polyalphabetic substitution and Hagelin. Related or unrelated alphabets.

+*GIMP: Polyalphabetic crib drag.

GROUPDATA: Prints formatted worksheets.

+HUSHPUPPY: Polyalphabetic crib and key drag. Monographic log weights.

INDEX: Index and frequency counts, user-specified sort order.

ISOM: Locates isomorphs.

JEZEBEL: Decrypts biliteral substitution. Coordinates may be summed, with variants, or appear nonconsecutively in cipher.

KRAKUP: Tests for cyclic phenomena in nonhomogeneous material.

KYOTO: Tests and exploits stagger bust situation in polyalphabetic.

*LACER: Interlaces 2 data streams to user specification.

LAMBRØS: Key recovery and decryption via generatrices and scores for periodic polyalphabetic.

LILINDEX: Index and frequency counts, user-specified sort order, limited amount of data.

+LOGDIFF: Computes monographic plain and theoretical difference log weights.

~~TOP SECRET UMBRA~~

MARTEE: Recovers key length for monoalphabetic-in-fixed-length encipherment.

+*MASK: Deletes characters or levels on cycling basis.

MODIRA: Coordinate recovery for monomedinome.

MONDIN: Prints monome-dinome worksheets and decrypts.

+MONDITRI: Mono-, di-, and trigraphic frequency counts of selected levels and level combinations.

MONOSEC: Replaces MARTEE (same options).

MYSTARS: Sorts 2-5 character groups from 1 stream; differences and sorts differences from 2 streams.

*NEPTUNE: Decrypts transposition within span of 100.

OVERLAP: 


PASDEDEUX: 


+PICKWICK: Theoretical cipher distribution and log weights for polyalphabetic.

POLLY: Lists overall and oncut polygraphic repeats. Statistics.

PROFILE: Displays trilateral frequency distribution a la MC-I, pg. 72.

PUSHUP: Tests polyalphabetic depths and prints depth reader's worksheet.

QUIKROB: Polyalphabetic depth test, modified Kappa scoring on limited data.

QUIKSTET: STET on limited data.

QUIKTWIST: TWIST on limited data.

QUIKWHIZ: GEEWHIZZER on limited data.

QUIKXIBAR: XIBAR on limited data. No frequency counts option.

RITWIDTH: General purpose worksheet preparation, user specifications.

ROBIN: Polyalphabetic depth search.

ROLLFAST: Generatrices for 1 stream or pairs of 2 or 3 streams, formatted output.

RUMDUM: Sorts message identification streams prepared for INDEX.

SALLY: Prints monome-dinome frequency count.

+SCOOT: Polyalphabetic crib and key drag. Tetragraphic weights and cribs from TAPIR.

~~TOP SECRET UMBRA~~

SHADOW: Profile monographic frequency count on data and on horizontal delta. Statistics.

SMARTSET: STET plus chi-square; threshold option.

STET: Prints standard diagnostic statistics and counts.

STUBBY: Remainder test.

+SUMDIF:



SYLLABLE: General purpose matrix decrypt (up to 36x36), plain and cipher unit sizes 1-5.

SYNDROME: Coordinate recovery, worksheets, frequency counts and decryption for monome-dinome.

TABLES: Tailor-made mathematical tables: chi-square and binomial probabilities; prime factors and numbers; combinations N things r at time; transposition column factors and matrix widths.

TAPECON: Produces hard copy from paper tape, acting on functions.

+*TAPIR: Alphabetic, inverse frequency lists and log weights for 3, 4, 5 character groups.

TASKAN: Single, double transposition key test.

THUD: Makes depth reader's worksheet.

TREES: General purpose book-breaker's package: counts, indexes, WMP's, codebooks, et al.

TWIST: Single, double transposition decrypt.

UNICORN: Stripped-down version of SHADOW.

*UNLACER: Creates 2 data streams from 1 according to user specifications.

+*VIGORO: Creates streams of X's and O's from 5 or 6 level tape.

+WARP: Difference or decrypt polyalphabetic substitution.

+WENDY: Prints binary worksheet (X's and O's) from 5 level characters.

WIDTH: Prints frequency counts and statistics for columns of width write-out.

XIBAR: Makes frequency counts overall on individual messages or on columns of width and subdivides them into homogeneous sets.

*XPAN: Creates data stream expanded positionally by specified characters.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

A Categorical Guide to the GUPPIES

Anagram

GEEWHIZZER
QUIKWHIZ

Baudot

BALK
BDELT
BEE
BUNK
DELTBDELT
DOPE SHEET
FINKSBURG
GEORGE
GIMP
HUSHPUPPY
LOGDIFF
MASK
MONDITRI
PICKWICK
SCOOT
SUMDIF
TAPIR
VIGORO
WARP
WENDY

Binary

BEE
FINKSBURG
MASK
MONDITRI
VIGORO
WENDY

Binomial

TABLES

Bookbreaking

FREQWIDTH
GOUPTDATA
INDEX
LILINDEX
POLLY
RITWIDTH
TAPIR
TREES

Bust Exploitation

CHICKADEE
CRAZYQUILT
KYOTO

Chi-Square

FINKSBURG
SMARTSTET
TABLES

Conversion

See Decryption

Crenelated

Diagram

DOODLE

Crib/Key Drag

BUNK
GIMP
HUSHPUPPY
SCOOT

Data Processing

BALK
LACER
MASK
ROLLFAST
(Cont'd in next
column)

TAPECON
UNLACER
VIGORO
XPAN

Decryption for Substitution

BISEC
DELPHI
DELT
DELTBDELT
DOBE
DOBE2
GEORGE
JEZEBEL
LAMBROS
MONDIN
SYLLABLE
TREES
WARP

Decryption for Transposition

BREN
GEORGE
NEPTUNE
QUIKTWIST
TWIST

Depth Test

ASKIT
CASANOVA
COPPERHEAD
CROSSUM
FLUSH
PUSHUP
QUIKROB
ROBIN

Desk Calculator

CALC

~~TOP SECRET UMBRA~~

Differences

BDELTA
BEE
BUNK
DELTA
DELTABDELTA
MYSTARS
OVERLAP
ROLLFAST
SHADOW
SUMDIF
WARP

Frequency Counts

BAYOU
BIGSTET
COLLEEN
DIANA
FREQUENCY
INDEX
LILINDEX
MONDIN
MONDITRI
PROFILE
QUIKSTET
QUIKZIBAR
SALLY
SHADOW
SYNDROME
TAPIR
UNICORN
WIDTH
XIBAR

Frequency Profiles

PROFILE
SHADOW
UNICORN

Generatrices

BISEC
LAMBROX
ROLLFAST

Hat Diagram

DOODLE

Homogeneity

BIGSTET
QUIKSTET
QUIKXIBAR
STET
XIBAR

I.C. and/or Sigmage

ASKIT
BEE
BIGSTET
CASANOVA
COLLEEN
CROSSUM
DELTA
DELTABDELTA
DIANA
EPICTETUS
GDELTA
KRAKUP
MARTEE
MONOSEC
MYSTARS
PASDEDEUX
POLLY
PUSHUP
QUIKSTET

QUIKXIBAR
SHADOW
SMARTSTET
STET
TAPIR
UNICORN
WIDTH
XIBAR

Index

INDEX
LILINDEX

Indicators

EPICTETUS
INDEX
MYSTARS
RUMDUM
SUMDIF

Inverse Frequency

TAPIR
TREES

Isomorphs

ISOM

Key/Alphabet Test

BISEC
DELPHI
DOPE SHEET
LAMBRØS
TASKAN

Local Roughness

BIGSTET
MARTEE
MONOSEC
QUIKSTET
SMARTSTET
STET

Log Weights

BAYOU
LOGDIFF
PICKWICK
TAPIR

Math Tables

TABLES

Matrix Factors/
Dimensions

TABLES



DELTBDELT
OVERLAP
SUMDIF

Monome-To-Dinome
Ratio

MODIRA

Polygraphic Repeats

BIGSTET
COLLEEN
COPPERHEAD
DOODLE
INDEX
LILINDEX
MYSTARS
OVERLAP
POLLY
QUIKSTET
STET
SUMDIF
TAPIR

Prime Factors/
Numbers

TABLES

Probability
Tables

TABLES

Remainder Test

STUBBY

Repeat Rate

COLLEEN
CROSSUM
DIANA
KRAKUP
SYNDROME
TAPIR
UNICORN

Sorts

INDEX
LILINDEX
MYSTARS
OVERLAP
SUMDIF
TAPIR

Statistics

See Chi-Square,
I.C. Sigmage,
Log Weights
Repeat Rate

Stub Test

STUBBY

Theoretical Cipher

LOGDIFF
PICKWICK

Variants

BIGSTET
GEORGE
INDEX
QUIKSTET
STET
SYLLABLE

Widths

BIGSTET
CASANOVA
COLLEEN
CROSSUM
DOODLE
KRAKUP
LAMBROS
OVERLAP
PASDEDEUX
QUIKSTET
SMARTSTET
STET
WIDTH
XIBAR

Worksheets

DOODLE
FREQWIDTH
GROUPDATA
MONDIN
PUSHUP
RITWIDTH
SYNDROME
THUD
WENDY

~~TOP SECRET UMBRA~~

Cryptosystem Guide to the GUPPIES

Following is a list of the cryptosystems covered in this Guide:

1. MONOALPHABETIC SUBSTITUTION -
Unilateral; bilateral; monome-dinome; matrix (bipartite, digraphic); code.
2. PERIODIC POLYALPHABETIC AND CYCLIC ADDITIVE SUBSTITUTION.
3. APERIODIC POLYALPHABETIC AND NONCYCLIC ADDITIVE SUBSTITUTION -
General; Baudot; binary; ciphertext autokey; Hagelin; monoalphabetic in fixed-length section; progressive.
4. TRANSPOSITION -
General; bisection, railfence; columnar (single, double); grille, local, route; transposed code.
5. PLAINTEXT PROCESSING

<u>UNILITERAL</u>	<u>FREQUENCY PROFILES</u>	<u>INDEX, SORTS</u>
<u>CHI-SQUARE</u>	FREQWIDTH	INDEX
<u>SMARTSET</u>	INDEX	LILINDEX
<u>TABLES</u>	LILINDEX	
<u>DECRYPTION</u>	QUIKXIBAR	<u>KEY/ALPHABET TEST</u>
DOBE	STETs	LAMBROS
GEORGE	XIBAR	
LAMBROS		<u>NULLS, MASKS</u>
	<u>HOMOGENEITY</u>	GEORGE
<u>DIAGNOSIS</u>	CROSSUM	MASK
STETs	QUIKXIBAR	
	STETs	<u>POLYGRAPHIC REPEATS</u>
<u>DIFFERENCES</u>	XIBAR	DOODLE
DELT	<u>I.C.</u>	INDEX
DELTBDELT	DELT	LILINDEX
ROLLFAST	DELTBDELT	POLLY
SHADOW	POLLY	STETs
	PUSHUP	
	QUIKXIBAR	<u>REPEAT RATE</u>
	SHADOW	CROSSUM
	STETs	UNICORN
	UNICORN	
	XIBAR	

~~TOP SECRET UMBRA~~

<u>VARIANTS</u> DOBE GEORGE INDEX	<u>I.C.</u> BAYOU COLLEEN DIANA MYSTARS STETS	<u>MONOME-DINOME</u> <u>COORDINATE RECOVERY</u> MODIRA SYNDROME
<u>WEIGHTS</u> BAYOU LOGDIFF	<u>INDEX, SORTS</u> INDEX LILINDEX MYSTARS	<u>DECRYPTION</u> MONDIN SYNDROME
<u>WORKSHEETS</u> DOODLE FREQWIDTH GROUPDATA PUSHUP RITWIDTH THUD	<u>NULLS, MASKS</u> DIANA MASK	<u>DIAGNOSIS</u> STETS SYNDROME
<u>BILITERAL</u>	<u>POLYGRAPHIC REPEATS</u> COLLEEN DOODLE INDEX LILINDEX MYSTARS POLLY STETS	<u>DIFFERENCES</u> DELT DELTBDELT
<u>DECRYPTION</u> DOBE2 JEZEBEL SYLLABLE	<u>REPEAT RATE</u> COLLEEN DIANA	<u>FREQUENCY COUNTS</u> MONDIN SALLY SYNDROME
<u>DIAGNOSIS</u> STETS	<u>VARIANTS</u> DOBE2 SYLLABLE JEZEBEL INDEX	<u>HOMOGENEITY</u> STETS SYNDROME
<u>DIFFERENCES</u> DELT DELTBDELT MYSTARS	<u>WEIGHTS</u> BAYOU LOGDIFF	<u>I.C.</u> BAYOU DELT DELTBDELT POLLY STETS
<u>FREQUENCY COUNTS</u> BAYOU COLLEEN DIANA FREQWIDTH INDEX LILINDEX	<u>WORKSHEETS</u> DOODLE FREQWIDTH GROUPDATA RITWIDTH	<u>INDEX, SORTS</u> INDEX LILINDEX
<u>HOMOGENEITY</u> DIANA QUIKKIBAR STETS XIBAR		<u>MONOME-TO-DINOME</u> RATIO MODIRA

~~TOP SECRET UMBRA~~

<u>POLYGRAPHIC REPEATS</u> DOODLE INDEX LILINDEX POLLY STETs	<u>HOMOGENEITY</u> DIANA STETs	<u>VARIANTS</u> INDEX JEZEBEL SYLLABLE
<u>REPEAT RATE</u> SYNDROME	<u>I.C.</u> BAYOU CASANOVA DELT DELTBDELT DIANA MYSTARS POLLY STETs TAPIR	<u>WEIGHTS</u> BAYOU TAPIR
<u>VARIANTS</u> INDEX MONDIN SYNDROME		<u>WORKSHEETS</u> DOODLE FREQWIDTH GROUPDATA RITWIDTH
<u>WEIGHTS</u> BAYOU LOGDIFF	<u>INDEX, SORTS</u> INDEX LILINDEX MYSTARS TAPIR	<u>CODE</u> <u>CODE BOOK</u> TREES
<u>WORKSHEETS</u> MONDIN SYNDROME	<u>INVERSE FREQUENCY</u> TAPIR	<u>DECRYPTION</u> SYLLABLE TREES
<u>MATRIX: BIPARTITE</u> <u>DIGRAPHIC</u>	<u>KEY/COORDINATE TEST</u> CASANOVA CROSSUM	<u>DIAGNOSIS</u> STET TAPIR
<u>DECRYPTION</u> DOBE2 JEZEBEL SYLLABLE	<u>NULLS, MASKS</u> DIANA MASK	<u>FREQUENCY COUNTS</u> FREQWIDTH INDEX LILINDEX TAPIR TREES
<u>DIAGNOSIS</u> DIANA STETs TAPIR	<u>POLYGRAPHIC REPEATS</u> DOODLE INDEX LILINDEX MYSTARS POLLY STETs TAPIR	<u>HOMOGENEITY</u> STETs TAPIR
<u>DIFFERENCES</u> DELT DELTBDELT MYSTARS	<u>REPEAT RATE</u> DIANA TAPIR	<u>I.C.</u> CASANOVA MYSTARS POLLY STETs TAPIR
<u>FREQUENCY COUNTS</u> BAYOU DIANA FREQWIDTH INDEX LILINDEX TAPIR		

~~TOP SECRET UMBRA~~

INDEX, SORTS

INDEX
LILINDEX
TAPIR
TREES
(BY CODE GP.,
MEANING,
VALIDITY, ANY
SPECIFIED
GROUPS)

INVERSE FREQUENCY

TAPIR
TREES

NULLS, MASKS

MASK

POLYGRAPHIC REPEATS

INDEX
LILINDEX
MYSTARS
POLLY
TAPIR
TREES

POSITIONAL ROUGHNESS

CASANOVA
STETs

REPEAT RATE

TAPIR

VARIANTS

INDEX
STETs
SYLLABLE

VMP

TREES

WEIGHTS

TAPIR

WORKSHEETS

FREQWIDTH
GROUPDATA
RITWIDTH

PERIODIC POLYALPHA-
BETIC AND CYCLIC
ADDITIVE

BUST EXPLOITATION
CHICKADEE
KYOTO

CHI-SQUARE
SMARTSET
TABLES

CRIB/KEY DRAG

GIMP
HUSHPUDDY
SCOOT

DECRYPTION

DELPHI
GEORGE
LAMBROS
WARP

DEPTH TESTS

CASANOVA
CROSSUM
FLUSH
PUSHUP
XIBAR
QUIKXIBAR

DIAGNOSIS

STETs

DIFFERENCES

DELT
DELTBEDELTA
MYSTARS
OVERLAP
ROLLFAST
SUMDIF
WARP

FREQUENCY COUNTS

BIGSTET
COLLEEN
QUIKXIBAR
WIDTH
XIBAR

GENERATRICES

LAMBROS
ROLLFAST

I.C.

CASANOVA
COLLEEN
DELT
DELTBEDELTA
MYSTARS
OVERLAP
POLLY
PUSHUP
QUIKXIBAR
STETs
TAPIR
WIDTH
XIBAR

INDEX, SORTS

INDEX
LILINDEX

ISOMORPHS

ISOM

KEY/ALPHABET TEST

DELPHI
LAMBROS

MATH TABLES

TABLES

DELTBEDELTA
OVERLAP
SUMDIF

~~TOP SECRET UMBRA~~

POLYGRAPHIC REPEATS

COLLEEN
DOODLE
INDEX
LILINDEX
MYSTARS
OVERLAP
POLLY
STETS
SUMDIF
TAPIR

REMAINDER/STUB TEST

STUBBY

REPEAT RATE

COLLEEN
CROSSUM
TAPIR

UNRELATED CIPHER

ALPHABETS
CASANOVA
DELPHI
GEORGE

WEIGHTS

BAYOU
LOGDIFF
TAPIR

WORKSHEETS

DOODLE
GROUPDATA
OVERLAP
PUSHUP
RITWIDTH
THUD

APERIODIC POLYALPHA-
BETIC AND NONCYCLIC
ADDITIVE

BUST EXPLOITATION

CHICKADEE
KYOTO

CHI-SQUARE

SMARTSTET
TABLES

CRIB-KEY DRAG

GIMP
HUSHPUDDY
SCOTT

DECRYPTION

DELPHI
DELT
DELTBDELT
GEORGE

DEPTH TESTS

ASKIT
COPPERHEAD
CROSSUM
FLUSH
PUSHUP
QUIKROB
ROBIN

DIAGNOSIS

STETS

DIFFERENCES

DELT
DELTBDELT
MYSTARS
OVERLAP
ROLLFAST
SUMDIF
WARP

FREQUENCY COUNTS

COLLEEN
XIBAR

GENERATRICES

ROLLFAST

I.C.

ASKIT
BAYOU
DELT
DELTBDELT
MYSTARS

POLLY
PUSHUP
QUIKXIBAR
STETS
TAPIR
XIBAR

INDEX, SORTS

INDEX
LILINDEX
MYSTARS
OVERLAP
SUMDIF

INDICATORS

EPICTETUS

ISOMORPHS

ISOM

KEY/ALPHABET TEST

DOPE SHEET

LOCAL ROUGHNESS

MARTEE
MONOSEG
STETS

MATH TABLES

TABLES

DELTBDELT
OVERLAP
SUMDIF

POLYGRAPHIC REPEATS

COPPERHEAD
DOODLE
INDEX
LILINDEX
MYSTARS
OVERLAP
POLLY
STETS

REMAINDER/STUB TEST

STUBBY

~~TOP SECRET UMBRA~~

REPEAT RATE

CROSSUM
OVERLAP
TAPIR

THEORETICAL CIPHER

LOGDIFF
PICKWICK

WEIGHTS

BAYOU
LOGDIFF
PICKWICK
TAPIR

WORKSHEETS, OVERLAP

DOODLE
PUSHUP
THUD

BAUDOT

CRIB/KEY DRAG

BUNK
GIMP
HUSHPUDDY
SCOOT

DECRYPTION

GEORGE
WARP

DIFFERENCES

BDELT
BUNK
DELTBDELT
SUMDIF
WARP

KEY/ALPHABET TEST

DOPE SHEET

SUMDIF

NULLS, MASKS

MASK

THEORETICAL CIPHER

PICKWICK

WEIGHTS

LOGDIFF
PICKWICK
TAPIR

WORKSHEETS

BALK

BINARY

CHI-SQUARE

FINKSBURG

DATE PROCESSING

VIGORO

DENSITY COUNTS

FINKSBURG

DIFFERENCES

BEE

LEVEL COUNTS

BEE
FINKSBURG
MONDITRI

MASKS

MASK

SIGMAGE

BEE
FINKSBURG

WORKSHEET

WENDY

CIPHERTEXT AUTOKEY

DECRYPTION

DELTBDELT
GEORGE

DIAGNOSIS

DIANA



MONOALPHABETIC IN
FIXED-LENGTH
SECTIONS

DECRYPTION

BISEC

GENERATRICES

BISEC

KEY/ALPHABET TEST

BISEC

LOCAL ROUGHNESS

MARTEE
MONOSEC

PROGRESSIVE

DECRYPTION

ROLLFAST

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

TRANSPOSITION

ANAGRAM
GEEWHIZZER
QUIKWHIZ

CHI-SQUARE
SMARTSTET
TABLES

CRELATED DIAGRAM
DOODLE

DECRYPTION
BREN
GEORGE
LACER
NEPTUNE
QUIKTWIST
TWIST

DIAGNOSIS
STETs

FREQUENCY COUNTS
STETs

FREQUENCY PROFILES
SHADOW
UNICORN

HAT DIAGRAM
DOODLE

I.C.
POLLY
SHADOW
STETs
TAPIR
UNICORN

INDEX, SORTS
INDEX
LILINDEX

LOCAL ROUGHNESS
STETs

MATRIX FACTORS/
DIMENSIONS
TABLES

NULLS, MASKS
GEORGE
MASK

POLYGRAPHIC REPEATS
DOODLE
POLLY
STETs
TAPIR

REMAINDER/STUB
TEST
STUBBY

REPEAT RATE
TAPIR
UNICORN

WEIGHTS
BAYOU
LOGDIFF

WORKSHEETS
DOODLE
FREQWIDTH
GROUPDATA
PUSHUP
RITWIDTH

BISECTION, RAILFENCE

DECRYPTION
LACER

COLUMNAR, SINGLE/
DOUBLE

BUST EXPLOITATION
CRAZYQUILT

DECRYPTION
GEORGE
QUIKTWIST
TWIST

KEY TEST
TASKAN

GRILLE, LOCAL, ROUTE

DECRYPTION
BREN
GEORGE
NEPTUNE

TRANSPOSED CODE

DECRYPTION
GEORGE/TREES

PLAINTEXT PROCESSING

CHI-SQUARE
SMARTSTET

DATA PROCESSING
LACER
MASK
ROLLFAST
TAPECON
TREES
UNLACER
VIGORO
XPAN

DIFFERENCES
DELT
DELTBDELT
SHADOW
SUMDIF

ENCRYPTION
GEORGE

FREQUENCY COUNTS

BAYOU
DIANA
INDEX
LILINDEX
PROFILE
SHADOW
STETS
TAPIR
TREES
UNICORN

POLYGRAPHIC REPEATS

INDEX
LILINDEX
POLLY
STETS
TAPIR

REPEAT RATE

DIANA
TAPIR
UNICORN

FREQUENCY PROFILES

PROFILE
SHADOW
UNICORN

THEORETICAL DIFFERENCE

WEIGHTS
BAYOU
LOGDIFF
PICKWICK
TAPIR

GENERATRICES

ROLLFAST

WORKSHEETS

DOODLE
PUSHUP
RITWIDTH

I.C.

BAYOU
DELT
DELTBDELT
DIANA
POLLY
SHADOW
STETS
TAPIR
UNICORN

* * * *

INDEX, SORTS

INDEX
LILINDEX
TAPIR
TREES

INVERSE FREQUENCY

TAPIR
TREES



DELTBDELT
SUMDIF



~~TOP SECRET UMBRA~~

Memorandum

TO : All Personnel concerned

FROM : Chief, color coordinating division

SUBJECT: File copies

It has been brought to my attention that a change in the standard color sorting scheme is necessary due to the loss of the green copies we have been receiving. The following steps will be taken to correct the situation until green copies are received again:

1. Blue - This copy is not received and will not be received. No change in handling is needed.
2. Green - Where green continues to be forwarded it will be filed in the green file in accordance with current procedures. This will be true at all times that green is forwarded along with yellow, pink, and gold. If forwarded without one or all of the other colors it will still be filed under green.
3. Yellow - Yellow will remain yellow and not be substituted for either green or pink. It will be held for a 30 day period and then thrown away as it is of no use at all. If it is the only copy it will be marked and placed in a special non-green file to prevent confusion.
4. Pink - Where green is not available pink will become green and be filed in the green file in lieu of green or yellow. In this case pink will NOT be thrown away. Note that pink can never be substituted for yellow.
5. Gold - If green or pink is unavailable, Gold will become green. It will be specially marked to prevent its being confused with yellow. Otherwise gold will always be thrown away.
6. White - This is not received. Handling procedures remain the same.

Please implement the above policy as appropriate.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



THE OPEN DOOR

*We seek to be companions along the way.
The lantern which we carry is not ours.
The spirit which we share is contagious thought;
The knowledge which we gain, an illuminating torch
And all who seek may perceive and learn.*

-The Concept of Dragon Seeds

A PEEBLES TO PEOPLE MESSAGE

Sally Peebles, G52, Ret.

We all expect our COMINT targets to become increasingly secure as time passes, and what we learn from reading early systems can be invaluable in enabling us to read successor, more difficult systems.

Search and Destroy Missions

Periodically we must undertake to weed out material in our over-stuffed cabinets, shelves, and desks to forestall ultimate suffocation under masses of our own paper. Nobody should argue against our cleaning our own figurative Augean Stables. It is the method of accomplishing this task that concerns me, since this job, if done ruthlessly and without informed discrimination, can seriously impair or even preclude future successes.

Youth Is Not Necessarily Beauty, Nor Beauty Youth

When the order to clean out is given, some enthusiasts zestfully fill burn bags and bulk burn boxes with anything non-current at hand in which they personally have no interest. This clean-sweep attitude promotes a feeling of accomplishment and virtue, since it makes room for new stuff and shows the boss that you are cooperating fully! However, the reckoning may come much later when the spree of "throwing out the baby with the bath water" causes analysts to waste hours, day - even months - searching for missing material, or trying to rebuild records which have been thoughtlessly destroyed.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Haven't you heard, "Whatever became of that ZEM personality file we used to have two reorganizations ago?" or, "We used to read a ZEA system. Don't we have any language patterns, any key studies, frequencies, or samples of decrypted traffic? How did that old system work?" (Have you ever tried to figure out how a system worked with no documentation except a Master File Sheet?).

One Man's Litter Is Another Man's Dead Sea Scrolls

Not too long ago I had cause to wail because somebody made a unilateral decision and threw away a precious, somewhat elderly, telephone directory which we treasured because it contained complete and explicit Order of Battle information *in clear* and *in Spanish*! Time after time this yielded answers which we could find nowhere else. (The target government got smarter after that, so that subsequent directories contained less helpful information.)

A similar invaluable, unique antique has a happier fate. This 1962 OB document I have worn thin but managed to preserve because I never let it stray from my possession. No other document provides such complete information, and *in Spanish*. (All too often we may know only the meaning or English translation of something without knowing how our special target expresses it in his own idiom.)

As for traffic, sometimes vintage traffic may be far more useful than recent stuff. Quality copy from happier days may get you farther faster than quantities of current slush even if some intervening changes in the system have been made. We all expect our COMINT targets to become increasingly secure as time passes, but what we learn from reading early systems can be invaluable in enabling us to read more difficult successor systems, whether the difficulty stems from sophistication or from the miserable quality of recent intercept.

But suppose the quality and quantity of traffic are not in question. It still is a general verity that early systems are less secure than later ones. Therefore it is wasteful and foolhardy not to squeeze as much long-term information as possible from the decryptions of early systems: the usual statistics, common beginnings and endings, characteristic expressions, etc. I never cease to be astonished at how *unlike* one another are the speech habits of different services

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



of the same country, let alone those of different countries, even though in all cases the language is Spanish. There simply is no substitute for knowing how each entity talks. So, both for now and for the future, get machine runs which can be readily manipulated to provide appropriate data on each target and see that these vital statistics are preserved and used. You can't count on maintaining continuity thanks to a goof which provides you with a golden compromise. That will be the message that didn't get intercepted!

And don't forget the treasures which may be found in plain text. The P/T reference to an encrypted message may provide you with a valuable clue to the context of the referenced message. "Think on these things" - preferably before the deadline day when your fat storage areas must lose all those pounds and reason is supplanted by muscle.

Some Suggestions and Exhortations

1. Don't entrust the "riffing" of overweight files to someone who has a limited specialty and a compartmented mind. Since some material is important for several related specialties, a person with broad experience and a long-range viewpoint should supervise destruction parties. When in doubt about the value of keeping something, don't be timid about asking knowledgeable experts to help make decisions.

2. Often there are several copies of the same material. Perhaps all but one copy, designated "Record Copy," can be thrown out. Make sure that the Record Copy is made available to all those who need it and who *return* it.

3. See if some bulky materials can't be reduced in size. That late lamented telephone directory I referred to could have been thrown away without a regret if I had first been given the opportunity to tear out and preserve about a dozen vital pages.

4. Perhaps in the future, some large machine runs could be printed on the new IBM "compact printing device" described in the December 1970 Keyword article "Train's In!" This could vastly reduce the storage space required for runs which should be retained for a long time.

5. What is the possibility of microfilming records which should be kept indefinitely for historical reasons but which are not used frequently?

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

6. How about converting that relatively static information now on cards in a bulky file box into a 2- or 3-page printed working aid?

7. I propose the consideration of creating a central crypt and T/A repository something like our G54 C/L library. Since NSA is so prone to organize and reorganize frequently and since personnel changes at all levels almost if not completely eliminate continuity, a repository for useful references, documentation, records, etc., would eliminate the necessity for duplicate copies in several organizational segments. This plan might overcome confusion and losses of background information caused by realigning entities like ZED, ZEA, ZEN, etc., which at one time were all in the same organization but later were separated: ZED in one division, the other ZE systems in another division. (Probably they will all be reunited in some future reorganization.)

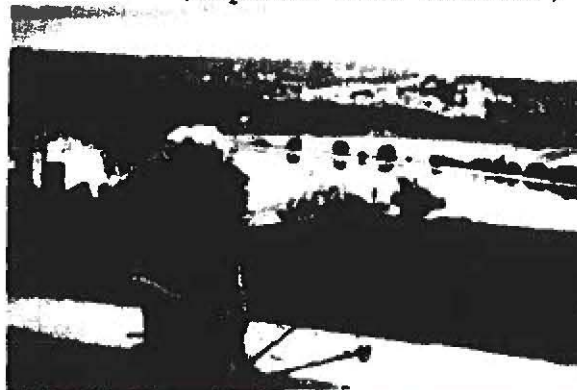
8. Everybody will hate me for this final suggestion because it involves just another tedious chore to do. However, since I'm about to leave the Agency, maybe I can get away before the Furies catch me.

When I was preparing some records as a legacy for any successor working on a particular system, I decided it would help to list the records vital to the system and the records or materials which are useful but of secondary importance. Such lists on all systems would help those who must decide what goes OUT in a pinch for space, and what must be kept or cogitated over before keeping or destroying.

In that repository, which I proposed, a single retention copy of Vital Records on non-current systems could be kept available for reference by everybody interested -- irrespective of current, past, or future organizational designations.

And now please excuse me. I really must slip out quickly . . .

(Reprint from *KEYWORD*, February 1971)



~~TOP SECRET UMBRA~~

B SIGNALS LAB CAPABILITIES AND MISSION
by Robert Earles, B43

Up until November 1973 the B4 signals lab was referred to as the "CYANIDE" lab. This label was certainly warranted because 80-90 percent of the work being done at that time was associated with the processing and analysis of CYANIDE material. However, since November we have greatly expanded our lab capabilities and our workload has grown commensurately. In fact, CYANIDE now comprises less than 5% of the analysis done in the lab.

With the equipment added to the lab during the past few months, we analyze, identify, and provide limited processing for signals which fall into any of the following categories: frequency division multiplex (FDM), pulse position modulation (PPM), phase shift keying (PSK), frequency shift keying (FSK), double frequency shift (DFS), and on-off keying (OOK). In addition, we can handle single channel, multichannel and multitone transmissions and process wideband tapes (7 or 14 track) with servo function.

The signals lab is here to provide a service to B, but we can provide that service only if each element is aware of why we are here and what we can do. If you now have, or expect to have in the future, any material which requires signals analysis and/or processing, let us know and we will provide you with meaningful results as fast as possible.

For further information concerning the capabilities of the B4 signals lab and its equipment, please call Mr. Robert Earles, B43, extension 5751, Room 7A197.

* * * *
**China Buying
Heavily in U.S.**

MEMPHIS (AP) — China will buy about \$1 billion worth of feed grains, soybeans and cotton in the United States this year, according to Dr. Willard Sparks, executive vice president of Cook Industries, Inc

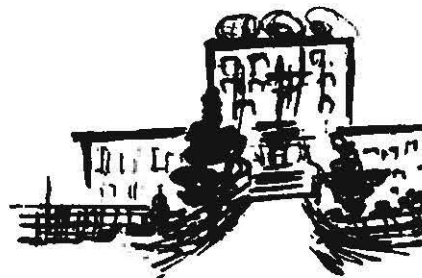
He said China would buy about 140 million bushels each of wheat and corn, about 900,000 tons of soybeans and about 830,000 bales of cotton.

Washington STAR-NEWS,
February 1974

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

RETURN OF.....

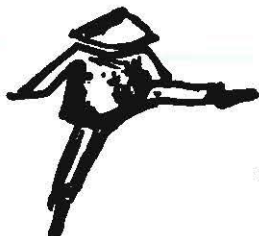


Practically every spare moment during the last week of January was spent preparing for our move from Friendship to Fort Meade. We managed to keep the product flowing despite severe disruptions such as the timely cessation of DDP and ADP support at Friendship which occurred three days prior to our move, concurrent with the B11 move of 25 January. Our gear was moved from Friendship on the evening of 28 January and expertly installed by the movers. We spent the next two days putting things where they belonged, when we were lucky enough to find them.

During the week, we used one million yards of masking and other types of tape, seventeen thousand boxes of all sizes, and one marking pencil. In addition, modest estimates for the division are that we consumed over nine hundred martinis. We entertained at least twenty logistics and security staff officers from every organizational level, and we were gracious even though they only talked among themselves. We sympathized with them in their inability to assist us with the actual manual labor since (1) they wore their good clothes; (2) most had never been SIGINT analysts, hence their time was more valuable than ours; and (3) they were enroute to a B4TDLA lecture entitled "How Chinese Children Learn to Eat with Forks."

Our office is located on the fifth floor of Operations Building #1, about 50 paces from where we were located in May 1972 prior to our exodus to Friendship. We have gained much in this latest move, but we lost the blonde in E02/FANX II and the thousands of female A Group workers who wear brow shades and who, as young ladies, danced in the courts of the Ottoman Empire until their ankles swelled. We're glad to be back and invite you to visit us, but please be careful of dangling phone plugs and electrical outlets.

....THE EXILES



LICAMELI
25



~~TOP SECRET UMBRA~~



---SD 4060 COM UPGRADE

The SD4060 COM system is scheduled for an upgrade to a SD4060 system in FY 1974. The present SD4060 system has been in use at the Agency since the late 1960's, when it replaced the original SC4020 COM system. The 4060 has proved to be a dependable means of producing textual data from magnetic tape at a high rate of speed, and of reducing large volumes of intelligence to a usable form in a fraction of the amount of space required for paper output. Through its graphic capabilities the 4060 has also enabled its users to create numerous charts and graphs as another form of computer output. The system has also supported applications in the printing of various foreign languages and in scientific studies, such as random number generators.

Output from all of these applications is now recorded on 16mm roll film only. This is one of the faults of the system, for the familiar roll of microfilm can be cumbersome in many applications, and none of the data can be printed on paper with any reasonable degree of quality. With the upgrade of the SD4060, all of the systems present capabilities are retained and the output capabilities are

increased. There will be a choice of producing an image on 16mm roll film in either a 24x or 48x reduction ratio, on 35mm roll film at a 13x reduction, or on 105mm microfiche at either 24x or 48x reduction. The 35mm roll film can be used to produce aperture card inserts, projection slides, or offset plates for printing.

The microfiche capability on the COM unit provides the necessary link between the computer and the reproduction facilities and makes it possible to automatically create and update microfiche documents for mass distribution. The new and more flexible COM system will provide microforms suitable for almost any application. Acceptance of information in a "not no new" physical form will be the key to effective use of the SD4460 as it was with its predecessors.

For additional information about this forthcoming system, contact Albert J. Herb, C741,

---CA WRITTEN EXAMINATION

The fifteenth professional qualification examination in cryptanalysis will be given on Monday and Tuesday, 13 and 14 May 1974.

All persons who took prior examinations are eligible to

take the May examination. To determine the eligibility of other candidates it is necessary that a copy of their Professional Qualification Record (PQR) be available to the CACP office by 19 April 1974. Although a PQR may have been submitted to M331, each aspirant should check with the CACP office to make sure that a copy of his PQR has been received by that office.

All persons who wish to take any or all of the three parts of the Examination (CA Objective, Related Fields, Essay) should notify the CACP office, Room 3C051-6, 3868sm by 26 April 1974. Each person will be notified by the CACP office of the time and place of the examination.

---TWO ADDITIONAL SESSIONS OF:
THE WORKSHOP IN THEORY AND
PRACTICE OF TRANSLATION (LG-230)

This workshop is designed to provide: a) intermediate translation training, comparable to the 200-level courses in Russian, Spanish, etc., in "low-density" languages where such courses cannot be offered presently; and/or: b) additional training for persons who have taken a 200-level course and desire to further refine their translation skills or for persons in a supervisory capacity desiring to become

conversant with emerging concepts in the area of translation and evaluating translations.

INSTRUCTOR: Cpt. James J. Hessinger

DATES: LG-230/2/74 - 22 April-
3 July; Monday and
Wednesday, 8:15-
10:15

LG-230/3/74 - 14 June-
15 August; Tuesday
and Thursday, 8:15-
10:15

LOCATION: To be announced

Enrollment in each session will be limited to between six and eight students. Preference will be given to nominees who desire training in the "low-density" languages mentioned above, and who are currently assigned to duties requiring end-product translation, preliminary translation, reporting or analysis based on foreign-language source material. Nominees who do not meet both of these criteria will be considered as space permits.

Prospective students should submit NSA form 7687b, NCSch Course Application, to the element training coordinator. Nominations must be submitted on NSA form 7687 to the Language Department

~~TOP SECRET UMBRA~~

(E11), Rm A2a26, FANX II, no later than 4 April 1974 (for LG-230/a) or 3 June 1974 (for LG-230/3).

Any prospective student should contact Cpt. Hessinger (796-6392/8027s) at the same time as he/she submits the Course Application, in order to notify him of the language in which training is desired and to permit the gathering of materials to be used in the course. A detailed description of the background, purposes and form of this workshop is available on request from the Language Department or from Cpt. Hessinger.

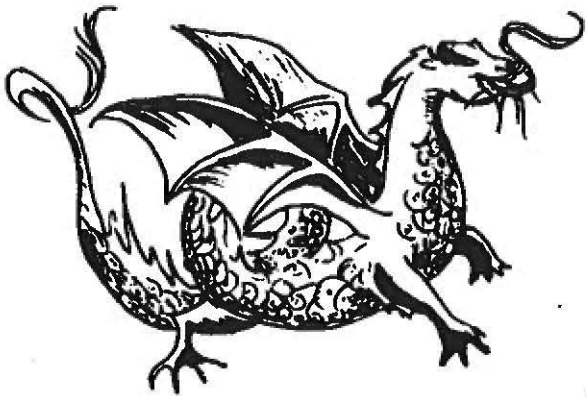
ANSWER TO "TRANSLATION, PLEASE?"

SAY WILLY! THERE THEY GO.
THOUSAND BUSES IN A ROW.
NO JOE. THEM IS TRUCKS.
SOME WITH COWS 'N
SOME WITH DUCKS.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)
PL 86-36/50 USC 3605



ASK
THE
DRAGON
LADY

Dear Dragon Lady,

I read Russ Myers' article, [redacted] in the last issue of DRAGON SEEDS. I found it interesting and am glad to see that B is beginning to be aware of the Bookbreaker's Package, thanks to you and Russ.

I found one small problem involving the terms "Decoded Index" and "Bookbreaker's Index." I'd like to suggest:

1. For "standard bookbreaker's index", substitute "standard code index (or, if there are any recoveries, a decoded index - showing the meaning on the information line for each recovered code group on major control)".

2. For "a Decoded Bookbreaker's Index", simply omit the word "Decoded", which is redundant.

Apropos - end of paragraph 2 - after messages are in case/date order do you assign a worksheet # to keep each message unique? If not, how do you solve that problem?

Keep writing; I wish others would do the same.

Kay Swift, G54, Ret.

* * * *

*May my eyes look always inward to
the source of all my faults!*

*And, to resolve any confusion
witnessed upon the unenlightened,
copies of "Definitions of Bookbreaking
Terms" are available from the Technical
Directorates of Language and Cryptanalysis.*

---Dragon Lady

~~TOP SECRET UMBRA~~

CONTRIBUTORS

BOB EARLES, B43, came to NSA as an Engineering Technician in 1960 after a three-year tour in the Army Security Agency where he served as a Cryptanalyst. He has been involved in Signals Analysis most of his Agency career and has worked in both B and G Groups. [REDACTED] Mr. Earles served as an Engineering Specialist [REDACTED]. He holds professional certification in Signal Collection and Signal Conversion and has completed 24 Agency-sponsored courses in signal analysis, engineering, and management. He presently has the responsibility of supervising the personnel and job functions within the B Group Signals Analysis Lab, located in B43.

VIRGINIA JENKINS, E13, who holds an MA in Romance Languages from Duke University, has worked at NSA as a Linguist, Cryptanalyst, and Data Systems Analyst. Most recently she has been instructing and developing cryptanalysis courses in the National Cryptologic School where she is currently Head of the Cryptanalysis Department, E13. She is a member of the Cryptanalysis Career Panel, an officer in CMI, and a recipient of the Meritorious Civilian Service Award.

SALLY PEEBLES, G Group Linguist and Cryptanalyst, retired in 1971 after a long NSA career involving in turn the Middle East, the Far East, and South America. Sally was born and reared in Boulder, Colorado. At the University of Colorado, she studied English Literature, French, and Spanish and received the BA and MA as well as a fellowship to teach conversational English at the girls' normal school at Le Puy, France. She spent one summer at the University of Mexico. Since her retirement, Sally has traveled a bit and has actively supported the work and goals of the Volunteers for the Visually Handicapped of Chevy Chase, an organization which helps the blind and visually impaired to cope with their problems. She is pursuing her own goal: to live as independently and as actively as possible.

~~TOP SECRET UMBRA~~

INDEX OF PREVIOUS DRAGON SEEDS ARTICLES

(BY AUTHOR)

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
ABBOTT, Walter D.	CINCPAC Intelligence Coordination Group	Vol 1, Nr 5 (Dec 72)	16
ABBOTT, Walter D.	Marketing Our Product	Vol 2, Nr 2 (Jun 73)	18
ATKINSON, Rich	Teacher Very Funny	Vol 2, Nr 3 (Sep 73)	19
BARNHILL, Peggy	AG-22 and You	Vol 1, Nr 1 (Dec 71)	9
BRANSTAD, Marti	Probing a New Technique	Vol 2, Nr 2 (Jun 73)	45
BUCK, Stuart H.	Computer-aided Bookbreaking (Not "Bookbreaking by Computer")	Vol 2, Nr 3 (Sep 73)	1
BUCKLEY, Dan	Ground Zero Approach to Language Analysis	Vol 2, Nr 1 (Mar 73)	12
CHUN, Richard S.	Need for a Centralized Transcription Operation	Vol 1, Nr 3 (Jun 72)	17
CHUN, Richard S.	Gist of the Korean SIGINT Problem	Vol 2, Nr 1 (Mar 73)	12
COURY, Sam	Surveying [redacted] Cryptosystems	Vol 2, Nr 3 (Sep 73)	24
CURTIN, Dick	Analyzation of Data	Vol 1, Nr 1 (Dec 71)	19
DELONG, Don	History of a Dragon	Vol 2, Nr 3 (Sep 73)	29
D'IMPERIO, Mary	CAMINO	Vol 1, Nr 2 (Mar 72)	15

EO 3.3b(3)
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
DUNN, Jane E.	Once More the TSR	Vol 2,Nr 1 (Mar 73)	29
DUNN, Jane E.	SAWTOOTH Answers the Q Question	Vol 2,Nr 3 (Sep 73)	8
FERGUSON, Morris L.	Christmas at the School	Vol 2,Nr 4 (Dec 73)	17
FLYNN, William G.	The Jack Butcher Case	Vol 2,Nr 1 (Mar 73)	1
FORBES, Rodney	Reflections on a Non-Random Bane	Vol 2,Nr 2 (Jun 73)	33
GEGAN, Jeryl O.	What Have They Done To Our Linguists?	Vol 2, Nr 3 (Sep 73)	14
GERHARD, William	One Chance in Three	Vol 2,Nr 2 (Jun 73)	10
GILBERT, Allen	Impact of ARDF on Traffic Analysis	Vol 1,Nr 1 (Dec 71)	7
GILBERT, Allen	Importance of Being Honest	Vol 1,Nr 2 (Mar 72)	20
GILBERT, Allen	SEADEV--Mechanization for T/A	Vol 1,Nr 4 (Sep 72)	14
GLENN, Tom	Creative Translator	Vol 1,Nr 1 (Dec 71)	16
GLENN, Tom	Uncertain Origins	Vol 1,Nr 5 (Dec 72)	5
GLENN, Tom	Time to Look at People	Vol 2,Nr 4 (Dec 73)	19
GRANT, Louis C.	Don't Say MUSSO -- Say USSID	Vol 1,Nr 5 (Dec 72)	28
GUY, Herb	Maybe It's Related to the Phase of the Moon	Vol 1,Nr 3 (Jun 72)	5

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
HRICIK, Mike	Things That Go Clank in the Night	Vol 1, Nr 4 (Sep 72)	7
HUNT, William	SIGINT Support on the Economic Front	Vol 2, Nr 1 (Mar 73)	18
JACOBS, Walter, Dr.	Are You Using Computers?	Vol 2, Nr 4 (Dec 73)	21
JOLLENSTEN, Ralph W., Dr.	Role of Mathematics in C/A	Vol 1, Nr 3 (Jun 72)	19
KENNARD, Bee	C Parallelogram or Vietnam Cover Story	Vol 2, Nr 2 (Jun 73)	22
KREINHEDER, Robert	Software Approach to Script Processing - The Why	Vol 1, Nr 4 (Sep 72)	19
LASLO, Mary Ann	<input type="checkbox"/> A Hitch-Hiking Cipher	Vol 2, Nr 2 (Jun 73)	38
LENAHAN, Donald	Cryptanalysis through Functional Linguistics	Vol 1, Nr 1 (Dec 71)	3
MILLER, Kenneth	Study of ZFK Message Activity	Vol 1, Nr 3 (Jun 72)	27
MILLER, Kenneth	Exploiting the Bust	Vol 2, Nr 1 (Mar 73)	25
MOLLICK, John	How Great COMINT Facts from Little Slivers Grow, or Making Russian Molehills Out of Chinese Mountains	Vol 1, Nr 2 (Mar 72)	26
MURPHY, Tim	Vietnamese Communist Tactical COMINT Operations	Vol 1, Nr 3 (Jun 72)	32
MYERS, L. St. Clair	Chinese Voice: Solu- tion to a Dilemma	Vol 1, Nr 4 (Sep 72)	17



<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
MYERS, Russ	Standardization????	Vol 2, Nr 1 (Mar 73)	33
MYERS, Russ	[REDACTED]	Vol 2, Nr 4 (Dec 73)	31
NUGENT, Michael	MFMUFS and Catnip	Vol 1, Nr 2 (Mar 72)	12
O'CONNOR, Ed	Viet Nam Odyssey, 1972-1973	Vol 2, Nr 4 (Dec 73)	8
ORR, E. E.	The Reality of Communications Changes	Vol 1, Nr 3 (Jun 72)	13
PALMER, Carolyn	RYE, an Extended Capacity Remote Access System	Vol 2, Nr 2 (Jun 73)	1
PATTERSON, George	Reflections on Crypt- analytic Accountability	Vol 1, Nr 2 (Mar 72)	2
PETERS, Bernie	RYE, an Extended Capacity Remote Access System	Vol 2, Nr 2 (Jun 73)	1
REINKE, F. John	Software Approach to Script Processing - The How	Vol 1, Nr 4 (Sep 72)	21
REMSBERG, Philip	CHICOM Development [REDACTED] and the AG-22	Vol 1, Nr 2 (Mar 72)	7
REMSBERG, Philip	AG-22: Where Do We Go Now?	Vol 1, Nr 5 (Dec 72)	22
SAWYER, E. Leigh	WADE-GILES System	Vol 1, Nr 5 (Dec 72)	35
SHARRETT, Jack	Development of COMINT Translation Course for Vietnamese Linguists	Vol 1, Nr 5 (Dec 72)	24
SMITH, Claire	Strategic Importance of Shenyang Military Region	Vol 1, Nr 2 (Mar 72)	23

~~TOP SECRET UMBRA~~

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
Staff Writers	SIGINT and Automatic Data Processing	Vol 1, Nr 4 (Sep 72)	12
STEPP, Leo	Viet Nam Odyssey, 1972-1973	Vol 2, Nr 4 (Dec 73)	8
STIVERS, Bill	B Needs Its Own Computer	Vol 2, Nr 4 (Dec 73)	24
STOFFEL, Wayne	Recovery of a Viet Communist Callsign System	Vol 1, Nr 1 (Dec 71)	5
SWANSON, Louise	Project KAY -- Or Another Kind of RYE	Vol 1, Nr 4 (Sep 72)	17
SWIFT, Charles	DDP--Dedupe, Delete and Progress	Vol 1, Nr 1 (Dec 71)	12
THOMAS, Jack L.	Chinese Communications Developments	Vol 2, Nr 4 (Dec 73)	2
TIREN, David J.	T/A -- Math Symposium Reviewed	Vol 1, Nr 5 (Dec 72)	36
WADDELL, Stanley	China-Wide Technical Specialists: A Way to Save Overseas	Vol 1, Nr 2 (Mar 72)	21
WILD, Norman	Machine Aided Translation, Part 1	Vol 1, Nr 3 (Jun 72)	23
	Part 2	Vol 1, Nr 4 (Sep 72)	24
	Part 3	Vol 1, Nr 5 (Dec 72)	31
WOOD, Geoffrey	Rebels in Thailand	Vol 2, Nr 1 (Mar 73)	6
WOOD, Thomas	How about the Olds-mobile M?	Vol 2, Nr 1 (Mar 73)	32

INDEX OF PREVIOUS DRAGON SEEDS ARTICLES

(BY TITLE)

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
<u>A</u>			
AG-22 and You, The	Peggy Barnhill	Vol 1, Nr 1 (Dec 71)	9
AG-22: Where Do We Go Now?	Philip Remsberg	Vol 1, Nr 5 (Dec 72)	22
Analyzation of Data	Dick Curtin.	Vol 1, Nr 1 (Dec 71)	19
Are You Using Computers?	Dr. Walter Jacobs	Vol 2, Nr 4 (Dec 73)	21
<u>B</u>			
B Needs Its Own Computer	William H. Stivers	Vol 2, Nr 4 (Dec 73)	24
	Russ Myers	Vol 2, Nr 4 (Dec 73)	31
<u>C</u>			
CAMINO	Mary D'Imperio	Vol 1, Nr 2 (Mar 72)	15
CHICOM Development  and the AG-22	Philip Remsberg	Vol 1, Nr 2 (Mar 72)	7
China-Wide Technical Specialists: A Way To Save Overseas	Stanley Waddell	Vol 1, Nr 2 (Mar 72)	21
Chinese Communications Developments	Jack L. Thomas	Vol 2, Nr 4 (Dec 73)	2

~~TOP SECRET UMBRA~~

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
Chinese Voice: Solution to a Dilemma	L. St. Clair Myers	Vol 1, Nr 1 (Dec 71)	14
Christmas at the School	Morris L. Ferguson	Vol 2, Nr 4 (Dec 73)	17
CINCPAC Intelligence Coordination Group	Walter D. Abbott	Vol 1, Nr 5 (Dec 72)	16
Computer-Aided Book-keeping (Not "Book-keeping by Computer")	Stuart H. Buck	Vol 2, Nr 3 (Sep 73)	1
C Parallelogram or Vietnam Cover Story, The	Bee Kennard	Vol 2, Nr 2 (Jun 72)	22
Creative Translator, The	Tom Glenn	Vol 1, Nr 1	16
Cryptanalysis through Functional Linguistics	Donald Lenahan	Vol 1, Nr 1 (Dec 71)	3
<u>D</u>			
DDP - Dedupe, Delete & Progress	Charles Swift	Vol 1, Nr 1 (Dec 71)	12
Development of COMINT Translation Course for Vietnamese Linguists	Jack Sharretts	Vol 1, Nr 5 (Dec 72)	24
Don't Say MUSSO--Say USSID	Louis C. Grant	Vol 1, Nr 5 (Dec 72)	28
<u>EF</u>			
 A Hitch-Hiking Cipher	Mary Ann Laslo	Vol 2, Nr 2 (Jun 73)	38
Exploiting the Bust	Kenneth Miller	Vol 2, Nr 1 (Mar 73)	25

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

G

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
Gist of the Korean SIGINT Problem	Richard S. Chun	Vol 2,Nr 1 (Mar 73)	12
Ground Zero Approach to Language Analysis	Dan Buckley	Vol 2,Nr 1 (Mar 73)	22

H

History of a Dragon	Don DeLong	Vol 2,Nr 3 (Sep 73)	29
How about the Oldsmobile M?	Thomas Wood	Vol 2,Nr 1 (Mar 73)	32
How Great COMINT Facts from Little Slivers Grow, or Making Russian Molehills Out of Chinese Mountains	John Mollick	Vol 1,Nr 2 (Mar 72)	26

I

Impact of ARDF on Traffic Analysis	Al Gilbert	Vol 1,Nr 1 (Dec 71)	7
Importance of Being Honest, The	Al Gilbert	Vol 1,Nr 2 (Mar 72)	20

JKL

Jack Butcher Case, The	William G. Flynn	Vol 2,Nr 1 (Mar 73)	1
------------------------	------------------	------------------------	---

M

Machine Aided Translation, Part 1	Norman Wild	Vol 1,Nr 3 (Jun 72)	23
Part 2		Vol 1,Nr 4 (Sep 72)	24
Part 3		Vol 1,Nr 5 (Dec 72)	31
Marketing Our Product	Walter D. Abbott	Vol 2,Nr 2 (Jun 73)	18
Maybe It's Related to the Phase of the Moon	Herbert S. Guy	Vol 1,Nr 3 (Jun 72)	5

~~TOP SECRET UMBRA~~

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
	<u>N</u>		
Need for a Centralized Transcription Operation	Richard S. Chun	Vol 1, Nr 3 (Jun 72)	17
	<u>OPQ</u>		
Once More the TSR	Jane E. Dunn	Vol 2, Nr 1 (Mar 73)	29
One Chance in Three	William Gerhard	Vol 2, Nr 2 (Jun 73)	10
Probing a New Technique	Dr. Marti Branstad	Vol 2, Nr 2 (Jun 73)	45
Project KAY -- Or Another Kind of RYE	Louise Swanson	Vol 1, Nr 4 (Sep 72)	17
	<u>R</u>		
Reality of Communica- tions Changes	E. E. Orr	Vol 1, Nr 3 (Jun 72)	13
Rebels in Thailand	Geoffrey Wood	Vol 2, Nr 1 (Mar 73)	6
Recovery of a Viet Communist Callsign System	Wayne Stoffel	Vol 1, Nr 1 (Dec 71)	5
Reflections on a Non-Random Bane	Rodney Forbes	Vol 2, Nr 2 (Jun 73)	33
Reflections on Crypt- analytic Accountability	George Patterson	Vol 1, Nr 2 (Mar 72)	2
Role of Mathematics in C/A	Dr. Ralph W. Jollensten	Vol 1, Nr 3 (Jun 72)	19
RYE, an Extended Capacity Remote Access System	Bernie Peters/ Carolyn Palmer	Vol 2, Nr 2 (Jun 73)	1

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
SAWTOOTH Answers the Q Question	Jane E. ^S Dunn	Vol 2, Nr 3 (Sep 73)	8
SEADEV--Mechanization for T/A Development	Al Gilbert	Vol 1, Nr 4 (Sep 72)	14
SIGINT and Automatic Data Processing	Staff Writers	Vol 1, Nr 4 (Sep 72)	12
SIGINT Support on the Economic Front	William Hunt	Vol 2, Nr 1 (Mar 73)	18
Software Approach to Script Processing - The How	F. John Reinke	Vol 1, Nr 4 (Sep 72)	21
Software Approach to Script Processing - The Why	Robert Kreinheder	Vol 1, Nr 4 (Sep 72)	19
Standardization????	Russ Myers	Vol 2, Nr 1 (Mar 73)	33
Strategic Importance of Shenyang Military Region, The	Claire Smith	Vol 1, Nr 2 (Mar 72)	23
Study of ZFK Message Activity	Kenneth Miller	Vol 1, Nr 3 (Jun 72)	27
Surveying Cryptosystems	Sam Coury	Vol 2, Nr 3 (Sep 73)	24
<u>T</u>			
T/A--Math Symposium Reviewed	David J. Tiren	Vol 1, Nr 5 (Dec 72)	36
Teacher Very Funny	Rich Atkinson	Vol 2, Nr 3 (Sep 73)	19
Things That Go Clank In the Night	Mike Hricik	Vol 1, Nr 4 (Sep 72)	7
Time to Look at People	Tom Glenn	Vol 2, Nr 4 (Dec 73)	19

~~TOP SECRET UMBRA~~

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
	<u>U</u>		
Uncertain Origins	Tom Glenn	Vol 1, Nr 5 (Dec 72)	5
	<u>V</u>		
Vietnamese Communist Tactical COMINT Operations	Tim Murphy	Vol 1, Nr 3 (Jun 72)	32
Viet Nam Odyssey, 1972-1973	Leo Stepp/ Ed O'Connor	Vol 2, Nr 4 (Dec 73)	8
	<u>W</u>		
WADE-GILES System	E. Leigh Sawyer	Vol 1, Nr 5 (Dec 72)	35
What Have They Done to our Linguists?	Jeryl O. Gegan	Vol 2, Nr 3 (Sep 73)	14

* * * *

**Chinese Made
Official Language**

Agence France-Press

HONG KONG, Feb. 13 —
The government was urged today to draw up a program to improve the standard of the Chinese spoken by residents and to use simple Chinese in its communications with the public.

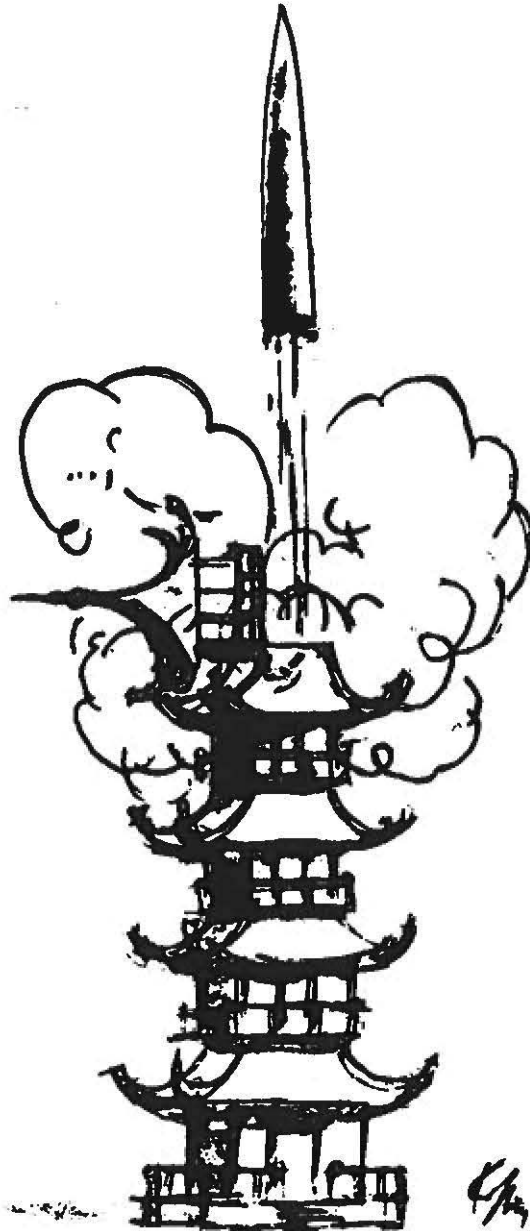
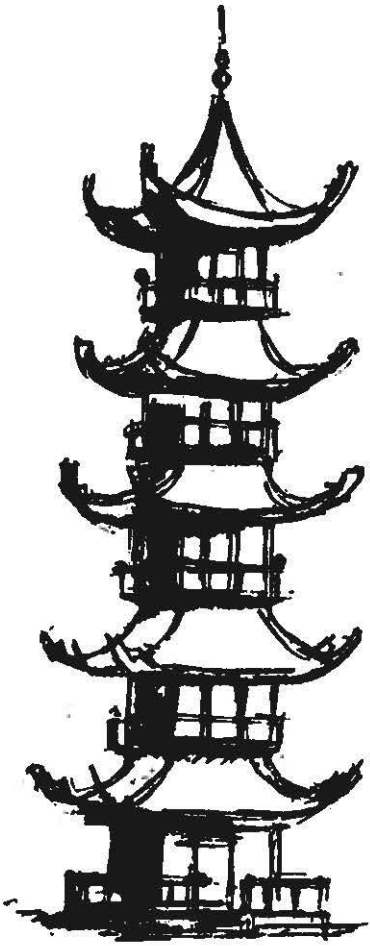
Hilton Cheong-Leen spoke in support of the official languages bill, which passed. It makes Chinese an official language alongside English.

Steps should be taken, Cheong-Leen said, to avoid use of esoteric and outmoded terms or too literal a Chinese translation of an English original. He also suggested making Mandarin equal in status with Cantonese.

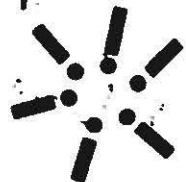
The Washington POST
February 1974

~~TOP SECRET UMBRA~~

A
CHINESE
MISSILE



5...
4...
3...
2...



~~TOP SECRET UMBRA~~