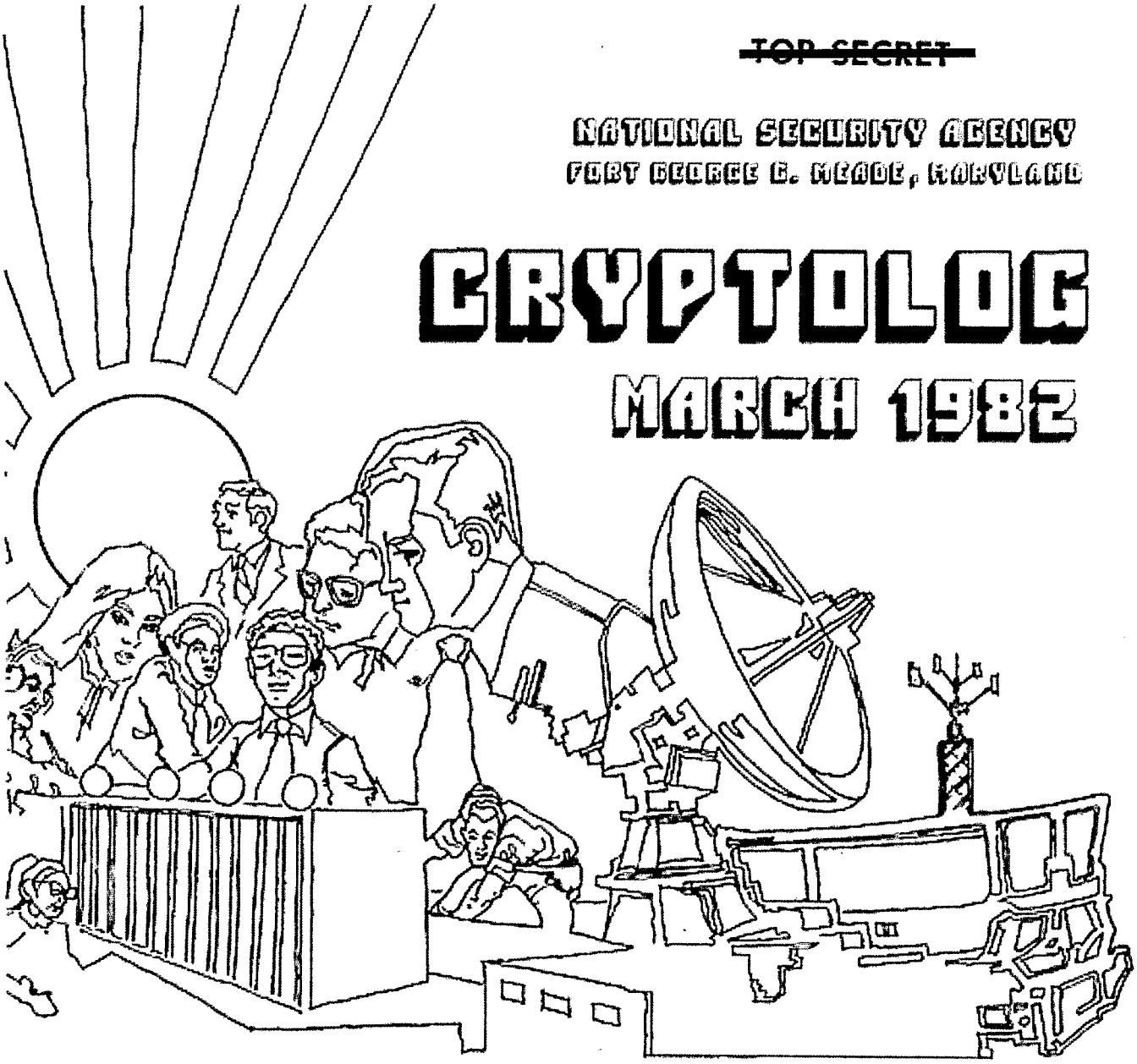
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1982



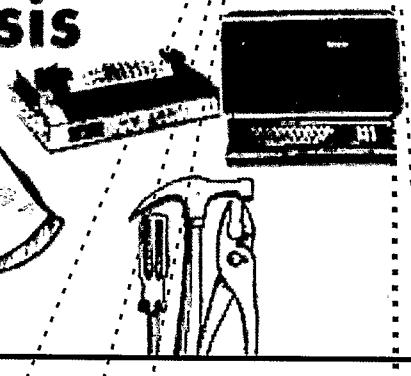
PL 86-36/50 USC 3605

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Mar 2012~~

The PERSONAL Computer: A *Current* Cryptanalysis Support Tool (U)



by [redacted] B53

Mrs. [redacted] article, "Desk Top Microcomputers: A Growing Part of NSA's Future," which appeared in the September 1980 issue of the Field Information Letter (FIL) was nowhere better received than in the Cryptanalytic Support Branch of the Office of Southeast Asia. Since April 1980, this element has used the TRS-80 personal computer as an integral part of our cryptanalytic effort against specific SEA Targets. I would like to share with you how the TRS-80 is being successfully used in our daily operations. Although reference is made to the TRS-80 throughout this article, many other personal computers would serve as well.

[redacted]

~~(SC)~~ Our most extensive and successful TRS-80 application to date has been against the [redacted] target.

[redacted]

~~(SC)~~ To handle both of these cryptographic features, two programs which were adapted for us by P13 for use on this personal computer: a [redacted]

[redacted]

~~(SC)~~

[redacted]

~~(SC)~~ In January 1980, the complexity and volume of [redacted] enciphered communications began to change rapidly.

[redacted]

programs were available in many areas of the Agency but what was really needed was computer support of a local, personal nature, the kind of computer with which the

~~SECRET STONE~~

analyst could work at his/her own speed and not tie up valuable machine processing time.

[redacted]

What's more, we needed an interactive capability not only to reproduce but also to replace our manual methods.

(S-CCO) Upon investigation, we learned of P13 and its work with the TRS-80, particularly in the area of [redacted]. By April 1980, P13 had adopted its already existing [redacted] program for use against the [redacted] target. With our basic TRS-80 we set to work. We obtained immediate positive results through use of the TRS-80 but also recognized a need for peripheral equipment such as mini disk drives and a printer. This equipment was subsequently purchased and the entire process was greatly speeded up. Then in the fall of 1981, our computer was upgraded to a TRS-80 MODEL III, which had built-in disks drives and interface, making it one complete package. A new printer was also acquired.

(S-CCO) Currently, our cryptanalytic approach to [redacted] with the aid of the TRS-80 involves several steps. The software is loaded on its own single floppy disk. The [redacted] were, in the past, manually loaded on another disk called CIPHER. But, in April 1981, the B33 TRS-80 was successfully interfaced with the CARONA Terminal Sub-system, (PDP 1170); thus, making the TRS-80 a "smart" terminal. Now, we can go across PLATFORM and process or retrieve our data from other systems such as BARDOLPH or CARILLON (IBM-370) or any other system connected to PLATFORM, and directly enter it onto the cipher disk.

[redacted]

(S-CCO) [redacted] It is interesting to note that this peculiarity of [redacted] was first discovered while routinely [redacted] on the TRS-80 microcomputer [1].

(S-CCO) Our [redacted] capability has been greatly enhanced by use of the TRS-80.

[redacted] The TRS-80 is a dedicated computer, accomplishing the entire [redacted] process locally, without having to "wait in line" on a major computer for execution at any stage of development. It is highly "personal in nature," allowing the analyst to work at his/her own pace. The TRS-80 can be tailored easily and quickly to individual analyst/target needs -- its most distinctive feature. It is also a very economic analytic tool -- giving optimum results for a minimal amount of money.

(S-CCO) The TRS-80 success rate [redacted] with very little hardship.

[redacted] That kind of volume alone could involve many manhours as well as much computer processing time if batch processing were used.

[redacted] With the interactive analytic application on the TRS-80, valuable time is indeed saved and analytic success achieved.

(S-CCO) The second program for use in the [redacted] was orginally designed for [redacted] but, in the fall of 1981, it was expanded to

~~SECRET STONE~~

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

[redacted] the Vietnamese target. Additional modifications to the existing program currently being considered are for the [redacted]

(S) [redacted]

(S) [redacted]

(S) Success with the "personal computer" on the [redacted] target has led to its usage by other Southeast Asian (SEA) analysts whose targets [redacted] Only a slight modification to the existing TRS-80 [redacted] was needed to accommodate [redacted] is now being done mechanically instead of by hand. An updated version of the program, provided by P13, includes the capability of minor differencing which will also greatly aid in the [redacted]

(S) In addition, [redacted] was initially tested [redacted] on the TRS-80 with negative results. Thus, the analyst was able to eliminate promptly his/her initial hypothesis and concentrate efforts in another direction.

(S) All of the TRS-80 applications in the Office of SEA have not been of a cryptanalytic nature. [redacted] traffic analysts with P13 assistance have established a PERSONALITY file. [redacted] This Personality File program has been upgraded to allow for greater manipulation of stored data. Thus, the analyst can keep the file current by making entries, changes or deletions. In addition to all of these applications on the TRS-80 microcomputer/printer, B53 can access BARDOLPH through TELNET; thus, giving us a fourth BARDOLPH terminal with limited applications. We are able to process daily traffic in the non-scan mode through the TRS-80 and print any BARDOLPH files locally. Also, as previously discussed, we can transfer BARDOLPH files onto TRS-80 disks for use with any of the existing off-line applications.

(S CCO) The analytic applications detailed above demonstrate the fact that the TRS-80 personal computer has proven to be a valuable asset to the Southeast Asian analytic effort. The TRS-80 has served us well in a short period of time and we have every expectation that it will continue to be used as a flexible, "personal" tool of the SEA analyst for a long time to come.

1. (S) For further detailed information concerning the actual software specifics of the [redacted] please consult P1 Informal No.5 (June 1981): "Automatic Input To [redacted] by [redacted]

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

PL 86-36/50 USC 3605

Request ID: 0001014786

UNCLASSIFIED

TRANSMITTAL OF MATERIAL

Type: OMAL

Submitted: 20200117

TO	FROM (RETURN ADDRESS)	
MR. MICHAEL MARTELLE THE NATIONAL SECURITY ARCHIVE THE GEORGE WASHINGTON UNIVERSITY GELMAN LIBRARY, SUITE 701 2130 H STREET, N.W. WASHINGTON, DC 20037 PHN#: (202)994-7000	DEPARTMENT OF DEFENSE NATIONAL SECURITY AGENCY 9800 SAVAGE ROAD FORT MEADE MARYLAND 20755-6000 ATTN: RAMSEY,VICKI LYNN SUITE: 6881	This transmittal may NOT be downgraded upon removal of the enclosure(s). This transmittal may NOT be declassified upon removal of the enclosure(s).

WRAPPED	COMSEC	SUBMITTED
☒ U ☐ S ☐ D	☐ YES ☒ NO	20200117

SHIPPING MODE	PACKAGE CT
USPS - First Class	1 of 1

LN#	UNCLASSIFIED TITLE/DESCRIPTION OF ITEM	QTY	TOT COST	MFG SERIAL#	BARCODE	CLASS. OF ITEM
1	SERIAL: MDR-107697, DATED 17 JANUARY 2020 SERIAL: MDR-107698, DATED 17 JANUARY 2020	1	0			UNCLASSIFIED

DESIG	ACCT	TYPE	PAS STATEMENT	APPROVAL
CPODIR	NO	NA	Not Applicable	

SPECIAL HANDLING INSTRUCTIONS (UNCLASSIFIED)

REQUESTED BY	SIGNATURE	ORG	PHONE
RAMSEY,VICKI LYNN (VLRAMSE)	Vicki Ramsey	P133	(301)688-7785

UNCLASSIFIED

DO NOT STAMP RECEIPT PORTION WITH CLASSIFICATION

Request ID: 0001014786

RECEIPT

(Please sign and return immediately. Avoid tracer action)

Type: OMAL

RETURN TO	FROM	
DEPARTMENT OF DEFENSE NATIONAL SECURITY AGENCY 9800 SAVAGE ROAD FORT MEADE MARYLAND 20755-6000 ATTN: RAMSEY,VICKI LYNN SUITE: 6881	MR. MICHAEL MARTELLE THE NATIONAL SECURITY ARCHIVE THE GEORGE WASHINGTON UNIVERSITY GELMAN LIBRARY, SUITE 701 2130 H STREET, N.W. WASHINGTON, DC 20037 PHN#: (202)994-7000	Receipt is hereby acknowledged for the material or documents listed under this Request ID SID (Typed or Printed) | DATE RECEIVED NAME (Typed or Printed) SIGNATURES