NOTE
This is final of folio 20 - not draft. BPL as I originally took it to be! 8/8

UPGRADE OF CRYPT PROCESSING FACILITIES AT DSD - ANALYSIS OF COMPUTER REQUIREMENTS

SUMMARY AND RECOMMENDATION

DSD's cryptanalytic effort is dependant on extensive computational support provided by large scale computer equipment. Due primarily to initiatives [redacted], the amount of computation done in support of cryptanalyses has increased by a factor of twenty over the six years from 1977 to 1983.

2. Cryptanalytic computing at DSD is currently supported by a CDC Cyber 175, which was installed in November 1977 at an investment cost of approximately $4.2Million. This machine operates 24 hours a day 7 days a week, and since early 1983 has been saturated.

3. An analysis of communications trends [redacted] of importance to Australia has shown that the demand for cryptanalytic computation will continue to rise rapidly throughout the remainder of this decade, reaching an estimated 30 times the existing computational capacity by the early 1990's.

4. To meet the immediate requirement the installation of a CRAY computer system is proposed in 1985 at an investment cost of $10.5M dollars, plus $1.315 for associated works. By this time it is expected that the existing CYBER system will be providing less than 30% of the required computational power, however, it is not considered feasable to shorten the project timescale due to works lead time.

5. The initial upgrade will provide 10 times the power of the Cyber 175. To meet projected requirements by the early 1990's, a further upgrade in 1989 is proposed, at an estimated cost of $3.0M

6. The estimate of $10.5M represents a substantial cost increase from the $5.5M programmed in the 1983/84, 87/88 FYDP. This increase arises from a combination of technical, international exchange [redacted] ralated factors. These are addressed in more detail in the body of the paper. However, in considering the cost of DSD's cryptanalytic activities, it is significant to recognise that the cost of the proposed system, adjusted for inflation, would be equivalent to $4.56M in 1977 dollars, 8% more than the $4.2M cost of the CYBER 175.

[redacted]

7 aug
June 1983 SM

UPGRADE OF CRYPT PROCESSING FACILITIES AT DSD -
ANALYSIS OF COMPUTER REQUIREMENTS

Reference: A. Cryptanalysis at DSD: Project Lobster - Upgrade of General Purpose Processor CHR/01/83

B. ADC minute to Dir 23 March 83

C, SM Technical Report No 50 [redacted]

INTRODUCTION:

Large scale computer support is an indispensable component of DSD's cryptanalytic capability. Even though the rate of technological advance in micro-electronics has enabled a spectacular rate of increase in power to be maintained in the development of new computers, the demand for computer power to support even a moderate cryptanalytic capability still requires the use of machines near the limit of what is commercially available.

2. DSD cryptanalytic computer support is provided by the Control Data CYBER 175, which was installed in Nov 1977 providing 20 times the computer power of the CDC 3400. The CYBER 175, although exceeded in general purpose power by many current computer systems, has features exploitable for cryptanalytic computation which have enabled it to operate at speeds which can still only be substantially exceeded by two other types of computer on the commercial market, the CYBER 205 and the CRAY machines.

3. Nevertheless the CYBER 175 is now fully loaded. Various steps have been taken since the introduction of the CYBER to increase its effective power, including equipment enhancements, optimisation of programmes and operating procedures, and extension of its operation to 24 hrs a day, 7 days a week. All major opportunities for refinement of the CYBER 175 system have now been exploited and it is estimated that at most an additional 3-5% capacity could be obtained by expenditure of further effort.

4. This is a matter of immediate concern to DSD, as even aside from the projected future growth in computation requirements described in Ref A and B, a very large growth has been experienced over the last two years, due in considerable part to changes in communication practices by one of DSD's most important targets [redacted]

5. There are substantial indications that this rate of growth will continue at least through 1983, which indicates that a capacity shortfall of over 50% will exist by the end of 1983. This will inevitably cause a reduction in timeliness of output, the dropping of lower priority work and increased dependence on [redacted]

Project Caveman

REQUIREMENT:

agreed

6. Two important factors determining the computer equipment appropriate to an upgrade in crypt processing capacity are computer power, and software compatibility, and these are considered separately below:

ese references
e internal
numents;
however
on included
a footnote.

(a) Computer Power

Internal studies (1,2) have shown a

There is a well substantiated need for a considerable upgrade of DSD cryptanalytic processing capacity. References A and B document the changes which are expected [redacted] which will require an upgrade of at least 10 times in processing power initially, and by a factor of 30 by the 1990's. The urgency of proceeding with all possible speed is also confirmed by an analysis of usage trends over the last six years which show:

these studies

(1) Cryptanalytic computer use since the introduction of the CYBER 175 has increased by a factor of over 20 compared with the use of the CDC 3400 in 1977.

(2) Growth in the last year was 64%.

(3) The CYBER 175 is now completely saturated, and although all processing requirements are currently being met, timeliness is affected. Further information on growth in computer usage is provided at Appendix A

Annex A

Para Heading →

(b) Software Compatibility

Apart from the need for greatly increased computer power, the increasing diversity and difficulty of target systems creates a corresponding increased need for complex software, which could considerably exceed the capacity of current DSD programming and cryptanalytic staff. The main cryptanalytic computers at GCHQ and NSA are compatible, and have been [redacted] for a number of years, and a large body of software [redacted] has been developed and is available at both centres.

staff?

40
8
320

The combined cryptanalytic programming manpower at NSA and GCHQ is approximately [redacted] the 8 available at DSD. Of this effort, approximately 25%, or [redacted] per year of cryptanalytic software development is of high interest to DSD, and another [redacted] per year of potential interest. If DSD obtained a computer compatible with GCHQ and NSA, it would allow access to this large and growing resource. [redacted]

Equipment Alternatives:

7. [redacted] However, there are substantial architectural differences between the CRAY and CDC computers, and so only limited compatibility exists between them.

8. In assessing equipment alternatives, due to the high rate of technological change which occurs in the computer industry, future machines which may become available in the timescales of interest must be considered as well as currently available machines. Extensive discussions have been held with the Control Data Corporation both in Australia and the U.S. and with the U.S. and U.K. representatives of Cray Research Incorporated. No other companies produce computers capable of meeting either the power or compatibility requirements.

9. The Control Data Computers which are capable of supporting [redacted] and other software of interest to DSD are the CYBER 7600, CYBER 176 and CYBER 170/875 systems. Of these, the most recent, and powerful model is the CYBER 170/875, which would cost approximately $6M and only offer a moderate increase in processor capacity (approximately 2 times). In addition, as the focus of all NSA and GCHQ cryptanalytic development is shifting to CRAY machines, the degree of compatibility obtained would decline to a negligible level by 1990. A somewhat more powerful computer (the "Theta machine") is planned for release by CDC in 1985 or 1986, however it will contain features which further prejudice its compatibility [redacted] The Control Data Corporation does produce a computer of appropriate power, the CYBER 205, however, it is of a different architecture to both the other CDC machines and the CRAY machines, [redacted] and so is not suitable.

? what CC175 ?

[redacted]

10. The Cray Research Corporation produces three computer models; and the 1S series, the 1M series and the XMP series which are all substantially similar in architecture, although the characteristics of cryptanalytic programs do place certain constraints on the configurations which are acceptable. The CRAY machines are the only machines available which provide the required increase in power, and possess the compatibility with NSA and GCHQ general purpose cryptanalytic processors at least until the 1990's.

11. Complete Cray computer systems can be obtained for between $A6.7M and $A13M depending on the model chosen. The model which would both meet DSD's initial needs in the 1986-88 time frame, and be the most economic in the longer term considering projected upgrade requirements is the "XUP22" system at an estimated cost of $A10.5M. This model is not currently commercially available, but it is expected that such a machine, a single processor version of the existing multiprocessor XMP22 will be released by 1985. The XUP22 should be field upgradeable to the XMP22. A more detailed analysis of the Cray machines is provided at Appendix B.

should be ANNEX B

Declassified by ASD - 7/02/2022
Information removed for national security and/or personal sensitivities

Financial Aspects

12. Provision of $5.5M for cryptanalytic computing exists in DSD's FYDP, for authorisation 84/85 and expenditure 85/86. This estimate was based on the characteristics and price of suitable CDC equipment which it was expected would be available by 1985. There are several reasons for the considerable disparity between this estimate and the amount of $10.5M now considered necessary. These are:

(a) The ~~large~~ reduced reduction in the value of the Australian dollar,

(b) The realisation after visits to NSA and to Control Data Headquarters in the U.S. in Oct 82 and subsequent consultation with visiting CDC personnel in Australia, that future Control Data machines would be considerably less powerful than expected, and have an architecture of limited use to DSD.

(c) The commitment [redacted] to CRAY XMP computers for general cryptanalytic processing.

(d) Increased perception of the rate of increase in difficulty of DSD's major targets, obtained both from local research in DSD and from consultation [redacted]

13. Much of the information which has influenced planning [redacted] is still confidential company product planning information, and was not available earlier.

14. Some early indication of the uncertain suitability of the Control Data equipment configuration on which the $5.5M estimate was based was obtained just prior to the FY 83/87 bids in July 1982. In the SM FYDP submission attention was drawn to the fact that the anticipated equipments may not prove a viable approach in which case an estimated $12M would be required. Because of the unanticipated equipment characteristics which were becoming evident in Control Data Corporations future computers, $0.6M was budgeted over 1985/87 for contracted operating system modifications to attempt to retain [redacted] compatibility. This is no longer required as further information has shown the CDC machines to be totally unsuitable. Provision of $0.350M p.a. for hardware maintenance was also provided in the 83/87 FYDP. For the system now proposed, an estimated $0.500M p.a. is required.

83/88 ?
NOT allowed to DP1 88

15. Equipment lease is an available alternative to purchase. Leasing costs are examined in detail at ~~Appendix~~ C.

ANNEX C

1985/86, 86/87 ?

Declassified by ASD - 7/02/2022
Information removed for national
security and/or personal sensitivities

Manpower

16. Software Systems support for a [redacted] system will be a task of significantly greater workload and complexity than support of the existing CYBER 175/NOS-BE system. There will be further demands on available skills and manpower in the first two years of operation of the system, as major software systems are acquired from NSA and installed, and DSD software is converted from the CYBER 175. To help support this initial phase, it is proposed that DSD seek the attachment to DSD of an NSA Data Systems Programmer and also obtain software support from the computer supplier.

17. The current establishment for support of the CYBER, one CS03, two CS02's and one CS01 will not be sufficient for the provision of adequate systems software support and specialist advice to users of the system, especially whilst maintaining concurrent operation of the CYBER 175. The uniqueness and complexity of the [redacted] operating system, the CRAY hardware, and the cryptanalysis application will make considerable demands on software support personnel. Also, because of the highly classified nature of the application, and the [redacted] of the operating system, a considerably greater independence from external software consultancy and support, such as that normally provided by the computer supplier, is also required.

must be met from within DSD ceiling

18. It is expected that another two positions will be required for [redacted] support. The classification levels require review, and this should be undertaken in conjunction with relevant A Branch and CESTAB personnel, with particular regard to the position classification standards relating to specialist computing activities.

"

19. The use of [redacted] cryptanalytic software will to a considerable extent enable DSD to cope with increasing target complexity whilst containing overall staff numbers. However, one additional cryptanalytic programmer at DO2 level will be required by CHR to assist in the installation and maintenance of software obtained from NSA and GCHQ.

Works/Facilities

([illegible] [illegible] NOT relevant to DPI Refer DFI

20. The installation of a CRAY computer system requires substantial works in the first floor computer area, and is dependant on the removal of the 3400. Of greatest significance however, is the requirement for considerably increased power and airconditioning capacity. The detailed requirements were provided to AG on 9 March 83 and are under consideration by the Works Committee in conjunction with other projected demands on building resources.

21. There will be additional works requirements for the placement and connection of VDU equipments. At this point it has not been resolved whether the terminals will meet, or can be modified to meet TEMPEST requirements. If TEMPEST criteria can be met by the VDU's, user terminals will be deployed in existing office space on the third floor.

Declassified by ASD - 7/02/2022
Information removed for national
security and/or personal sensitivities

ANNEX

22. An initial assessment of works requirements has provided a cost estimate of $1.315M (see Appendix D). It has been proposed that initial works be limited to those items critical to the initial operation of the system, in order to meet the early target date. The provision of additional building backup power, and shielded work areas for VDU's if necessary, would proceed over the two years following IOC.

Travel Requirements

MARSIK

23. As stated earlier, project LOBSTER requires the installation and support of [redacted] software developed within NSA. As a result the support structure which normally is expected for the distribution and installation of commercially obtained software does not exist. Therefore we are reliant on NSA and GCHQ to make available the software and associated documentation, and for developing the necessary skills in DSD specialist software staff. The only practical way to achieve this is by a combination of TDY's and long term attachments to NSA and GCHQ. A one month TDY in 83/84 has been programmed for a software specialist to resolve technical and planning matters, and two 12 month attachments of software specialists has been programmed for 84/85 to allow for adequate technical training and acquisition of software.

TDY acceptable alternative?

24. To enable acquisition of cryptanalytic applications software, and training in its use, two 12 month TDY's of CH cryptanalytic staff will also be necessary, one in 84/85 and one in 85/86.

Implementation Schedule

25. The proposed implementation schedule is as follows:

	Early	Late
Preliminary Planning Papers to support revised programme estimates.	June 83	June 83
Project Submission to Director	Aug 83	Aug 83
Detailed Implementation Plan	Dec 83	Dec 83
Project Approval	Apr 84	Apr 84
Specifications for equipment procurement	Apr 84	Jul 84
Release of request for tender	Aug 84	March 85
Equipment Selection	Dec 84	Nov 85
Equipment Delivery	Aug 85	Nov 86
Equipment Acceptance	Nov 85	Feb 87
Operational Availability of LOBSTER system (MARSIK)	Feb 86	May 87
Phased installation of major NSA utility software.	Feb 86- Dec 86	May 87- March 88
Conversion of Applications software from CYBER 175.	Feb 86- Feb 89	May 87- May 90
Decommission CYBER 175	March 89	June 1990

Delete intermediate milestones

Remain CDC 3400

WORKS

A NNEX

APPENDIX A

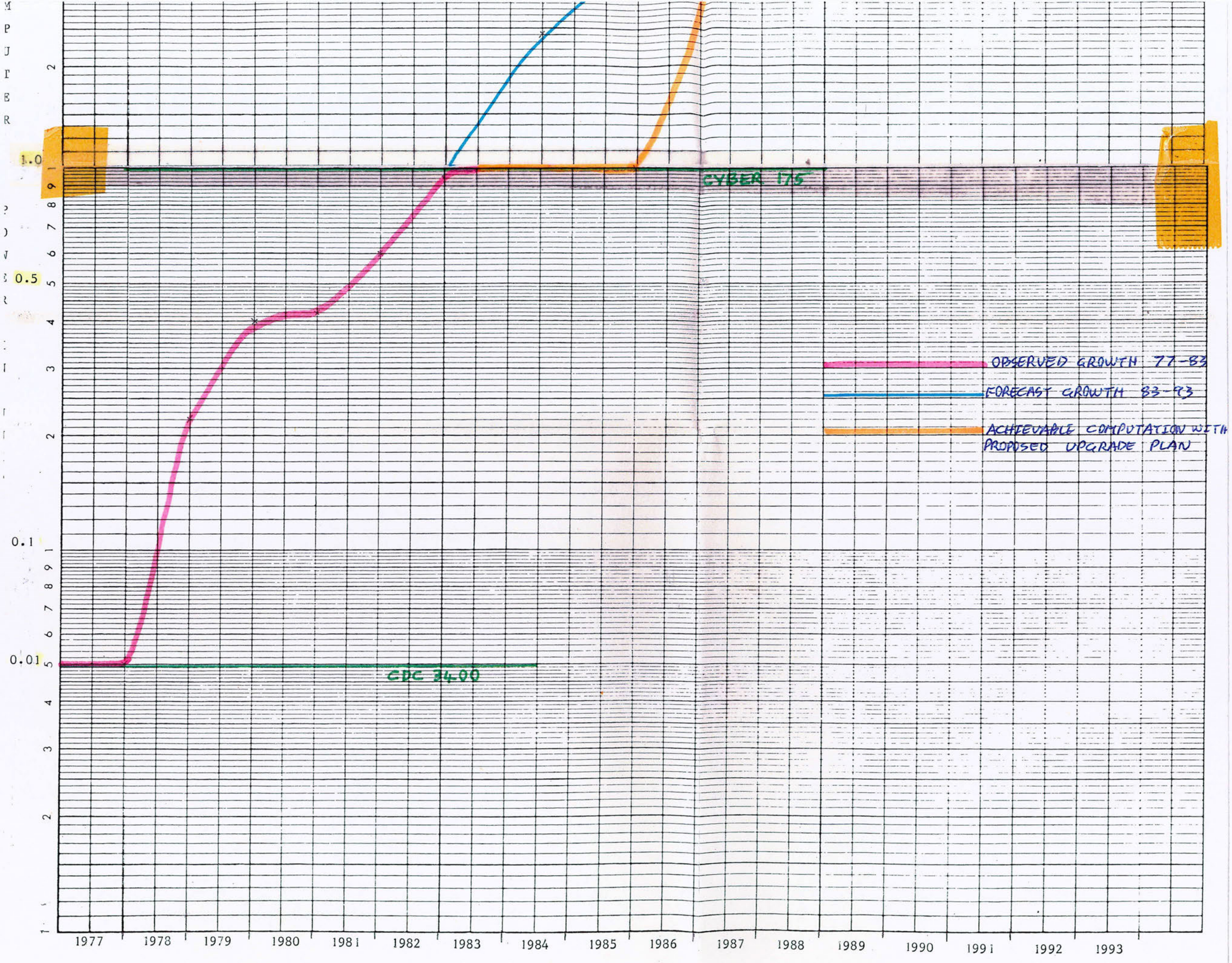
COMPUTER USAGE FOR CRYPTANALYTIC COMPUTATION

Computer usage on the CYBER 175 since its introduction in Nov 77 is shown on the attached graph. Due to difficulties in obtaining an accurate separation of cryptanalytic and other use in the historical data available, total computer use on the 175 is shown. Computer use on the CYBER 175 for other than cryptanalytic processing is now less than 8% of the total usage. The use of the CYBER 175 for other processing has if anything decreased over the last two years, and so the actual growth rate of cryptanalytic processing has been higher than the graph would indicate.

The very high growth rate in cryptanalytic processing requirement is expected to continue over the next 7 to 10 years, and this is represented by the extrapolated curve shown in blue. In practice, growth does not occur at a constant rate as rapid growth tends to be associated with the introduction of improved communications security procedures or new equipment in specific target countries.

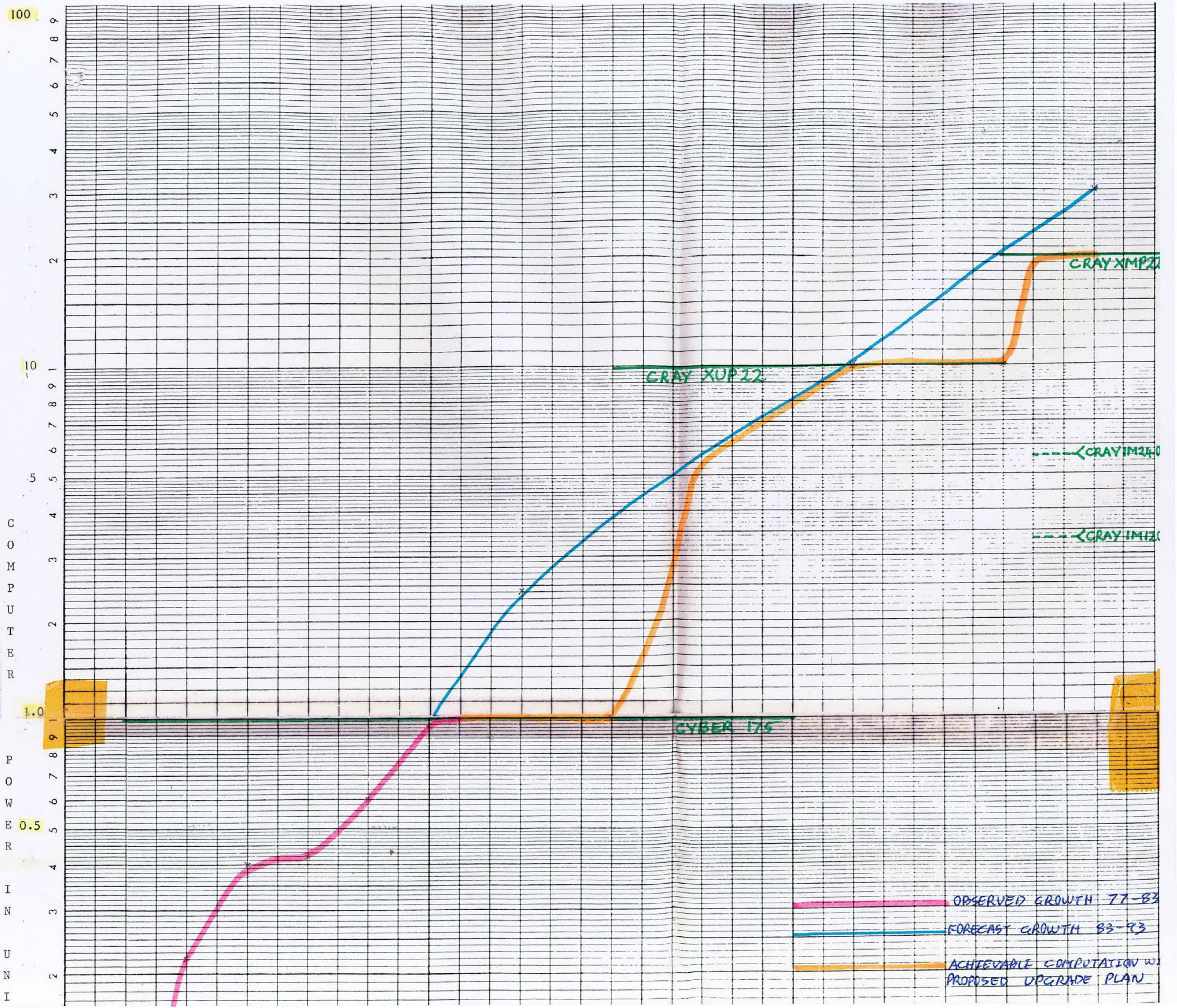
Achievable computational power with the proposed upgrade plan is shown in orange. This line shows that DSD's cryptanalytic computational power has now plateaued and a considerable shortfall in capability will develop prior to the proposed installation of a new system in late 85. An additional factor illustrated by this line is that it takes a significant time to exploit the available power of a new system due to the software conversion and development work involved. The green lines indicate the maximum achievable power of the various computers considered in this report.

not a real [illegible]


M
P
J
T
E
R
P
O
W
E
R
1.0
0.5
0.1
0.01
CYBER 175
CDC 3400
OBSERVED GROWTH 77-83
FORECAST GROWTH 83-93
ACHIEVABLE COMPUTATION WITH PROPOSED UPGRADE PLAN
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993

37H(ii)

Declassified by ASD - 7/02/2022
Information removed for national
security and/or personal sensitivities



ANNEX B

APPENDIX B

CRAY RESEARCH COMPUTERS SUITABLE FOR DSD CRYPTANALYTIC PROCESSING

1. Cray Research currently market three different models of computer systems. All three models have substantially the same architecture, and a range of options is available within each model. The three models are the 1S, 1M and XMP ranges.

2. The 1S is the oldest model, and it is expected that within a year it will no longer be produced. The 1M range uses the same Central Processor technology as the 1S range, but has more modern and cost effective memory technology.

3. Due to the different characteristics of this memory technology the smallest, most economic machine in the 1M range, the 1M1200, is not particularly satisfactory for optimised cryptanalytic programmes.

4. The XMP range represents the technological direction of the next range of CRAY machines. It has higher density, higher speed circuitry than the CRAY 1S and 1M ranges and in terms of performance per dollar is considerably cheaper. However, the initial machine released, the XMP22 is expensive as it is a large, two central processor machine. It is expected that this range will be extended in the future by the addition of both single processor and four processor models to the range. The machine of interest to DSD is the single processor version of the XMP and is referred to in this paper as the "XUP22".

5. Below is a tabulation of the estimated prices and performance of various CRAY configurations. In all cases the same configuration of peripheral equipments is used, and is the configuration described in 2.1 through 2.4 of SM Technical Report No. 50 "LOBSTER [redacted]

6. Costs are based on known U.S. domestic prices, except for the price of the special 3rd IOP added to the 1M2200, to make a 1M2300, and the predicted price of the XUP22 which were obtained from informal sources. Cray international prices are 10% higher than domestic prices, and adjustment must also be made for exchange rate to obtain prices in Australian dollars.

Exchange rate: $1A = 0.868 $U.S.

Equipment		Price $U.S.	Price $A
Peripheral Configuration		1,244,460	1,577,081
1S2300 Processor		7,410,000	9,390,553
1M1200	"	4,000,000	5,069,124
1M2300	"	5,710,000	7,236,175
XUP22	"	7,000,000	8,870,000
XMP22	"	9,000,000	11,405,529
XMP4	"	15,000,000	19,009,216

Total system costs are obtained by adding the cost of the peripheral configuration to the cost of the particular processor selected.

System	Price, Millions of $A	Performance Times CDC 175 on optimised cryptanalytic code
1M1200	6.7	3.3
1M230C (B)	8.8	5.6
1S2300	11.0	6.9
XUP22 (A) (C) (D)	10.5	10
XMP22 (C)	13.0	20
XMP4 (C) (D)	20.6	40

NOTES: A. The expected XUP22 model meets DSD initial upgrade requirements at an estimated cost of $A10.5M.

B. The 1M2300 as well as falling considerably short of the projected initial upgrade requirement of 10 times the power of the CDC 175, has no upgrade capability. Even assuming an optimistic recovery of 50% of the purchase price of the 1M2300 processor on replacement, upgrade to an XUP22 would cost $5.25M, a total cost to the department of $3.62M more than if the XUP22 was obtained initially.

C. Due to expected further advances in technology of both processor circuitry and memory components, further changes in price and/or performance may occur.

D. These machines are not yet available.

Maintenance Costs:

Maintenance costs vary very little between the systems considered. This is due to:

(a) The large fixed cost of the test and repair facility required for all CRAY machines, and

(b) The use of newer more reliable higher density circuitry in the faster machines, which compensates for their increased complexity.

The expected maintenance costs of the systems considered are all within approximately ± .020 of $0.5M p.a.

Declassified by ASD - 7/02/2022
Information removed for national
security and/or personal sensitivities

APPENDIX C

PROCUREMENT OF CRAY COMPUTERS BY LEASE

1. An alternative to purchase of computer equipment is the use of leasing arrangements. Lease could be arranged directly from the CRAY company, [redacted]

2. Lease from the computer company is the more flexible, as it would allow either purchase conversion of the equipment at a subsequent date, or return of the equipment to the supplier when an upgrade was necessary. Lease from the computer company is cheaper for short term lease, but only provides limited equity in the equipment. If purchase conversion is chosen at a later stage, only 55% of the lease payments are credited against the purchase price. The purchase price used is also the company list price rather than the depreciated used equipment value which further reduces the attractiveness of this option.

3. Third party lease is typically a full payout lease, and as such is effectively a loan with the equipment as security. On a long term lease a third party lease can be considerably more attractive than lease from the equipment supplier.

4. Lease costs for the various CRAY CPU's is shown below:

Processor	Performance factor, times CDC1/5	Processor Cost, $A	CRAY 3 yr Lease, cost p.a.	3rd Party full payout Lease (Cost from Hill Samuel)	
				3 Yr Lease $M p.a.	10 Yr Lease $M p.a.
1M1200	3.3	5.07M	1.60M	2.22M	0.91M
1M2300	5.6	7.24M	2.29M	3.18M	1.29M
1S2300	6.9	9.39M	2,97M	4.12M	1.68M
XUP22	10	8.87M	2.80M	3.89M	1.59M
XMP22	20	11.41M	3.61M	5.00M	2.04M
XMP4	40	19.00M	6.01M	8.33M	3.40M

5. As can be seen, the cost of short term lease is such that there is no financial benefit in the use of lease to enable a cheaper interim machine to be installed for, say 3 years and then subsequently exchanged.

6. If the peripheral configuration was purchased, the total costs per annum, on a 10 year lease, including 0.5M p.a. for maintenance, are as follows:

Processor	First Year Cost, Including peripheral purchase	Subsequent Years
IM1200	3.01M	1.41M
IM2300	3.39M	1.79M
IS2300	3.78M	2.18M
XUP22	3.69M	2.09M
XMP22	4.14M	2.54M
XMP4	5.50M	3.90M

APPENDIX D

PROPOSED WORKS BUDGET

		Budget	Works to be completed by
1.	Works for accommodation for frequency converters and refrigeration plant, extensions to mechanical services riser.	$0.130	Aug 85
2.	Floor load spreading on first floor, upgrade of goods left capacity.	----?	Aug 85
3.	Maintenance room for computer.	$0.015	Aug 85
4.	First floor mechanical, including upgrade of air conditioning arrangements.	$0.030	Aug 85
5.	Upgrade SEC substation.	$0.020	Aug 85
6.	Electrical and mechanical reticulation, and rework of main switchboard.	$0.200	Aug 85
7.	Additional Cooling Tower.	$0.280	Aug 85
8.	Additional electrical and mechanical reticulation and rework of main switchboard for	$0.150	Dec 87
9.	Additional Diesel.	$0.400	Dec 87