~~SECURITY INFORMATION~~

US BRUSA REPORTS TO BE AVAILABLE FOR 1953
BRUSA COMSEC CONFERENCES

BRUSA PAPERS FORWARDED TO UK	BRUSA NO.	BRUSA PAPERS TO BE FORWARDED TO UK
1. REENTRY SYSTEMS		
a. AFSAM 7 (POLLUX/ADONIS	74,83,91,92,93,95, 96,97,98,99,109(NSA-34), 140,145,154,180,252 (NSA-34),253,257,268, 270	
b. AFSAM 9 (IRIS/PYGMALION, ATHENA, AENEAS)	69,76,82,89,90,100, 101,102,103,112(NSA-34), 126,130,155,187,198,258, 261	
c. AFSAM 7 - AFSAM 9	88,163,266	
d. General	184,276	
2. REFLEX TELETYPE SYSTEMS		
a. ASAM 2-1 (MINERVA/APOLLO/ ORCUS)	263,277	
3. CALL SIGN CIPHER SYSTEMS		
a. AMAZON	278	
b. PENELOPE	271	
c. General	53(NSA-34),255	
4. CCM SYSTEMS		
* a. AJAX	70,72,84,85,86,87,94 133,147,148 and addendum 174,179,254	156-"Recovery of Setup for Two Isologous Encipherments in AJAX or HERMES with R4 Misplaced"
* b. HERMES	77,115,120,183,191	
* c. AJAX-HERMES	135,144,165 and addendum 193,194(NSA-34)	171-"Length of Crib Needed and the Time Required for an Exhaustion Attack by a Catalogue Process on AJAX, HERMES and LUCIFER

* Papers are included since they contain valuable supporting material for discussions of LUCIFER. There will be no need to discuss AJAX or HERMES per se.

~~SECRET~~

BRUSA PAPERS FORWARDED TO UK	BRUSA NO.	BRUSA PAPERS TO BE FORWARDED TO UK
d. LUCIFER	111,141,152,169,175,176 177,185,199	
e. BRUTUS	25,71,79,81,127,128,129 164	172-"Identification of the Cores and Notch Rings in LUCIFER from Matched Plain and Cipher Text"
f. BRUTUS-JUPITER	195	
g. PORTEX	173,178,192	
h. General	48,49(NSA-34),108, 110(NSA-34)	189-"Identification of LUCIFER MARK I Setup from R5 Offset Situation"
5. ELECTRONIC KEY GENERATOR		
a. KOKEN	56(NSA-34),57(NSA-34), 262,265	264-"Analysis of Combining Circuit of 37 Stage KOKEN"
b. ARTICHOKE		279-"Coincidence Tests on ARTICHOKE Key"
c. ROLLICK	45	281-"An Evaluation of the Crypto-security of ROLLICK"
d. DEM 22	113	
6. IFF SYSTEMS	259,269	256-"Tentative Crypto-security Evaluation of the BSI System"
7. ECM SYSTEMS		
a. HERCULES	260	
8. ENIGMA SYSTEMS		
a. TYPEX	280	
b. DEM 17	116,117,189	
c. SIMPLEX	191	
9. HAGELIN SYSTEMS		
a. M-209	104,105,106,107,134 (NSA-34)	

BRUSA PAPERS FORWARDED TO UK	BRUSA NO.	BRUSA PAPERS TO BE FORWARDED TO UK
b. MEM (MARS)	62,139,167,186,196	
c. DEM 21	151	
10. AUTHENTICATION SYSTEMS		
a. DEM 498	162(NSA-34),267	
b. SATYR	181	
11. ONE-TIME EQUIPMENT SYSTEMS		
a. AFSAW 7200	200,274	
12. CODES		
a. ASREX	73	
13. WEATHER SYSTEMS		
a. DEM 31	150	
14. MANUAL SYSTEMS		
a. PLAYFEX	44	
b. MERCURY	272	
c. STRIP SYSTEMS	43,80,158(NSA-34),159 (NSA-34),160(NSA-34), 273	
15. CIPHONY SYSTEMS		
a. AFSAY 806(THOR)	142	
b. AFSAY 816 (BELLEROPHON)	131	
c. DEY 804	146	
d. DEY 807	149	
e. DEY 808	137	
f. DEY 809	143	
g. AFSAY 830	166	
h. HALLMARK Key Generators	46	

BRUSA PAPERS FORWARDED TO UK	BRUSA NO.	BRUSA PAPERS TO BE FORWARDED TO UK
16. CIPAX SYSTEMS		
a. AFSAX 500 (CYCLOPS)	123,125	
b. DEK 503	136	
c. METFAX	47	
17. DUP 1	12	
18. GENERAL CRYPTANALYSIS	NSA-34: 50,51,52,54, 55,58,59,60,61,67,114, 118,119,132,157,161, 194,251 NSA-412: 63,64,65,66,68, 78,121,122,124,182,197, 275	
19. GENERAL REPORTS	170	

MISCELLANEOUS ITEMS SENT:

1. "Recommended New AJAX-HERMES Procedure" - (no BRUSA number)
2. CCM Summary Sheets

- -

BRUSA PAPERS BEING PREPARED FOR CONFERENCE

1. Cryptosecurity Evaluation of DEM 17 With One CCM Cascade
2. Cryptosecurity Evaluation of RASSIM
3. Cryptographic Data Sheet of PYGMALION Cryptosystem (Tentative)
4. Cryptographic Data Sheet of IRIS and AENEAS (Tentative)
5. Cryptosecurity Evaluation of IRIS Cryptosystem
6. Cryptosecurity Evaluation of ATHENA Cryptosystem
7. Cryptosecurity Evaluation of BALDER Cryptosystem

8. Cryptosecurity Evaluation of PANDORA Cryptosystem

9. LOUSE Method of Attack on POLLUX (BRUSA C/S 282)

10. Reconstruction of R7 Core Wiring and R4 Notch Ring on POLLUX/ADONIS

11. Effect of Faulty Stepping on AFSAM 7