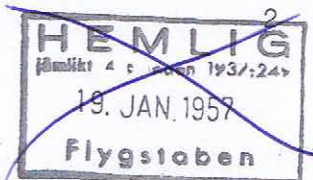


H 19



ORIENTERING I TELETJÄNSTEN

19/1 1957

Delgivning:

Enl fljch (motsv) best.

Särskild utsändningslista: Nr 5-12, 14-23, 64-65, 68 utdelas ej.

KRYPTOKONTROLL.

Vid granskning av kryptotrafiken till CFV under december (fr o m 9/12) visar det sig att genomgående samma fel, som upptagits i OTEL nr H 17 den 3/12 1956, fortfarande göres vid FV förband.

Söndagen den 9/12 utsändes ett kryptomeddelande från CFV (tnr 1100) för kontroll av kryptotjänsten, varvid framkom att erinringarna i ovannämnda OTEL icke medfört önskad förbättring.

Förteckning över respektive avsändares enskilda fel vid svar på CFV tnr 1100 9/12 redovisas i bilaga 1, sid 1.

Tiden, innan CFV tnr 1100 9/12 blivit dekrypterat, har vid F 6, F 8, F 11 och F 17 varit ovanligt lång; detsamma gäller tiden för kryptering och sändning av svar från F 1 och F 14. Jfr fo A H 13/1956.

Iakttagelser från kryptotrafiken till CFV under tiden 10/12 - 31/12 redovisas i bilaga 1, sid 2.

Det måste ånyo understrykas att en förutsättning för att önskvärt textskydd medelst krypto skall kunna erhållas såväl i dagsläget som för framtiden är att givna bestämmelser noggrant efterlevas.

Flygledningen är väl medveten om svårigheterna främst för dagoff (som normalt icke sysslar med kryptotjänst) att väl behärska kryptomateriel och föreskrifter. Det är dock ofrånkomligt - om ÖB anvisningar och FV beredskap skall kunna innehållas - att till förbandet ankommet meddelande snabbt kan lösas (fo AH 13/1956 p 9) och att tydligt och om möjligt helt korrekt svar kan avges inom begränsad

2.

tid. En generell förbättring av kryptotjänsten är därför påkallad.

Kryptotjänsten vid förbanden måste övervakas bättre.

Kryptomeddelanden från FV-förband visar genomgående, att bruket av skiljetecken och ordskillnad (GBKK mom 422 och 423) icke helt behärskas. Brott mot dessa två moment försvårar mottagarens redigering av klartexten, och felaktigheter kan lätt uppstå.

Krypterings- och dekrypteringstid för kryptomeddelanden kan minskas genom att för dagen gällande F-X nyckel, som i första hand användes vid beredskapsmeddelanden, inställes i förväg.

Beträffande formulering av meddelanden se Ufl 6/1956 sid 167-168 (Är Du "Signalminded"?).

På tpr-nätet förmedlas viss trafik från armén och marinen. Denna trafik innehåller emellanåt hemliga meddelanden på klartext, beroende på att användningen av trådfjärrskrift inom dessa försvarsgrenar har ringa omfattning och att sekretessbestämmelserna därför medge viss möjlighet härtill. Enligt överenskommelse vidarebefordras sådana hemliga meddelanden t v i klartextform på tpr-nätet.

Iakttagelser från kryptotrafiken vid svar på CFV tnr 1100 9/12 IL.

(avsänt med tpr kl 1130).

Förband	Dekrypterat kl	Svar CFV tillhanda kl	Begångna fel	Hänvisning
F 1	1307	1546 4,15	Felaktig ordskillnad. Adressmening i klartext.	GBKK 422 GBKK 417
F 3	1215	1224 1	Svar i klartext.	GBKK 318
F 4	1225	1302 1,20	--	
F 5	1235	1306 1,20	--	
F 6	1340	1516 2,75	--	
F 7	1225	1323 2,-	Felaktig ordskillnad.	GBKK 422
F 8	1430	1441 3,15	Svar i klartext.	GBKK 318
F 9	1220	1304 1,20	Felaktig ordskillnad.	GBKK 422
F 10	1230	1310 1,45	--	
F 11	1350	1435 3-	Meddelandet ej avdelat. Felaktig ordskillnad.	IMGB 43 GBKK 422
F 12	1227	1304 1,20	--	
F 13	1230	1829 2-	Meddelandet olösligt 1)	
F 14	1215	1417 2,45	Felaktig ordskillnad.	GBKK 422
F 15	1222	1247 1,15	--	
F 16	1220	1310 1,45	Felaktig ordskillnad. Fel datumbokstav (H = 8).	GBKK 422 Krybet I 15
F 17	1350	1512 3,25	Meddelandet ej avdelat. Felaktig ordskillnad.	IMGB 43 GBKK 422
F 18	1230	1409 2,20	Meddelandet olösligt. 2)	
F 21	1223	1332 2-	Felaktig ordskillnad.	GBKK 422

1) Nytt medd sedan CFV begärt "corr". Det nya medd var huvudsakligen en repetition av CFV tnr 1100 samt hade felaktig ordskillnad.

2) Nytt medd sedan CFV begärt "corr". Felaktig ordskillnad i medd.

Iakttagelser från kryptotrafiken till CFV under tiden 10/12-31/12 1956.

Förband	Tnr	Begångna fel	Hänvisning
F 11	1100 10/12	"Hemlig" felplacerat.	GBKK 418
F 14	1600 14/12	Ordskillnad skall göras å ömse sidor av namn	GBKK 422
CVA	1140 14/12	Fel krybet. HGHG visar på "HGC (0-9)". "Hemlig" felplacerat.	Krybet I 18 GBKK 416 b)
F 6	2226 17/12	Adressmening "de dagoff" i klartext. Skiljetecken i slutet av medd. (QQ). Fel krybet. NGNG visar på "Komplettering (0-9)".	GBKK 417 GBKK 415 d) Krybet I 18
F 14	1136 17/12	Adressmening "de dagoff" i klartext.	GBKK 417
F 17	2240 17/12	"Hemlig" felplacerat. Felaktig utfyllnad.	GBKK 416 b) IMGB 44 GBKK 544
F 7	1010 18/12	Klartextmeddelande med hemligbeteckning 1).	
CVA	0920 19/12	Klartextmeddelande med hemligbeteckning 1).	
CVA	0935 20/12	- " - - " - - " -	
F 21	1150 29/12	Adressmening "de sigoff" i klartext.	GBKK 417

1) Signalmeddelande som av avsändaren angivits som "Hemligt" skall krypteras, se Sig I mom 70. I detta speciella fall motiverade innehållet i medd dock ej hemligstämpling.