Lecture Cards & Notes

(1)

364 Cards (=8)

Cards retained here since
Cards reviewed 19 Jan 1961

and were not Considered

Classified.

CAUTION THESE R[illegible] BE USED FO[illegible] PURPOSES ONLY, DO NOT REMOVE PAPERS NOR REVEAL CONTENTS TO UNAUTHORIZED PERSON(S)

RECORDS CHARGE-OUT

7356

DATE OF REQUEST	SUSPENSE DATE
25 Jan 1961	10 Feb 61

FILE OR SERIAL NUMBER AND SUBJECT

From File of Special Consultant (Friedman)

Lecture Cards & Notes consisting of 364 Cards used for lecture purposes.

	NAME AND EXTENSION OF PERSON REQUESTING FILE	ORGANIZATION, BUILDING, AND ROOM NUMBER	DATE RET'ND	INITIAL HERE
TO	Mr. William Friedman LI-6-8520	310 Second Street, SE, Wash. D. C.		
RETURN TO	Mrs. C. Christian, AG-24, NSA, Ft. Geo. G. Meade			

INSTRUCTIONS WHEN TRANSFERRING FILE TO ANOTHER PERSON, COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE

2ND TRANSFER COUPON

7356

TO:

FILE (serial number and subject)

TRANSFERRED TO (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE	(sig)	(ext)

#1 ✓ 34 cards ✓

SLIDE 1

Cryptography and cryptanalysis go back to the dawn of the invention of writing, but we won't have time here to go back quite that far, even though the story is very interesting. But I must tell you right off that these two subjects, cryptography and cryptanalysis, are, of course, very closely related - in fact, they may be regarded as the two faces of the same coin. /Explain/

Now may we have the first slide, please?

LECTURE REF ID:A62870 FOR SLIDE 6.21

The syllabary used by Thomas Jefferson (Extract from decoding section)

/That all 'round genius also may be regarded as being the first American inventor of cryptographic devices -- as will be discussed later./

LECTURE NOTE -- [illegible] WW I -- and COMINT

Recall I said when U.S. entered in 1917 had no cryptologic organization. The French, German, and Austrians had organizations which had been functioning many years. Russians had, too, but coordination was poor! Tannenberg -- British had none but built up "Room 40" -Earl of Halifax evaluated its work:

"To Room 40 the country owes an immense debt of gratitude -- a debt which at the time, at least, could never be paid. Secrecy was of the very essense of its work, and never was secrecy more successfully observed.

REF ID:A62870 SLIDE 169

(Portrait - Collange)

Cryptanalysis and the average layman's imaginative picture of a cryptanalyst!

REF ID:A62870

Marshall - Dewey correspondence - TIME Magazine

LECTURE NOTE REF ID:A62870 SLIDE 150

Magic Machine

LECTURE REF ID:A62870 FOR SLIDE 131

The Riverbank "Polyalphabet" -- the first cryptanalytic aid.

[My use of AT&T machines to compile DFC's (1921-22)]

REF ID:A62870 SLIDE 134

My memo begging for one set of IBM, dated 30 Oct 1934.

The IBM contract, dated 12 Nov 1934!

Just one half month later - a remarkable record.
The memo must have been pretty potent medicine!

REF ID:A62870

One wing of IBM installation in WW II

An analog.

(This was for JAS system (Jap MilAtt)

CARD 1

Extracts from: "GREEN [illegible] Intelligence, dated April 1946.

- -

"Signal intelligence was a chief source of information in the German Army. In the eastern theater, where there was offensive warfare primarily, the signal intelligence service was well-organized with well-defined purposes, efficient personnel, and adequate equipment. In the course of the campaign, it was reorganized to exploit to the fullest the success already experienced, and, by 1943, there existed a complete and smoothly functioning machine sufficient to meet all demands."

* * * * * * * *

(OVER)

"Most of their signal intercept success came from low echelon traffic. Armored and artillery radio nets passing operational traffic were followed closely and were one of the chief sources of signal intelligence. Artillery radio nets were given first coverage priority. Apart from messages intercepted in code or in clear, signal procedure, peculiarities of transmitting, and characteristics of Allied radio operators provided enormous assistance in helping to evaluate signal information. The Germans noticed that call signs were often the same for a unit over long periods and that even frequencies remained unchanged for weeks at a time.

Much tactically important information was drawn from the enemy Air Force liaison net. It was assumed that an

(CONTINUED ON CARD 2)

independent net served all Air Force liaison officers attached to the various headquarters and once one of these stations had been picked up and identified, it could be used to trace all other stations over a considerable area. Air Force traffic dealing with bombing targets was intercepted by Air Force units, and was sent through liaison channels to Western Theater Command. From here, over a network going down to divisions, the information would be flashed to all Army formation headquarters. Receiving sets at all levels, including division, were tuned in continually to this broadcast frequency."

* * * * * * * *

(OVER)

"Importance of Signal Intelligence During the Invasion (Normandy).

During the invasion, the G-2s in the West drew about 60 percent of the operationally important information from signal intelligence. The remaining 40 percent was derived from all other fields of intelligence. The amount of information decreased during the months of mobile warfare. During the retreat, although the possibilities of obtaining information became less frequent, the amount of information from signal intelligence remained high. Most of the information was deduced from the organization of enemy radio traffic networks, from decoded messages, and from the radio nets of the enemy Air Force liaison officers who were attached to ground

(CONTINUED ON CARD 3)

troops. Based upon this information the evaluation center of signal intelligence often came to conclusions which, at first, sounded hypothetical to the operational command and were therefore doubted. In 90 percent of all these cases the events verified the signal intelligence information so that eventually more credence was given to its conclusions."

(THE END)

The Analog for Jap "Green"

A "brute force" machine.

Machine for matching messages.

The "Camel"

The "Auto-scritcher"

(Rodin - the "Thinker")

"Camel Code Indicator"

Unit for deciphering message texts.

The "Dudbuster"

LECTURE NOTE REF For Lupa 62870 secrecy

"Importance of secrecy has been long known for it is quite obvious, but its real significance is not well appreciated. The veil of secrecy cannot be removed simply because events are long past."

Extracts from: "Results of Axis Analysis of United States Communications as Revealed by TICOM and other Sources of Intelligence." - Vol. C - German Traffic Analysis of United States Communications dated 16 August 1946. (CARD 1)

"a. "Colonel FRIEDRICH, head of the Signal Intelligence Agency of the Air Force High Command (OKL/LN), had a very poor opinion of allied security, and said that Allied signals were careless to a degree that would not have been tolerated by the German Armed Forces. He agreed that, with the material superiority in possession of the Allies, this lack of security did not make any difference in the outcome of the war. He felt, however, that if the Allies had not been in that particular

(OVER)

position the story would have been quite different." (Chapter III, paragraph 13, page 62).

* * * * * * * *

"c. From the intercept of plain text and other traffic of the United States Army, the Germans had a complete picture of our army organization and even names of officers down to Captain, their units and locations. Ninety-five percent of the information contained in a manual issued to the German troops on the organization of the American Army was gained from radio intelligence. American nets were identified by solving traffic, by operators' characteristics, and by captured Signal Operating Instructions (SOI's). Up until December 1944 our Army Call Sign Book had been almost completely reconstructed with the aid of

(CONTINUED ON CARD 2)

captured sequence sheets." (Chapter III, paragraph 14, page 21.)

* * * * * * * *

"d. "Colonel METTIG, cipher expert of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), stated that it was not at all surprising that some Converter M-209 and American Strip traffic was read by the Germans, since mistakes in the use of these systems were made in one out of every three messages." (Chapter III, paragraph 14, page 22.)

* * * * * * * *

"f. Although the traffic transmitted by Allied observation posts was sent in clear and transmitted by radio sets using low power, it was frequently audible

(OVER)

to the Germans and intercepted by them. This traffic was concentrated upon by [illegible] operators, for then the Germans had time to institute evasive action," (Chapter III, paragraph 14, page 23.)

* * * * * * * *

"g. American radio and radio-telephone traffic afforded a greater amount of data to German traffic analysts than did the British traffic. Colonel GRUBE, chief of Telecommunications of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) stated that United States radio security was generally good on tactical nets but that supply and liaison nets gave everything away, including United States order of battle and intentions." (Chapter III, paragraph 14, page 23.)

* * * * * * * *

(CONTINUED ON CARD 3)

"i. From the c[illegible] which the United States 8th Air Force handled its radio traffic, Lt. Martin LUDWIG, an expert on Allied air order of battle, said 'It can be stated that no attack of the 8th Air Force came as a surprise. General advanced warnings were given some hours before the raids'." (Chapter III, paragraph 14, page 25.)

*** * * * * * *

"t. Lt. Colonel METTIG, of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) said that traffic analysis by the Germans during the landings by the Allies in North Africa was not successful and did not reveal the approach of the landing forces. The approach was carried out in complete radio

(OVER)

silence and took the Germans completely by surprise. The German Navy, said MELLENTHIN, was to blame for the lack of success, but he did not explain just how the Navy was responsible." (Chapter V, paragraph 28, page 109.)

* * * * * * * *

"u. .....

.....

The greatest success achieved by Col. MUEGGE in the whole African campaign occurred in March 1943 when he intercepted an American order to some small American units to maintain complete radio silence until 2200 hours on 17 March. Col. MUEGGE realized that this meant preparations for a big move, so he promptly went to KESSELRING's Chief of Staff, who would not listen to him. The Chief of Staff had no faith in radio

(CONTINUED ON CARD 4)

intelligence. Col. MUEGGE gave up trying to convince the Chief of Staff and returned to his station, where he heard a second, and later a third message, ordering radio silence until 17 March. He went back to KESSELRING's headquarters, this time forcing his way into KESSELRING's own office to report to him in person. KESSELRING listened to him and the next day flew from Sicily to Africa and made complete plans for a defense in case the Allies did make a move. Col. MUEGGE said he actually prayed the Allies would attack, and on the night of 16 March they did attack. This was the greatest German success achieved by Col. MUEGGE's outfit, and in his estimation was derived solely from careless Allied radio procedure." (Chapter V, paragraph 28, page. 116.)

* * * * * * * *

(OVER)

"w. A Russian message announcing the presence of the American planes at the Poltava base was intercepted and decoded by his unit (Sgt. Paul RAATZ's unit. He was a German Army radio intelligence man), resulting in a highly successful operation against the air base on the part of German aircraft.

From newspaper sources it was found out that actually on 21 June 1944, a group of 175 planes of the 8th United States Army Air Force in England arrived at the Poltava base on a shuttle run from their English bases. There were P-51's in addition to the above B-17's in the formation. Of the B-17's, 53 were destroyed." (Chapter V, paragraph 33, page 133.)

* * * * * * * *

"x. (Concerning German knowledge of preparations for airborne operations in the Western front in the last

(CONTINUED ON CARD 5)

days of the war, [redacted] the 82nd and 101st Airborne Divisions from England to the Continent.)
The first indication of a planned operation was the transfer of the 52nd and 53rd Wings from England to France. At the same time, the German Army picked up a Military Police message which revealed that both the known airborne divisions, the 82nd and 101st, had been pulled out of operations at the front, and were in rear areas preparing for new operations. One of these divisions, the Germans knew, was stationed on the military maneuvers reservation at Mourmelon, near Rheims. The Military Police message from which the Germans obtained this information read approximately as follows:

'THE ROAD FROM MOURMELON TO RHEIMS IS TO BE BLOCKED TO ALL TRAFFIC TOMORROW MORNING EARLY

(OVER)

BECAUSE THE 82[redacted] WILL BE MOVING TOWARDS MOURMELON WITH APPROXIMATELY 1,000 VEHICLES.'" (Chapter V, paragraph 38, page 139.)

(THE END)

Berlin (Oshima) to Tokyo, serial number 988, parts 1-3, SSA Bullentin No. H-134920, 10 Aug 44, translated 12 August 1944, sent in the JAD (diplomatic) system. This message, reproduced in full, has been described by officers in MIS as "worth allthe expenses of maintaining the SSA." The text describes conversations with the head of the Todt organization, Albert Speer, in which the latter revealed to the Japanese, and, thus to us, highly important information concerning the production of munitions in Germany. See Appendix, No.6

From "The Achievements of SSA in World War II, p.18

Berlin to Tokyo, serial number 878, parts 14-17 inclusive SSA Bulletin No. D-3348, 9 Nov 43, translated 4 Dec 43 sent in JAS (Military Attache system). The message from which this sample is taken consisted of 32 parts, all of which were ultimately translated. The full text, too long for reproduction here, is a report of a visit made in the fall of 1943 by a subordinate of Baron Oshima to the German western fortifications. The military information contained in this message was of incalculable advantage to the planning of the invasion of France. (See Appendix 5)

From "The Achievements of SSA in World War II",p.19

Hanoi to Tokyo, no serial number, SSA Bulletin No. H-164499, 22 Jan 45, translated 1 Feb 45, sent in the JBB (diplomatic) system. This message is important because it reveals that the Japanese were interested in obtaining uranium. See Appendix, No. 7.

From "The Achievements of the SSR in World War II", p.19

Moscow (Sato) to Tokyo, serial number 1476, SSA Bulletin No. Spec. 011, 29 July 1945, translated 30 July 1945, sent in the JAA-2-JAJ (diplomatic) systems. This three-part message, the translation of which was available to President Truman during the Potsdam Conference, reveals the activity of Sato, Japanese Ambassador to Moscow, at the time of the conference. See Appendix, No. 8.

LECTURE FOR SLIDE 129

Drying out some Japanese code material alleged to have been destroyed.

/U.S. delayed report: 7 Jul 44. Saipan, 2Bn CPs of 105th Reg near Tanapag Harbor overrun by powerful J. attack which wiped out everything and everybody in sight. When area was recaptured a Salvage Co. recovered what could be, and when all reports were in three crypto-documents were not accounted for except to assume the Japanese got them. 105th reported to Hq 27th Div. but the Div. HQ sent a report to AG Washington by letter noting the loss and saying merely "our records have been changed." News reached CSO on 16 Aug, one month after the loss. Documents were Joint Army-Navy key lists for

(OVER)

M-209 and covered the period of 1 June to 31 July - the last 24 days after the loss. The Japanese undoubtedly read considerable traffic. The fact that 5,000 men later lost their lives in the Saipan compaign cannot be attributed entirely to this incident but it seems more than a coincidence that most of these casualties were suffered through well-planned Japanese counterattacks after 7 July, i.e. after the day the first two battalions of the 105th were overrun.