Description of document:	Experiences 1920-1939, by Brigadier John H. Tiltman Presents cryptanalytic experiences of Brigadier John H. Tillman in India and England during the period 1920-1939, both as British Army officer and as War Office civilian cryptanalyst. Discusses details of some early Soviet transposition, additive and one-time pad systems and describes the roles of several other British military and civilian cryptanalysts.
Requested date:	01-August-2017
Released date:	15-May-2018
Posted date:	16-July-2018
Source of document:	FOIA Request National Security Agency Attn: FOIA/PA Office 9800 Savage Road, Suite 6932 Ft. George G. Meade MD 20755-6932 Fax: 443-479-3612 (Attn: FOIA/PA Office) Online FOIA Request Form

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 102197
15 May 2018

This is our final response to your Freedom of Information Act (FOIA) request, which was received by this office on 1 August 2017, for "Experinces 1920-1939, by Brig. John H. Tiltman." Your request has been assigned Case Number 102197 as stated in our previous letter sent to you on 3 August 2017.

Your request has been processed under the provisions of the FOIA. Enclosed is the material you requested. If you need further assistance or would like to discuss your request, please do not hesitate to contact me at foialo@nsa.gov or you may call (301) 688-6527.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd - OGIS
College Park, MD 20740
ogis@nara.gov
(877)684-6448
(202)741-5770
Fax (202)741-5769

Sincerely,

Paul K
for

JOHN R. CHAPMAN
Chief, FOIA/PA Office
FOIA Public Liaison Office

Encl:
a/s

Experiences 1920–1939

BY BRIGADIER JOHN H. TILTMAN

Presents cryptanalytic experiences of Brigadier John H. Tiltman in India and England during the period 1920–1939, both as British Army officer and as War Office civilian cryptanalyst. Discusses details of some early Soviet transposition, additive and one-time pad systems and describes the roles of several other British military and civilian cryptanalysts.

During the summer of 1920, I was on a Russian language course in London. At the end of it, I was about to return to regimental duty, but the War Office intervened and on 1 August I went to work on temporary attachment for 2 weeks at the Government Code and Cipher School, which at the time had a growing backlog of untranslated Russian diplomatic messages. After a few days the War Office decided to hold me there for a year and, in fact, I never returned to my regiment. When I joined it, the Government Code and Cipher School occupied the whole of Watergate House on the Thames Embankment near Charing Cross. GC&CS was formed after World War I of officers from Admiralty 40 OB and the War Office Cork Street office. It was directed by Commander A. G. Denniston, who had been in 40 OB during the war. His deputy was Commander E. W. Travis (later Sir Edward Travis, our director 1942–1952), who at the time represented the Admiralty on COMSEC matters.

I worked as one of a group of from 5 to 7 persons on Russian diplomatic ciphers under the direction of Ernst Fetterlein. Fetterlein had been Chief Cryptanalyst of the Russian Czarist Government and held the ranks of both admiral and general; he had practiced cryptanalysis since 1898 or earlier. At the Revolution he walked out of Russia across the Finnish frontier and was specially naturalized on arrival in England.

At the time of my arrival, Fetterlein's small section was entirely occupied with the solution of the current Moscow-London and London-Moscow diplomatic traffic intercepted in the cable office. All messages were enciphered by simple columnar transposition of Russian plain text conventionally transliterated out of Cyrillic characters. As each message was transposed on a different key, all messages had to be individually solved. The average delay was, I believe, 1 or 2 days.

About November 1920 the system changed, dinomes being substituted for the plaintext letters before transposition. The substitution table used provided variant dinomes for the letters according to frequency, there being, I remember, 7 variants for each of the vowels; In transposition the dinomes were not split.* The original dinomic substitution table was solved by Fetterlein from a "bust"—one of the transposition keys of the earlier system was reused. Solution of the individual messages then proceeded more or less as before. But early in 1921 a new substitution table was introduced, and messages from that time carried the cipher discriminant "DELEGAT" in the preamble. There were this time no busts and for some weeks no progress was made. The only hope appeared to be to find a message containing a long flush repetition, and this could only occur if the variants were badly used. I made the first entry about April 1921. I must admit that I was very lucky in finding an unusually favorable message. None of the workings of those days have survived and I have had to make up a simplified example to show what happened. Suppose Table A to be the substitution table in use. The message which gave me the solution contained the word DOGOWOR (meaning "treaty") seven times. In each case the encipherer had used the first, second and third variants for the letter O in that order and, in fact, had produced an identical 14-digit sequence (11 07 04 18 17 22 19) seven times. Two of these sequences started in the same column of the transposition matrix, as can be seen in the skeleton example Table B, in which all dinomes have been omitted except those forming part of the 14-digit sequence representing DOGOWOR and those entering into the beginning and end of the message. The cipher message is assumed to have been written out in columns of 14 dinomes in order to show that, if the key-length is 24, the elements of the sequence appearing twice starting in the same column will lie in the fourth and twelfth lines in the cage, respectively. The message was the second part of a three-part message and, therefore, the plain text began PROD (i.e., abbreviation for "continuation") and ended PROD. SLED (i.e., "continuation follows") and these overlapped the flush repetition to a certain extent.

Table C shows, again in skeleton form, the appearance of the cipher text on the assumption of a key-width of 24. The elements of the flush sequences are squared. In Table D the columns containing the elements of the flush repetition were grouped together and rearranged when it was realized that the DOGOWOR sequence occurred a third time at an offset of one dinome from the start of the flush repetition.

*On another link a similar system was used in which the dinomes were split and columns of single digits transposed. In this system Fetterlein had some success, but only in the cases of one bust and a few perfect rectangles.

From this point, it was possible to complete the matrix as shown in Table E and recover a considerable part of the substitution table. This enabled us to recover a number of other transposition keys. It had long been suspected that the keys were derived in the orthodox manner from running text, probably from lines of poetry, in view of the variation of key-length, and Fetterlein had tried to reduce the recovered keys to Russian without success. One day I tried English instead of Russian and met with immediate success. Fetterlein had shown me how to display a key by writing the consecutive numbers from left to right and dropping a line every time a number was to the left of the next lower number. Table F shows the derivation of the key I recovered from the DOGOWOR message. To cut a long story short, I traced the source of the keys in the British Museum Library. It turned out to be an out-of-print pocket edition of the works of George Wither, an obscure poet of the Seventeenth century. I do not remember the method of indicating keys, but I know it was simple and that, after finding the source book, we were in a position to decrypt DELEGAT messages as soon as the intercepts reached us.

In the summer of 1921 the War Office was looking for a replacement in India for Colonel W. H. Jeffery, who had been an officer in a southern infantry regiment of the Indian Army, but had in fact never served with his regiment. He had spent the first few years of the Twentieth Century in China learning the language and had gone straight from there to South Africa in charge of Chinese coolies in the mines. About 1912 he had been posted to the intelligence branch (MO3) of the General Staff in Simla. Simla was the summer capital of India in the foothills of the Himalayas to which the Viceroy, Commander in Chief, and Governor of the Punjab repaired, with their staffs, from the plains in the summer months. There Colonel Jeffery took up the study of Chinese ciphers. To the best of my knowledge, he reported only to the Indian Government and up till 1921 had not been personally in contact with GC&CS or any other cryptanalytic group. He had been very successful in reconstructing some Chinese ciphers consisting of very large one and two-part codes. After World War I he had begun working on Russian ciphers. He had been promoted to Brevet-Colonel and the General Staff had ruled that he could not retain his rank unless he returned to his regiment for duty. This was a prospect he could not face and he contemplated retirement as soon as a suitable replacement could be found for him. At first it was suggested that Captain A. G. S. Muntz (at that time working as a cryptanalyst in Baghdad in Iraq—of Muntz more later) should replace him and that I should go as assistant military attaché to Meshed in Persia (for which post Muntz was intended, as some forward exploitation of Russian intercepts was contemplated there). As a result of my success

with DELEGAT I was selected to relieve Colonel Jeffery, and it was decided to drop the Meshed project and leave Muntz in Baghdad.

After a month working as a cipher clerk in the War Office (which gave me experience for which I was later extremely grateful) I departed for India in September 1921. While I was on the high seas, the Indian General Staff relented and decided to allow Colonel Jeffery to remain in Simla and retain his rank, but on the condition that he took a year's leave of absence away from India, leaving me in charge. This arrangement he eyed with deep misgivings, and we didn't part on the best of terms at the end of the year.

I remained eight and a half years in Simla, staying there in the winter when most of the General Staff moved down to Delhi. The Section (MO3G) consisted usually of Colonel Jeffery, myself, one army officer Russian interpreter, one clerk and one officer interpreter in Eastern languages, chiefly Persian. Our main (almost our sole) Russian task was the exploitation of diplomatic messages passing between Moscow and Kabul in Afghanistan and between Moscow and Tashkent in Turkestan. We had two radio intercept stations (civilian manned), one at Cherat in the hills above Peshawar on the Northwest frontier and one at Pishin in Baluchistan. Later we had a station at Maymyo in Burma for a time.

When I first arrived, the Russians were using dinomic syllabaries reciphered by repeated cyclic use of 5-digit additives (a different one, as far as I remember, for each message). This was pretty easy stuff for Colonel Jeffery after his work on Chinese, even although he refused absolutely to learn any Russian. Shortly after my arrival, a new cipher with the discriminant name AZIYA was introduced. This was slightly more troublesome, as one of about seventy 20-digit additives was employed for each message, first reading from left to right, then from right to left, then left to right and so on. This was my first success in Simla.

Colonel Jeffery departed on leave for England in December 1921, and I was left in charge. But just before he left, the Russians had introduced an entirely new type of cipher system. Again I have to make up an example. They used a dinome syllabary for the basic substitution and what we called a conversion table, providing random dinome equivalents for each of the dinomes 00 thru 99. The intermediate text was reciphered by use of the conversion table off the dinome cut, leaving certain digits unaltered. This system was introduced in three stages. In the first system, called KONSUL, dinomes from the conversion table were substituted for the bc and de dinomes of the 5-figure groups of the intermediate text, leaving the first digit of groups unaltered. This produced the strange result that conversion was off the

dinome cut in groups of odd position, but on it in groups of even position. Therefore, the 4th and 5th dinomes of each set of 10 digits retained the frequencies of the original syllabary. Table G shows the effect of reciphering a common cliché such as AFGANPRA (abbreviation for Afghan Government) on the 5 possible "cuts." I reconstructed the KONSUL syllabary from the portions of messages which retained the dinome cut and read the messages without fully understanding what happened in the case of the other three-fifths of the text. By this time I was in touch with Muntz in Baghdad and had the mortification of being told the explanation by him. I should perhaps say here that neither Colonel Jeffery nor I had any general cryptanalytic training nor any knowledge of statistics. Our experience was limited to the very few types of systems which we had handled, and there were no satisfactory technical books to which to refer. Fetterlein had taught me a little but only in the field of transposition—it used to be said in GC&CS in 1920-1921 that I was the only person Fetterlein had ever been known to help.

The same idea in another form appeared a little later in the cipher "ALTAI." Here the intermediate text derived from a dinome syllabary was arranged in 6-figure groups and the bc and de dinomes reciphered by use of a conversion table. Table H shows the effect of applying the rules of ALTAI to the elements of Table G. Sometime in the spring of 1922 I prophesied that the next change would be to continuous dinome conversions "off the cut" leaving only the first digit and the last digit of a message unchanged. I felt extremely gratified when very shortly afterwards this exact change took place, but at first could make no headway. This was partly due to the fact that the messages of different days of the month appeared not to repeat into one another. Muntz produced an elaborate theoretical analysis and method of solution based on the observation that *repetitions in the intermediate* text would be mostly represented in the cipher text by repetitions two digits shorter. It should therefore be possible to group together (a) dinomes of the cipher text representing dinomes beginning with the same digit and (b) dinomes representing those ending with the same digit, and thus produce a provisional table which would work as well as the true one. But we both found in practice that this process produced only confusion, with every dinome equal to every other. So I took off to see Muntz in Baghdad, carrying my problem with me. After about three weeks, I solved the traffic of one day by reading probable words (such as AFGANPRA) into the repetitions in the cipher text and reconstructing the syllabary and conversion table bit by bit. It turned out that there were six different syllabaries and six different conversion tables, and these were used in various random combinations for the various days of the month.

Captain Muntz was an artillery captain, younger than myself, with a fine brain and an enormous capacity for work. He was a good linguist with a knowledge of Russian (entirely self-taught) of about the same standard as mine. (I had just scraped through the Army language examination in 1920 as a second class interpreter; I later passed first class but the standard was quite low as we couldn't go to Russia to learn.) We suffered a great loss when Muntz died aged about 40. He spent a year or two at GC&CS in 1923–1924 working in other linguistic fields and was consequently not with us when Colonel Jeffery and I were held up in our solution of Russian ciphers. When I left India at the end of 1929 to start the Military Section of GC&CS, Muntz took over from me in Simla and remained there till he died.

Sometime in 1923 the Russians introduced long additives for the first time and, in the absence of obviously significant repetitions in the cipher text and owing to our failure through lack of general experience to recognize concealed indicators, we did not succeed in diagnosing the new type of cipher for several months. From 1923 to 1928 a succession of additive series, all of the same general form, were introduced, applied to a number of code-books widely differing in dimensions and form. Starting point indicators were concealed, I believe, by addition of textual groups in prearranged positions and placed in positions varying with the system. The additives were all 1000 5-figure groups long arranged in 100 lines of 10 groups each and were applied "bou strophedon," i.e., reading first line left to right, then the next right to left, etc. The starting point for a message was chosen by the operator and could be at any of the 1000 groups of the additive. The construction of the additives was frequently far from random, exhibiting various personal idiosyncrasies, but was not often predictable and had to be solved figure by figure. During the lifetime of an additive, sufficient depth was usually provided for solution of a considerable portion of the traffic. In the late summer and fall of 1924, I recovered a great part of the additive and the code book of the first of these systems. The code book contained 2000 groups from 0000 to 1999 and was completely alphabetic (i.e., one-part). In about November 1924 I went back to England for a month, visiting on the way Baghdad and our War Office intercept station at Sarafand in Palestine. It appeared that in London Fetterlein had in fact solved an additive system similar to ours and some time earlier than we realized what we had but the solution had not been reported to us in India.

Between the time when I returned to Simla and the summer of 1928, we recovered vast amounts of additive and 4 or 5 more code books. I remember particularly one which contained (a) a 3000 group 1-part code, 4-figure groups beginning with 0, 1 and 2, (b) 400 random trinomes representing the commonest words beginning with 3, 4, 5 and 6 and

(c) a dinomic alphabet, the dinomes 70 thru 99 representing the letters of the Russian alphabet in alphabetic order. Another code which did not retain a constant "cut" contained 9000 4-figure groups beginning 0 thru 8 and 10,000 5-figure groups beginning 9.

In the fall of 1925 the Government of India sent a column (known as the WANA column) to the northwest frontier to occupy Waziristan to deal with unrest among the northwest tribes, a more stormy situation than usual. Stark, the Russian Ambassador in Afghanistan, sent a cipher telegram to Moscow in which he inquired what joint action was proposed between the Russian and Afghan Governments "in view of the occupation of Waziristan (W Widu Okkupacii Waziristana)." Our interpreter, who was quadrilingual in Russian, English, French and German, but not outstandingly literate in any one of them, translated this—"with a view to the occupation of Waziristan." The intelligence branch of Army Headquarters was in Delhi, and we were in Simla, and there was a day of near crisis in Delhi before someone, realizing that it would take something like six months for Russians and Afghans to join forces over the Hindu Kush, queried the translation back to us. I well remember Colonel Jeffery saying: "In future all startling statements of this nature will be viewed with the utmost suspicion." The outcome was that I was told to check all our interpreter's translations before they went out. My knowledge of Russian was very inferior to his but my standards of accuracy were a lot higher and the new order meant a great deal of extra work for me. At this time I was in fact involved in all aspects of the work, diagnosing the ciphers, recovering the additives, reconstructing the code books, performing the rudimentary traffic analysis tasks necessary, visiting one of the intercept stations at Cherat and directing the intercept coverage, translating or checking translations and frequently having to argue the meaning of messages with the general staff. On two of my three visits to Baghdad, I also worked in the Baghdad intercept station in the set room. All this gave me breadth of experience which comparatively few other cryptanalysts have had the opportunity of acquiring. Also, at this time I had to provide a practical field cipher for the Indian Army. This and its weakness are described in *NSA Technical Journal* (Vol. XI, No. 3, Summer 1966, paras. 4 and 19). In November 1925 I retired from the British Regular Army to become a War Office civil servant, the first of two classified as "Signal Computers." It was arranged that I should stay on in Simla. In 1927 I took eight months leave in England during which I worked for three months at GC&CS (then in a house in Queen's Gate).

In 1928 the Russians for the first time introduced one time pads but we were not able to do very much with them. There were two sizes:

(a) 11 lines of five 5-figure groups, i.e., 275 figures, used with messages of not more than 550 figures of intermediate text and (b) 11 lines of ten 5-figure groups, i.e., 550 figures for longer messages, but any message exceeding 1100 had to be divided into parts. The operator was permitted to use a pad twice and no more.—The pads were used "boustrophedon" and therefore there were depths of two but reading in opposite directions as the additives were arranged in an odd number of lines. We were hardly able to read anything at all except in the case of one or two very stereotyped proforma messages.

One anecdote I must tell in reference to our earlier more successful days: In 1926 there were two Russian cipher clerks in Kabul, named Kotlov and Serafimowich. The latter was the less reliable of the two and when suffering from frequent morning hangovers made so many mistakes in encipherment that eventually an order came from Moscow that in future all cipher messages must be signed in cipher by the clerk responsible. From this time on, messages were signed either Zachifrowan Kotlov or Zachifrowan Serafimowich, which presented us each time with 40 or 50 additive figures. But the day came when Serafimowich himself deciphered a message ordering him to return to Moscow, as his papers were not in order. He fled at once for sanctuary to the British Embassy but was ejected, and I regret to say was never heard of again.

In 1929 the War Office decided it needed a military section in GC&CS and I was chosen to start it. There had been a naval section there ever since the end of World War I, the residue of 40 OB. I left India at the end of 1929, having been with Colonel Jeffery for eight and one-half years during which I had learned how to parry his sharp wit or divert it on to others, and we had become firm friends. At the beginning of March 1930 I joined GC&CS again, this time as head of the newly formed military section, but on the War Office payroll. Captain F.A. Jacob (afterwards Colonel Jacob who later succeeded me as SUKLO Washington in 1954) retired from the Army and joined me as deputy. He had in 1925 won a prize in the first of two cryptanalytic competitions open to army officers in India which I had instituted and prepared under the auspices of the Intelligence Branch of the General Staff in India. I was also allotted an establishment of four posts to be held for three years by regular army officers (normally with language qualifications) seconded for training in military cryptanalysis. Except in the case of Italian, which I left entirely to Jacob, there was at the time virtually no military intercept to work on, and I set myself the objective of getting as much cryptanalytic training and experience as possible for myself and my officers by collecting cipher systems that others couldn't or wouldn't deal with. This policy was criticized more than once by my paymaster in the War Office, but there was really no

alternative if we wanted to gain experience in cryptanalysis, and particularly cryptanalytic diagnosis. The decision to use army officers to form a reserve in case of war was not an unqualified success. Only one of the first batch, Pritchard, was with me through World War II. Another of them was recalled against my wishes during the Abyssinian War at a critical stage in his career, and he suffered professionally as a result.

The Government Code and Cipher School had by now moved to Broadway Buildings, part of which it occupied in conjunction with M16 until we moved to Bletchley Park in 1939. A.G. Denniston was still Director. Ernst Fetterlein was still in my opinion far the best general-purpose cryptanalyst. Oliver Strachey held the title of Chief Cryptographer, which he retained until I took it over in 1942. He had been in the War Office Cork Street department during World War I and had a considerable reputation for successes both during the war and since its end.† J.E.S. Cooper, who joined together with four or five other young men in 1925, became the first head at the Air Section in 1936. There were also 10 or 11 survivors from World War I, most of them normally engaged in the reconstruction of code books.

Much of my activities in London from 1930 until the outbreak of war in September 1939 has already appeared in the *NSA Technical Journal*. The story of our solution of the various Comintern ciphers 1931 through 1934 appeared in the *Technical Journal*, Vol. VIII, No. 4, Fall 1963 in an article "The Development of the Additive," of which it forms the first part.

My connection with Japanese ciphers and the Japanese language was described in some detail in the *Journal*, Vol. XI, No. 3, Summer 1966, pages 4–9. I took no part in the British solution of the Japanese Red machine. The direct part in this was taken by Hugh Foss, who joined us about 1932. Foss also performed the first analysis in the British office of the German commercial Enigma machine.

†He was the brother of Lytton Strachey, the famous biographer.

TABLE A

A 05 12 25 37 50 90 97	P 19 38 48 77 87
B 42 69	C 15 34 54 81 95
Б 17 51 66 78	Т 08 16 57 75 83
Г 04 58 79	У 14 26 33 64 67 86
Д 11 52 68	Ф 00
Е 18 20 32 46 65 72 91	Х 24 61
Ж 06	Ц 19
З 27 80 85	Ч 30 59
И 13 17 36 56 76 94 98	Ш 03 74
Й 92 99	Щ 62
К 29 41 70	Ь 09 71
Л 02 40 43	Ы 45 73
М 21 47 53	Ю 22
Н 28 31 49 88 96	Я 35 63
О 07 18 22 44 60 82 93	. 01 84
П 10 39 55 89	, 23

TABLE B

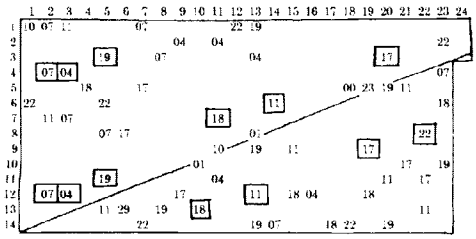

TABLE C

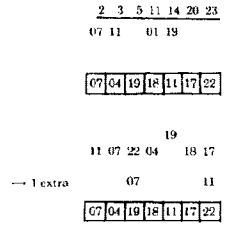

TABLE D

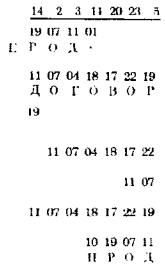

TABLE E

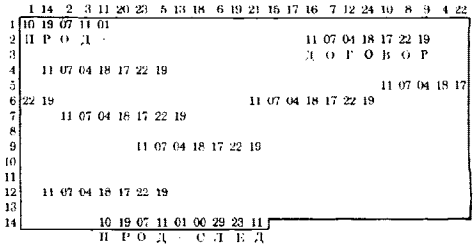

TABLE F

1	14	2	3	11	20	23	5	13	18	6	19	21	15	17	16	7	12	24	10	8	9	4	22
1		2	3																			4	
							5			6						7				8	9		
																			10				
				11													12						
								13															
14													15		16								
														17									
									18		19												
					20							21											22
						23												24					

A N D D I S T E M P E R S N O N E I T F E E D S

TABLE G

EXTRACT FROM CONVERSION TABLE

07	08	10	15	24	31	48	50	63	72	81
82	25	61	05	50	27	83	19	22	40	91

A	F	GA	N	P	RA
63	15	07	24	81	08

6	2	7	1	9	7	5	0	9	1	0												
	3	0	5	8	2	2	8	3	6	1	8											
2	2	1	1	9	4	0	4	9	1	2	5											
	2	7	5	9	2	5	0	8	8	1												
2	2	0	5	0	4	0	8	3	1	2	5											

TABLE H

6	2	7	1	9	7	2	8	3	6	1	8											
	3	0	5	8	2	2	4	9	1	2	5											
	3	1	1	9	4	0	4	8	6	1												
2	2	1	5	8	2	5	0	8	1	2	5											
	2	7	5	0	4	0	8	3	1	0												
2	2	0	5	0	7	5	0	9	1	0	8											

Non - Responsive