Telegrams on Negotiations on Capturing Petrograd, 1919

Samu Potka
Finnish Defense Research Agency
PO BOX 10, FI-11311 Riihimäki
samu.potka@mil.fi

Mikko Kiviharju
Finnish Defense Research Agency
PO BOX 10, FI-11311 Riihimäki
mikko.kiviharju@mil.fi

Abstract

We decipher a 1919 telegram encrypted with an irregular columnar transposition cipher. The telegram details negotiations between Finnish activists and the Russian anti-Bolshevik White Movement regarding capturing Petrograd.

1 Historical Background

In the "October Revolution" in 1917, Bolsheviks seized the power in Russia. The (former) Grand Duchy of Finland was then able to negotiate full sovereignty, becoming an independent state. However, the revolution resulted in a civil war in Russia lasting to 1923. There was some uncertainty if it would end in the victory of the anti-Bolshevist factions, led by Admiral Kolchak and General Yudenich, for example, and supported by the Entente, and whether they would still be in support of the Finnish independence.

In 1919, with the focus of the Russian Civil War shifting north, the temporary Regent of Finland, Baron Mannerheim, along with a group of right-wing activists, was in favor of Finland militarily assisting the Russian White Army of anti-Bolsheviks in capturing Petrograd (St. Petersburg) (Volanen, 2019). Mannerheim was negotiating the terms of this involvement with the leaders General Marushevsky and General Miller of the "Northern Army", the northern branch of the White Army, based in Arkhangelsk. Telegrams, for example, reveal that the terms presented by Mannerheim included acknowledging Finland's independence, ceding a port in the Pechenga Gulf together with land for a railway, and "to refer at future date to special conference the question of self-determination of certain Karelian districts whose population has leanings towards Finland".

Meanwhile, however, Mannerheim was also supposed to sign Finland's new democratic system of government, removing him the power of deciding on such an operation, and as enough political support never materialized, nothing ever came out of these negotiations — the large majority was clearly opposed to the idea (Volanen, 2019). It did not help that the Supreme Ruler of the White Movement in Russia, Admiral Kolchak, refused to recognize Finland's independence, at least de jure (Pipes, 1993), despite the leaders of the "Northern Army" as well as General Yudenich supporting it.

2 Telegrams

Details of the plans and expectations of the Finnish military high command in general are preserved in the military correspondence of that time in the form of telegrams. The received (but undeciphered) telegrams can still be found in the Finnish national archives. However, their interpretation has so far been tedious manual work case-by-case. To our knowledge, a systematic effort to decrypt these types of telegrams has not yet emerged.

During a history research project on early Finland, some of the telegrams from 1919 were rediscovered, and a request to try to decipher them was put forward.

The authors were provided with two encrypted telegrams, stored in the National Archives of Finland. These were part of the aforementioned negotiations and sent from General Miller to Mannerheim, the first on July 22 and the second on July 26, 1919. See Figures 1 and 2. A note, signed July 28, 1919, accompanied the second telegram, describing its decryption, see Figure 3. There was no such note for the first. The decryption note reveals that an irregular columnar transposition cipher was used for the second telegram.

2.1 Columnar Transposition

Transposition ciphers simply change the order of the letters in a plaintext. According to Kahn (1996), columnar transposition appeared as

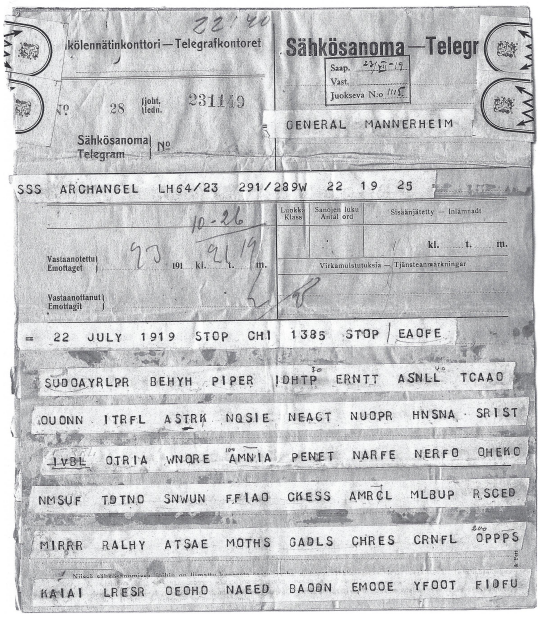

Figure 1: The first page of the first telegram, dated July 22, 1919.

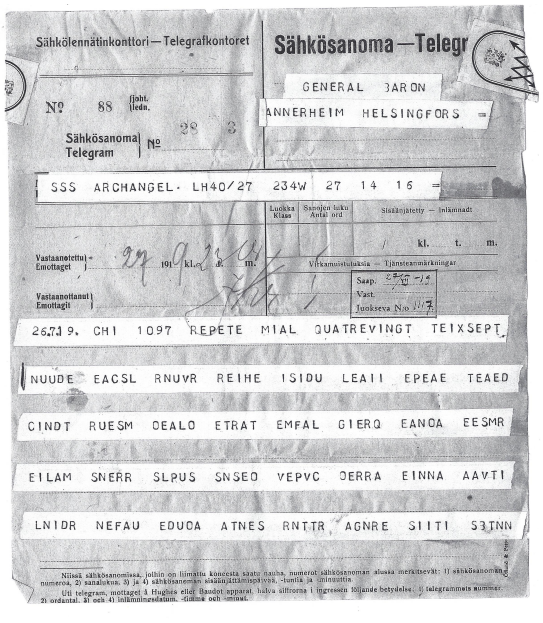

Figure 2: The first page of the second telegram, dated July 26, 1919.

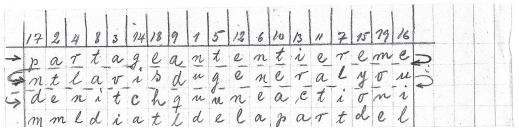

Figure 3: Part of the first page of a note, signed July 28, 1919, detailing decrypting the second telegram. An irregular columnar transposition cipher was used.

early as 1685. It has been widely used: Kahn mentions "French military ciphers, Japanese diplomatic superencipherments, and Soviet spy ciphers", Bauer (2021) mentions Britain's Special Operations Executive (SOE) agents in occupied Europe and German operatives in Latin America until the spring of 1941, and Mahon and Gillogly (2008) discuss the 1920s' Irish Republican Army (IRA). Germany, for example, used double columnar transposition, where columnar transposition is repeated twice, in the beginning of World War I and as part of the ADFGX and ADFGVX ciphers at the end of it (Kahn, 1996). In between, they used various ciphers, including columnar transposition combined with substitutions.

In columnar transposition, the plaintext is divided into rows of width specified by the key length. The cipher is called "regular" if the last row is completed, with random letters, for example, if it is shorter than the other rows, and "irregular" otherwise. The key is either a permutation or a keyword or phrase, and the alphabetical order of the letters specifies a permutation. This permutation determines the order in which the columns are read off, top to bottom.

As an example, consider the irregular columnar transposition cipher in Table 1. Reading the columns in the order specified by the key ("WORDS"), we have the ciphertext "ADTANTTCAAKW". For deciphering, the process is repeated backwards.

5 (W)	**2** (O)	**3** (R)	**1** (D)	**4** (S)
A	T	T	A	C
K	A	T	D	A
W	N			

Table 1: Example of an irregular columnar transposition cipher.

2.2 The Method of Lasry et al.

The history of cryptanalysis of columnar transposition ciphers goes back to at least the beginning of World War I, when the French could already regularly break the variations of columnar transposition the Germans used (Kahn, 1996). In World War II, Germany, for example, had machinery for automatically solving single columnar transposition, Kahn mentions. The machines were based on computing bigram frequencies in prospective

pairs of consecutive columns.

In the 1990s, modern computerized approaches based on optimization techniques, such as genetic algorithms, simulated annealing, hill climbing and tabu search, started appearing. More on this can be found in (Lasry et al., 2016), which introduced the most recent method for cryptanalyzing columnar transposition ciphers, improving on previous algorithms, allowing shorter ciphertexts and long keys. Their method is based on hill climbing, which

1. starts from a random candidate key,
2. iteratively scores certain permutations of the current candidate by decrypting with them and scoring the corresponding plaintexts,
3. and once a better candidate is found, replaces the current candidate and goes back to 2. If improvement was not possible, either stop or start again from a new random candidate.

The score function used in this part of the algorithm is the sum of the log-frequencies (in the selected language) of the quadgrams found in the plaintext. The permutations considered are called segment swaps and segment slides, the former swapping non-overlapping segments of the same length in the key and the latter sliding around key segments. The point is to be able to preserve the adjacency of most key elements while changing the positions of a large number of them.

They further improve the algorithm for long keys by adding a phase to find a better initial candidate key. The phase is more complicated in the irregular case but turns out to be especially useful there. The general difference compared to the regular case is that in addition to finding the correct order of columns, figuring out which columns are one letter longer than the rest is also needed. See (Lasry et al., 2016) for the full details. Here the key is quite short, so we may also skip this phase.

2.3 Deciphering the First Telegram

The complete ciphertext is provided in Figure 4.

Some somewhat manual cryptanalysis using "cribs" (or known or guessed plaintexts) and bigrams had been tried first. Letter frequencies seemed to correspond to English as is, indicating that substitution was not used — only transposition. This, along with the second telegram, suggested considering irregular columnar transposition. However, then the need to determine the correct column lengths complicates any analysis. Additionally, some cribs included Russian family names which may be transliterated in a variety of ways into English and the Latin alphabet.

EAOFE SUDOA YRLPR BEHUH PIPER IDHTP ERNTT ASNLL TCAAO OUONN ITRFL ASTRK NQSIE NEACT NUOPR HNSNA SRIST ..... OTRIA WNQRE AMNIA PENET NARFE NERFO OHEKO NMSUF TDTNO SNWUN FFIAO CKESS AMRCL MLBUP RSCED MIRRR RALHY ATSAE MOTHS GADLS CHRES CRNFL OPPPS KAIAI LRESR OEOHO NAEED BAODN EMOOE YFOOT FIDFU DCEIN DSNIG IDNSF NPCRI RSERA SIENR CHTEL VPONT GTTST NEUUC NIEGU TOFNL OVLLT SENTS ANMSL ONVER HARAE MIOPI NOOTT TTNHA DETOO EAIRA ITOIO OURIC AESET ITMAL SEDOE TRCHI ANEMM IEIOA NOETC DFEAC LNCSL AECEN LOSWA OQHAO DWIHA YTNBD NPAMT AHIVU DRIIP EHDNO ITFHA LORSH FTHOF NRRON RSANE TSILF EUIEP GNTFN RPRNR CSKNS EEEOY TYDTM YBEUY ULUSR APHFE YESOM TRLET THINR AMAES ALAFT EIERE EIHIA TOORI ESANO YSSAE NDRES GLONO ETEGR OTTEE DDDIO FENTU RSIYE ..... AAOOD INYYS TLIIN DWLWO SDORR ENMAS TTTDA TEROP BSRTY ODOWO SWEMN CUBOR TLFRG ESANT SMECM OENOI IEDAN FTTSL DNITO NIYIN IIAII IITEP NIKRW IONGP NRMLR EFPPF CFLCA STESS GGIOO IOEDT IDEEA NEPOM RENAO EOEOP AEEIR ASHHH IMPTT ALVNO EVREL TRLAN SVESP DOARP HIARO TINSR EFTET HFTYE EEIWE NOUYE STFAN FAHDN NQEQA RLFIH SOEDL HTIVR EMKIN CDNMY AYNPR TRSHE SODSK ACHAW NRISA IPTHN LUAYP DHACP MOEAA AANSK OOSED PTRNT HEDEE IRIDC ..... RHEEA DURPN ITMIP WRDRD ELRCA NNIIN OANTT ANWTT TLSST LSHSR DUDED DIDPO GAATN RNETO OSATL RTASH ECSRW DTNUD ETUFF FTOSN NYOSS ALEIS TEUIS CNPRE LOIEI HPAET INEII ENODY RAIYO EOFHL COSAN EDPND RTPDL TCDAS LADFC HISNE ODSTN OONDO DUEOM IINNS AARAS PRRER NCOTE SNGNF MHMTE STRMF NNEER ADAAT TAUOI DLENF EUILO PIPUL NBRCH RLFTN HNCEM GEOTD DWLSM FRCON AWFOW DOSFP SNLWS EGLTT FCOOD AAEIW TIRTI HUMRU HRIIN SYVPW ENNNO ..... TOYTI UAACE FFTUO HEVUI THSIE OEOOG NBPTN OOSID ILNTI UTGUS SNDQL ISOPU

Figure 4: The ciphertext in the first telegram, see Figure 1. The dots indicate groups of characters over or underlined in the telegram. These are shorter or longer than the (standard) groups of five and have therefore been replaced with five unknown characters each.

To decipher, we implemented the algorithm of Lasry et al. in a SageMath (Python) notebook (Sage, 2021), in roughly 100 lines of code (without any specific attempts to make it more concise). Note that the (different) hill climbing algorithm in CrypTool 2 (`https://www.cryptool.org/en/ct2/`) could also be used but we opted for our own implementation for flexibility in this case, a priori, and potential future use.

To use the algorithm, the language of the plaintext as well as the key length need to be guessed (the alternative is to go through all possible key lengths until the correct key is found). The second telegram has a French header and the recovered plaintext in the decryption note is French. The header of the first telegram is English, hinting that English should be the first language to try. The non-normalized index of coincidence of the first telegram is approximately 0.0645, rather close to

the 0.0661 computed from the English letter frequencies in (Norvig, 2013). The decryption note in Figure 3 also reveals that the key length used for the second telegram was 19, so this is likely a good starting point.

Using the bigram and quadgram counts from (Norvig, 2013) and (Lyons, 2009), respectively, the algorithm returns the key 5 2 4 11 7 6 13 17 9 18 1 19 15 3 8 14 10 16 12 or EBDKGFMQIRASOCHNJPL. This results in the text in Figure 5. Note that if an actual keyword or phrase existed, it remains unknown. Finding the key took around 15 minutes on a basic business laptop with an Intel i5-6300U CPU and 16 GB RAM, without any serious optimization attempts. Two reasons it is rather slow are Python and that in the worst case it may need to score a large number of permutations of a key before finding an improvement, if at all.

Upon Marushevskys return I telegraphed Koltchak as follows STOP [M]annerheim offers mobilise within ten days seven divisions numbering about one hundred thousand men [a]nd o[c]cupy Petrograd Seco[n]dly to avoid pillage a[n]d murder F[i]nnish army [w]ill not enter Petrogr[a]d but will [i]mmediatel[y] push on to [V]olhov STOP To preserv[e] order Petrograd will [b]e entered by a spe[c]ial[l]y form[e]d detach[]ment of picked White Finns STOP Thirdl[y] under cover of Finnish army Iudenitch accompanied by staff and officers corps will enter Petro[g]rad and commence form[a]tion [o]f army STO[P] Fort[h]ly a[s] Russian units ar[e] for[m]ed they graduall[y] replace Finns who the[n] go home STOP Fifthly the Finnish army operates having on the we[s]t the alread[y] form[e]d Ru[s]sian corps in Est[]oni[a] and to the north e[a]st the Russian [f]orces [o]f the M[u]rman regio[n] ST[O]P As compensation for assistance rendered Mannerheim demands as follows STOP First acknowledg[e]ment of Finlands total independence [S]econd a port in Petchenga Gulf with necessary land strip for railway to be ceded to Finland STOP Thirdly to refer at future date to special conference the [q]uestion of selfdetermination of certain Karelian districts whose popu[l]ation has leanings towards Finland meanwhile Finland does not and will not in future follow any po[l]icy of conquest STOP On the other hand it is pro[m]ised to pay for Russian state propert[y] taken in Finland during last year over whi[c]h que[s][]tion a special [R]ussian and Fin[n]ish commission is at w[o]rk apparently without any misunderstandings STOP The question of the neutralisation of the Baltic is relinquished and its consideration aban[d]oned STO[P] I on my part supported acceptance your help.

Figure 5: The plaintext obtained from the ciphertext in Figure 4 with the key 5 2 4 11 7 6 13 17 9 18 1 19 15 3 8 14 10 16 12. Incorrect letters fixed by the authors are indicated with square brackets.

The text contained about 50 errors in roughly 1400 characters. Some of these may be Morse code errors, but we believe most of them originated elsewhere: our impression is that the typical error rate of a proficient operator was not that high, and the operator has marked 18 errors and corrected some, but many of the legible corrections turn out wrong in the plaintext. The end of a sentence is (as customary) marked with "STOP", and could be a useful crib in other telegrams.

The plaintext reveals that the telegram informed Mannerheim of Miller telegraphing Kolchak Mannerheim's group's offer and demands in exchange for Finnish help in the capture of Petrograd. The same text can also be found in (Heninen, 2013), likely translated from Russian. Thus the decipherment has not revealed any new relevant historical information. However, it does lend itself to providing the text more authenticity and traceability to formal archives.

The implementation could also be used to decipher other enciphered military telegrams of that time more systematically and with good generality (considering especially the aforementioned cases of longer keys and shorter ciphertexts).

References

Craig P. Bauer. 2021. *Secret History: The Story of Cryptology*, 2nd edition. Chapman and Hall/CRC.

Andrew Heninen. 2013. *Telegram to General Mannerheim*. `http://heninen.net/miekka/1919_e.htm`.

David Kahn. 1996. *The Codebreakers*, 2nd edition. Scribner.

George Lasry, Nils Kopal and Arno Wacker. 2016. Cryptanalysis of columnar transposition cipher with long keys. *Cryptologia*, 40(4):374–398.

James Lyons. 2009. *Practical Cryptography*. `practicalcryptography.com`.

Tom Mahon and James J. Gillogly. 2008. *Decoding the IRA*. Mercier Press, Cork, Ireland.

Peter Norvig. 2013. *English Letter Frequency Counts: Mayzner Revisited or ETAOIN SRHLDCU*. `https://norvig.com/mayzner.html`.

Richard Pipes. 1993. *Russia Under the Bolshevik Regime*. Alfred A. Knopf, New York.

The Sage Developers. 2021. *SageMath, the Sage Mathematics Software System (Version 9.2)*. `https://www.sagemath.org`.

Risto Volanen. 2019. *Nuori Suomi sodan ja rauhan Euroopassa*. Otava.