

Cryptographic postcards

Tobias Schrödel

IT Security & Awareness

Munich, Germany

tobias@schroedel.email

Abstract

This document is about postcards written in code or cipher, which is a field in historic cryptography with only few information available. While military and business related cryptography is examined in depth, these cards give insight in the civil use of pen & paper ciphers. The author has scanned and evaluated his private collection of more than 400 encrypted postcards. Although statistics and data are not representative, this paper allows a first classification and should encourage other collectors to contribute data as well.

1 Introduction

According to a base of more than 400 encrypted postcards, private correspondence in code was mainly performed in the early 20th century. Nevertheless, encrypted postcards of the 19th century are rare but also exist. While historical cryptographic books, letters, and documents have been evaluated and inventoried since decades, this has not been the case for encrypted postcards. About these, the reader can only find minimal information.

2 Finding encrypted postcards

Historic postcards can be found in different places. But besides special fairs, flea markets, and online auctions, there is no typical marketplace for historic postcards. Especially not for encrypted postcards.

2.1 Sources

Bookstores selling antiquarian books sometimes offer historical postcards as well. The author notes that private stamp collectors quite often also collect postcards. They sometimes offer them on flea markets. Finding encrypted postcards in packs of hundreds of cards is like searching the needle in a haystack. The author

notes, that most of the (private) collectors are of higher age and are not aware what an encrypted postcard is. Their reason for collecting is either the stamp or the motive of the postcard (city, area, military, or cards with applications). Therefore, many postcards written in code or cipher may rest unnoticed in such big packs of cards. Some collectors have mentioned that the interest of younger people in ancient postcards is minimal and that the cards have no high value in general. It is, therefore, possible, that the cards will be disposed once the collector dies.

Professional stamp and postcard dealers can be found on the Internet.¹ They offer thousands of catalogued cards often including a search function. The author unregularly performs checks on search terms like “Geheimschrift” (German for “secret writing”), “written in code”, or “cipher”. The hit rate over the last approximately ten years was minimal (below 5 pieces). According to akpool, a German vendor with over 1 million cards and a sales quantity of 400.000 cards per year, they have no interest in marking cryptographic cards, as this is not asked for by buyers.

A very promising place for finding encrypted postcards is eBay. The reason why this platform is popular for the sale of cryptographic postcards is unclear. It is possible, that once a layman identifies a postcard written in cipher, due to “strange” symbols, it is acknowledged as something special and put up for sale (maybe in expectation of a high price). This assumption is

1 <https://www.ansichtskarten-center.de>

<https://www.delcampe.net>

<https://www.akpool.de>

hardened due to the many false-positives on eBay. Private sellers very often sell postcards written in shorthand as “a very rare card written in code”. However, shorthand was very common in the early decades of the past century and is no cipher or code.

2.2 Prices

The prices for encrypted postcards vary from 1€ to 250€ and sometimes even more. These cards are collector items and as such the price depends extremely on the number of collectors, interested in it. For a regular and “common” encrypted card, the author normally payed up to a maximum of 30€. For special cards with beautiful symbols or cards belonging to an existing series, the author is willing to pay more.

Average prices for encrypted postcards have increased massively in the past three to five years. Even unattractive cards nowadays regularly achieve prices of over 50€. The reason for the increase is unknown and may be a sign of more collectors. Proper statistics on payed prices for the cards described in this paper are not available.

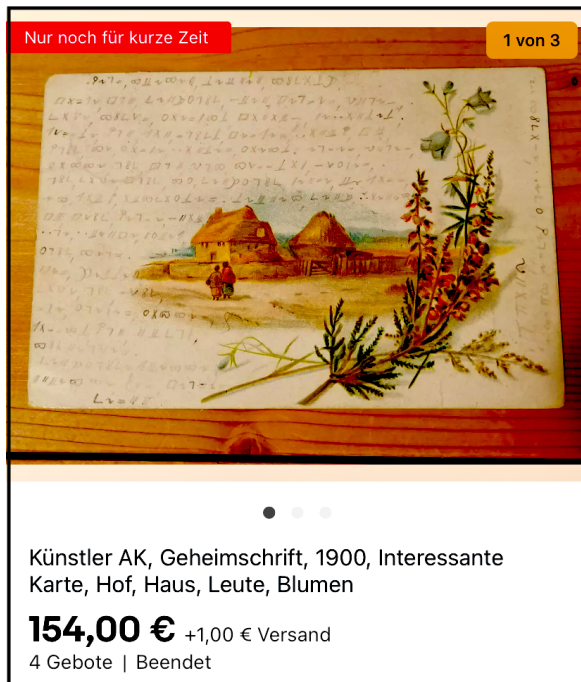


Figure 1: An encrypted postcard from 1900 sold on eBay Germany for 154€ (June 20th, 2021). There were four bidders. At least two were willing to pay more than 150€ for this postcard.

2.3 Other resources

The author knows only of one other collector (in Thuringia) specialized in encrypted postcards.

Another source for encrypted postcards is Klaus Schmeß's blog “Cipherbrain” aka “Klausis Krypto Kolumne” where more than one hundred postcards have been described over the past years.²

3 The collection

The following paragraph will provide numbers and statistics about the evaluated card collection. Although the collection has no focus and spans over all periods and locations, the numbers are not representative. The author has mainly searched and bought cards in Germany and mainly from German websites and sellers. In addition, not all cards ever on sale are in the evaluation, as there are other collectors, and the author has lost several eBay auctions to other people.

3.1 Quantity

The author's collection contains 428 encrypted postcards. This includes 38 cards most probably written in shorthand, which will be left out or marked in the statistics. Shorthand is no encryption method. But there are many abbreviations in shorthand that are often personalized and therefore difficult for others to identify. So a few cards cannot clearly be identified as code or shorthand by the author. Some of these cards also combine shorthand with number codes. Anyway, there is a certain uncertainty in the numbers.

3.2 Period of time

The date of an encrypted postcard can be evaluated in two different ways. Sometimes, there is a written date on the card. However, it is more accurate to read the postmark on a devalued stamp.

Sometimes a handwritten date differs from the postmark date. This happens when the card has been sent days after writing. For the following statistics, the author used whatever date was the

2 <https://scienceblogs.de/klausis-krypto-kolumne/>

most clearly readable one. If none was readable, they do not appear in the following table.

Written dates: Handwritten dates appear in cleartext just like on unencrypted postcards. The author knows of no postcard, where the date was also part of the encryption. (This applies only to cards, that are already deciphered).

Postmark dates: Some postcards are postmarked twice. The first punch was made, when the card was delivered to the sender's post office and a second time, when it arrived at the recipient's post office.

Period	Count
1880-1889	6
1890-1899	21
1900-1909	148
1910-1919	161
1920-1929	4
1930-1939	1
1940-1949	3
1950-1959	0
1960-1969	2

Table 1: Overview by decade

The date of the postmarks on the cards do not follow a standard format. Therefore, some dates cannot be identified with certainty, especially when only two digits and not four represent the year. For example, 01-03-14 can be read either as 14th of March 1901 but also as 1st of March 1914. As philatelist catalogues (and websites) state in which period a specific stamp was in use, the stamp (if present) can help to clarify or at least to narrow the date of the card.

The number of encrypted cards during WW1 and WW2 is lower than in the preceding years. The author assumes, that this is (at least partially) a consequence of the ban of the use of codes during the war in many countries. However, for the period of WW1 the collection contains seven encrypted cards (shipped within Germany) and a large set (same sender and recipient) of 140 cards

shipped within Hungary. For the period of WW2 there are only two encrypted cards available in the collection (plus one in shorthand). It is not known, why these two cards (1940 within Nazi Germany and 1942 within France) were not removed by censorship.

The above table clearly indicates a significantly higher number of encrypted postcards in the time between 1900 and 1920. This may correlate to the availability of books about simple cryptography for the public (and not military nor government). These books were mostly addressed to lovers, who wanted to correspond secretly. Many are listed on the cryptobooks-website, and some are available on Google-books.³ The method(s) described in these books are normally easy-to-use pen & paper ciphers, mainly monoalphabetic substitutions (simple MASC). Although the authors of these books claim "absolute security" for the messages, a MASC was no problem for an experienced cryptanalyst at that time. However, the method probably fulfilled its task to hide the message on a postcard against curious family members and the postman.



Figure 2: Books aimed to lovers about encrypting private correspondence. Left: Geheimschrift für Liebende (Erwin Le Mang, 1923). Right: Sicherster Schutz des Briefgeheimnisses (Emil Katz, 1901).

3.3 Sender & Recipient

The following paragraph gives an overview of the origin and destination of all evaluated encrypted postcards.

Some cards can be assigned to be part of a set. A set is defined as postcards from one sender to the same recipient. They normally used the identical cipher over time. In the examined collection of 428 postcards, 347 cards are part of 24 sets. While two large sets of 45 and 120 pieces are outstanding, the average number of cards in a set is 6.6.

Sender: The country and city of the sender can only be obtained, when the punched stamp on the card is readable, as it shows the name of the city (post office). If the recipient's address does not contain a country name, it is assumed, that the card was shipped within one country, as only international cards require the destination country to be named. Sometimes, the originating city can be derived from the card itself. E.g., when the printed picture on the card states "Greetings from ...". However, this is an assumption.

The author found some ambiguities, especially from cards around the time of WW2. There were cases, where cards were sent within Germany with German stamps. However, the origin and/or destination city is today in Poland. In the following table, these cards are counted for the country of the time, they were sent.

Recipient: The recipients address is mostly easy to find out. It has to be written on the card, if the card was shipped. Anyhow, a small number of cards has not been shipped. It is mostly unclear, whether they were dropped personally, sent in an envelope, or just used as a note.

Country	From	To
HU Hungary	171	171
DE Germany	159	165
US United States	27	25
UK United Kingdom	17	17
AT Austria	12	9
FR France	6	7
BE Belgium	4	3

CH Switzerland	2	5
CZ Czech Republic	1	1

Table 2: Country of origin and destination

165 of the Hungarian cards are part of only two sets while all other countries represent a variety of senders and recipients including smaller sets.

3.4 Stamps

Collectors removed the stamps on some cards. In most cases, this led to unreadable parts or missing postmarks made by the post office. In these cases, it was much harder to find out the shipping date as well as the origin city – if even possible.

However, many stamps remain on the cards, and it is obvious, that they were quite often not placed straight in the right corner of the postcards. Some of the stamps were put on in a 45° angle or even upside down. The author wants to note, that the alignment of the stamps was often used for a short note, such as "I miss you", "Write back soon" or "Forever yours". The interested reader can find different instructions and meanings for the stamp placement using Google or other Internet search engines with the keywords "language of stamps".



Figure 3: A postcard explaining the "language of stamps". Date unknown, according to the shown stamps probably around 1935

4 The Ciphers

The used cipher type is only known for sure, when the postcard has been decrypted or if the used cryptographic method is obvious (e.g.

pigpen). In most cases, a simple monoalphabetic substitution cipher (simple MASC) was used.

4.1 Cipher type

This table shows, what kind of encryption method is used on the cards – if known or obvious.

Cipher type	Count
Simple MASC	71
(Shorthand)	38
Pigpen	20
Morse code	8
Anamorph writing	2
Square writing	2
Mirror writing	1
Wigwag	1
Caesar shift	1

Table 3: Cipher types

4.2 Used symbols and characters

In most cases, numerical substitutions are used. However, some cards use symbols or standard Latin characters. The following table shows substitution with symbols as the leading type. The reason is that two sets from Hungary contain 165 cards with symbols. To get a more meaningful statistic, the reader might want to subtract them.

Special encryption methods such as square writing (writing horizontal and vertical) or hidden messages (under stamp) are not counted.

Symbols used	Count
Symbols	199
Numbers	132
Characters	3

Table 4: Used symbols for the cipher text

4.3 Plaintext

For 76 cards, the plaintext is known. The length of these messages ranges from 27 to 1.955 characters. The average length of these messages is 297 characters.

Length of message	Count
1-99	24
100-199	17
200-299	11
300-399	9
400-499	3
500-599	5
600-999	2
> 1.000	5

Table 5: Message length

4.4 Language

The language of the encrypted message is a very interesting and an important part regarding cryptography. However, there were no surprises. For the evaluated collection of postcards, the language of the known plaintext matches the language spoken in the sender's and/or recipient's country. All evaluated cards within Germany as well as from Germany to German speaking countries (like Austria) were written in German language. Cards within Hungary were written in Hungarian language, cards within Czech Republic were written in Czech. A card from Paris (France) to San Francisco (USA) was written in French. Only one card differs. It was sent from Finland to Russia in 1906 and is written in German language.

5 Conclusion

This collection of cards soon is subject to a more detailed analysis within the DECRYPT⁴ project. Therefore, all postcards were scanned (both sides) and uploaded to the DECODE⁵ database. Other collectors are invited to do so as well.

A complete publication of the scans is planned shortly to allow students and any other interested people to participate in the exciting world of "postcard cryptology".

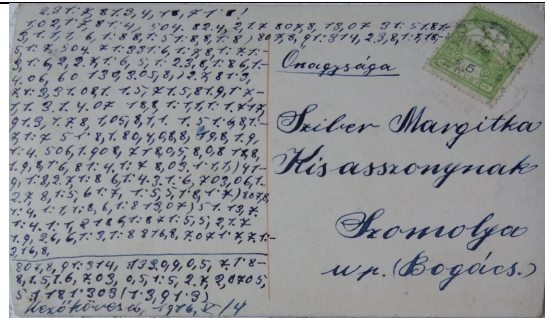
⁴ <https://www.de-crypt.org/>

⁵ <https://de-crypt.org/decrypt-web/>

6 Addendum



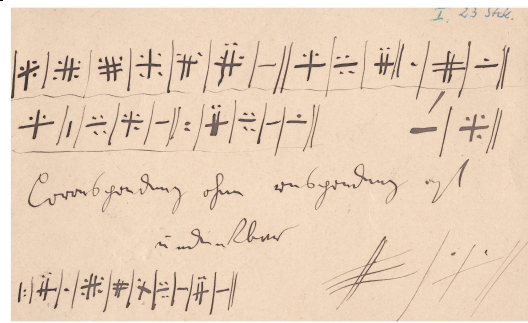
Card with a MASC from a set of twelve cards in German language



A numerical code and a stamp in 45° angle dated May 4th, 1916



Mix of a numerical code with shorthand from 1898



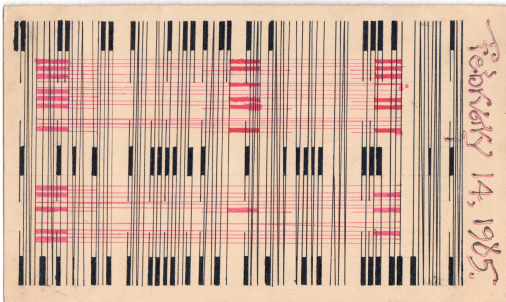
Postcard to a Bavarian princess from her brother (1890)



The daughter of an Earl has a message for the shoemaker's son. She wants to meet him on Sunday and hopes for good weather (1902)



MASC using numbers



Postcard with anamorph writing and Valentine's day greetings



Beautiful, encrypted card from July 1907