Transposition Ciphers in Historical Context

William Ricker

Agenda

1. Crypto News Review
2. History: Transposition Ciphers in Historic Context
3. How To Reminder for GPG/PGP Key-signing
4. GPG/PGP Key-signing

Crypto News review: from 2014-09

- 2014-fall
  - SHELLSHOCK wasn't crypto
  - POODLE - “Padding Oracle on Downgraded Legacy Encryption” - Yet another side-jack exploit – HTTPS in Starbucks not safe if SSLv3 downgrade allowed !
  - SSLsplit - tool for MITM intercept
  - "Let's Encrypt" announced for 2015
  - Whatsapp adds E2E
- 2015
  - FREAK (downgrading session to export ciphers)
  - RowHammer (DRAM abuse)
  - TrueCrypt Audit
  - LogJam “ Imperfect Forward Secrecy” (per Sggrc) – export-grade TLS
  -
-
- 2016
  - CacheBleed: A Timing Attack on OpenSSL Constant Time RSA
  - Drown – riffing SSLv2 to compromise TLS (turn off old ciphers!)
  - BadLock – overblown!
  - CA follies continue
    - many more named exploits, mostly over-sold
  - CVE-2016-6313 Random Number prediction
    - 4640 bits from the RNG needed **yawn**
  - The Million-Key Question—Investigating the Origins of RSA Public Keys
  - weaponizing of Rowhammer with “Flip Feng Shui,”

2. Transposition Ciphers in Historic Context

- Using Codes and Ciphers !

Cryptographic Taxonomy

- Steganography
- Codes
- Ciphers
- Composite

Taxonomy: Steganography

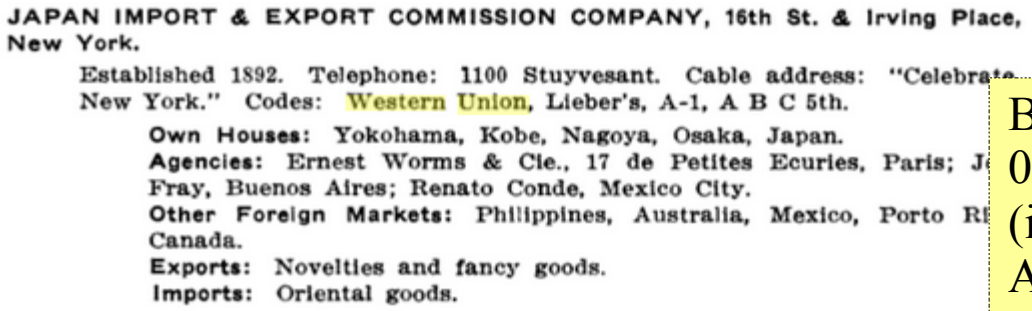
- message, what message ?
- e.g, Acme::Bleach or lemon juice
- Example, “Attack at Dawn” becomes:

Taxonomy: Codes

- Semantic level substitution
  - One Part vs Two Part
  - Complete or partial
- Nomenclator – one-part, partial
  - “Attack At Dawn”
    to “GrapeJelly At Dawn”
- Commercial Codebooks – one-part.

  Mostly for brevity;
  - registration required.

- Trench Codes
- Military & Diplomatic Codebooks
  - Normally two part (plus additive)
  - Washington Naval Conference of 1922
  - Gray
  - Midway (JN-25b)
  - “GrapeJelly Textbook”



JAPAN IMPORT & EXPORT COMMISSION COMPANY, 16th St. & Irving Place, New York.

Established 1892. Telephone: 1100 Stuyvesant. Cable address: "Celebrate New York." Codes: Western Union, Lieber's, A-1, A B C 5th.

Own Houses: Yokohama, Kobe, Nagoya, Osaka, Japan.
Agencies: Ernest Worms & Cie., 17 de Petites Ecuries, Paris; J... Fray, Buenos Aires; Renato Conde, Mexico City.
Other Foreign Markets: Philippines, Australia, Mexico, Porto Ri... Canada.
Exports: Novelties and fancy goods.
Imports: Oriental goods.

BOHORDER PESTANEABA
04206 114976
(inserted ATTACK in 1st custom space after Attach; used **5am Thursday** for DAWN)

Taxonomy: Ciphers

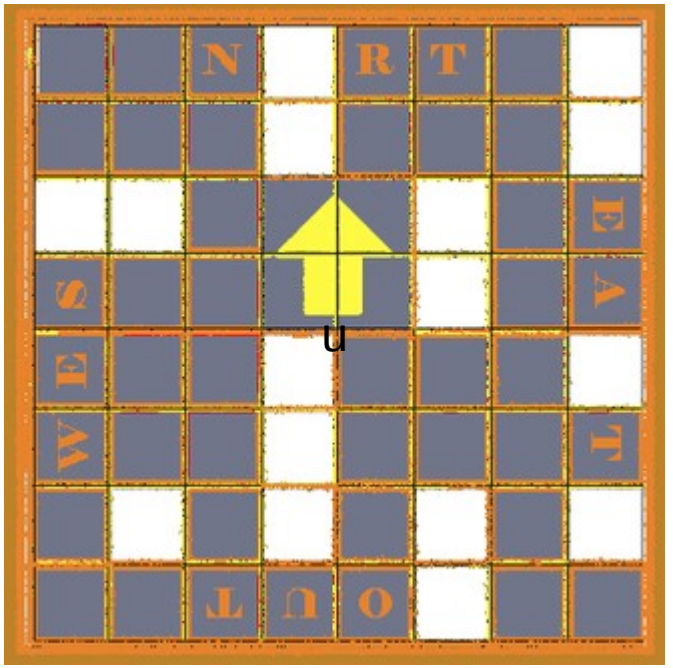
- Orthographic level
- Substitution –
  - from Caesar, ROT13 to Enigma to Vernam to Solitaire
  - (Hebrew Atbaš was before Caesar.)
  - Digital stream ciphers
- Transposition
  - Rearrange the deckchairs
- Hybrid
  - Digital Block ciphers Feistel rounds of S&P(DES, AES)
  - Tunny (Baudot TTY bits toggled and swapped);

All of the above

- Diplomatic (or commercial) codebooks with Additives and/or Transposition super-encipherment
- Substitution Cipher with Jargon phrasebook to avoid probable words
- KGB/VIC ciphers: straddle or Vigenère, proper-noun inclusions, hidden OTP, double transposition with voids, microdot or secret ink, hollow-nickel.

Transposition Ciphers

- Scytale (Wikipedia image)
- Grilles (primitive)
- Rail fence (combines with bifid substitution naturally)
- Columnar
- Double
- Variations
  - Disrupted (Voids)
  - Myszkowski (POTATO, TOMATO)
  - Unpadded / Ragged



Transposition -

- Disadvantages
  - limited key-space
  - Shape choices of key are tied to size of message trivially
  - Error prone by hand
    - And the More-secure variations are more error prone (and may be *complication illusoire*)
  - Frequency analysis matches input
    - Discloses transposition in use
    - And/or discloses input language or prior substitution's frequencey
- Advantages
  - Cryptanalysis requires either probable word or 'depth' on a key
    - Simplest substitution does not; yields to entropy
  - But 'the' may be enough of a probable word

Historic Example 1. USMTC (Y-150)

- Smithsonian/Zooniverse/ Huntington Library Citizen-science initiative to transcribe Lincoln's war telegrams “Decoding the Civil War”
  - http://www.smithsonianmag.com/smart-news/you-can-help-decode-thousands-top-secret-civil-war-telegrams-180959561/
  - https://www.zooniverse.org/projects/zooniverse/decoding-the-civil-war
  - https://www.zooniverse.org/projects/zooniverse/decoding-the-civil-war/about/education
  - https://blog.decodingthecivilwar.org/
  - https://web.archive.org/web/20160628222057/http://www.c3teachers.org/wp-content/uploads/2016/01/Anatomy-of-a-Cipher.pdf
  - *Really looking for transcribers*
  - See also William Rattle Plum, The Military Telegraph during the Civil War in the United States v1 & v2
    - https://archive.org/search.php?query=Plum%2C%20William%20Rattle

Lincoln's War Dept Code

- Nomenclator code
  - With multiple replacements
  - Single-part
  - Does not include small /common words
    - But recommends punning homophony
      - Anna Police = Anapolis (will fractionate)
      - Tooth = To The, Toby = to be (won't help anagramming)
- Superencrypted by Transposition
  - Route encryption by words
    - Words are easier in manual telegraphy
    - Columnar variant with reversed columns (typically alternately but 2^N choices)
    - Prefix of 3 blind (commencement) words to indicate the columns & Route and lines.
    - Suffix of a blind word after each column as a buffer, ?indicating which it was?

U.S. MILITARY TELEGRAPH.
Apr 12 1865
By Telegraph from War Dept

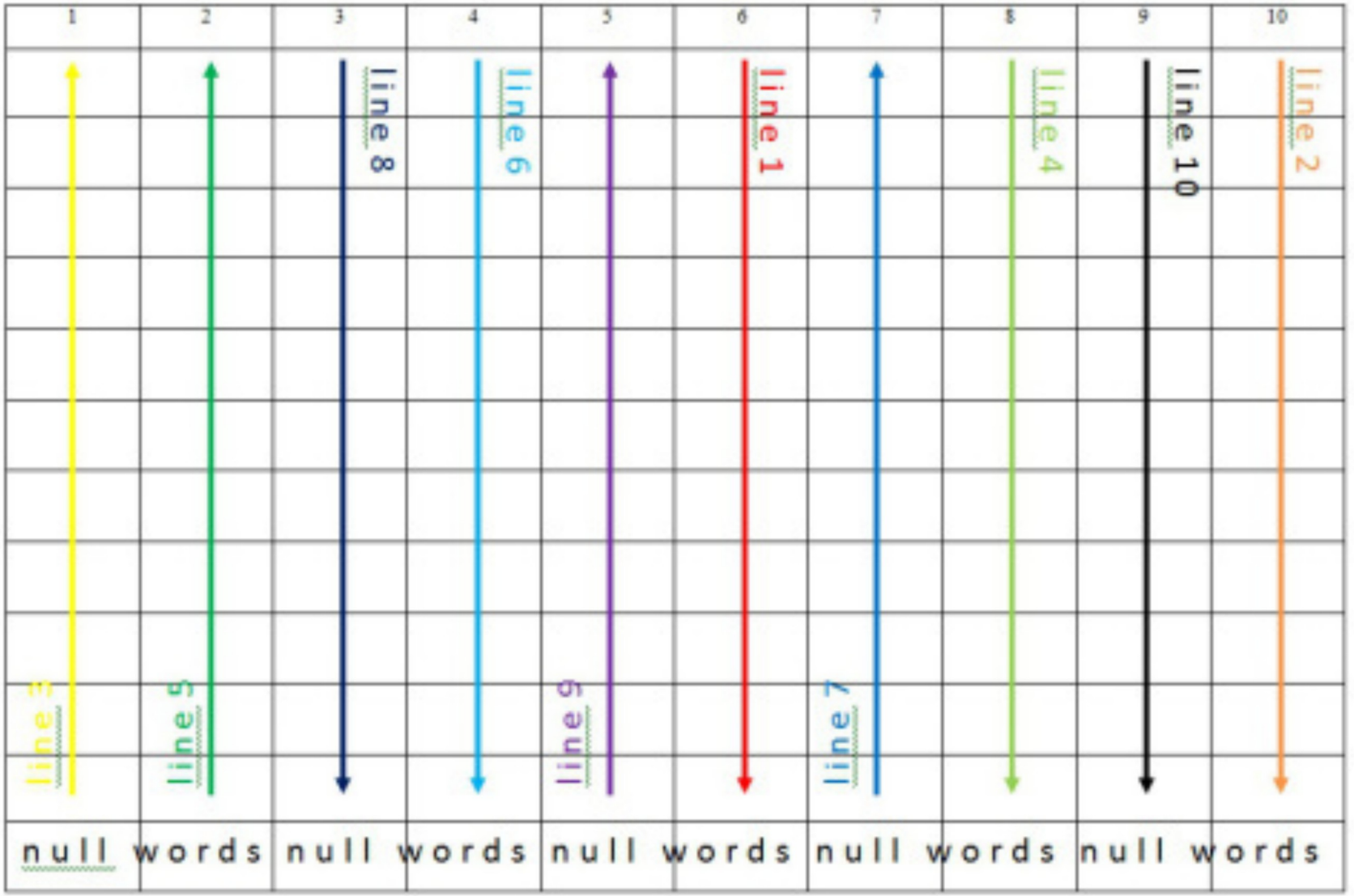
To J. H. Emerick
Whats next news I the prayers I to while coming star what you you mean dispatch zebra I you spirit there understanding any if the piloted your offer there such of any and have was I to Emma never seen of of no toby Zodiac on there is with what remains yoke as sign my sign temper acted in to paradise flood over weitzel abe remember pekin that my walnut to form such why not say may it if together there you have spoken matter have senses shelter bardie not galway in manifested torch letter in no bologne plenty dont sign me you legislature me appeared but bearing out unity in your prayers while doubt the is the is pedlar draw you down
T. T. Eckert
123

- From “Anatomy of a Cipher” Daniel W. Stowell
  https://web.archive.org/web/20160628222057/http://www.c3teachers.org/wp-content/uploads/2016/01/Anatomy-of-a-Cipher.pdf

Decryption

- Note check 123 is 2 less than body count 125. It's the original's count ! !
- To Emerick, From Eckert – those are the Operators. Routing to operator with inner addressee.
- “**Whats next news** I the prayers I to”
  - Blinds. In current code,
    - “Whats” is 10 columns and below Route (negative = up)
    - Next:2 + News:9 = 11 Lines
    - `  ROUTE:  6  10  -1  8  -2  4  -7  3  -5  9`
    - `  count:  1  2  3  4  5  6  7  8  9  10`
    - `unROUTE:  3  5  8  6  9  1  7  4  10  2`

Sample Route WHATS



Decryption... break to columns

```
C  6( 1):I  the  prayers  I  to  while  coming  star  what  you  you  mean
C 10( 2):dispatch  zebra  I  you  spirit  there  understanding  any  if  the  piloted  your
C -1( 3):offer  there  such  of  any  and  have  was  I  to  Emma  never
C  8( 4):seen  of  of  no  toby  Zodiac  on  there  is  with  what  remains
C -2( 5):yoke  as  sign  my  sign  temper  acted  in  to  paradise  flood  over
C  4( 6):weitzel  abe  remember  pekin  that  my  walnut  to  form  such  why  not
C -7( 7):say  may  it  if  together  there  you  have  spoken  matter  have  senses
C  3( 8):shelter  bardie  not  galway  in  manifested  torch  letter  in  no  bologne  plenty
C -5( 9):dont  sign  me  you  legislature  me  appeared  but  bearing  out  unity  in
C  9(10):your  prayers  while  doubt  the  is  the  is  pedlar  draw  you  down
```

- This is output of a Perl program,
  - using Perl 5.24 features that were experimentally introduced in 5.20
  - Come to Boston Perl Mongers to see it !

Decryption: column check blinds

```
C  6( 1):I  the  prayers  I  to  while  coming  star  what  you  you
C 10( 2):dispatch  zebra  I  you  spirit  there  understanding  any  if  the  piloted
C -1( 3):offer  there  such  of  any  and  have  was  I  to  Emma
C  8( 4):seen  of  of  no  toby  Zodiac  on  there  is  with  what
C -2( 5):yoke  as  sign  my  sign  temper  acted  in  to  paradise  flood
C  4( 6):weitzel  abe  remember  pekin  that  my  walnut  to  form  such  why
C -7( 7):say  may  it  if  together  there  you  have  spoken  matter  have
C  3( 8):shelter  bardie  not  galway  in  manifested  torch  letter  in  no  bologne
C -5( 9):dont  sign  me  you  legislature  me  appeared  but  bearing  out  unity
C  9(10):your  prayers  while  doubt  the  is  the  is  pedlar  draw  you

col checks MEAN YOUR NEVER REMAINS OVER NOT SENSES PLENTY IN DOWN
```

Decryption... unreverse

```
C  6( 1):I  the  prayers  I  to  while  coming  star  what  you  you
C 10( 2):dispatch  zebra  I  you  spirit  there  understanding  any  if  the  piloted
C 10( 2):dispatch  zebra  I  you  spirit  there  understanding  any  if  the  piloted
C  1( 3):Emma  to  I  was  have  and  any  of  such  there  offer
C  8( 4):seen  of  of  no  toby  Zodiac  on  there  is  with  what
C  2( 5):flood  paradise  to  in  acted  temper  sign  my  sign  as  yoke
C  4( 6):weitzel  abe  remember  pekin  that  my  walnut  to  form  such  why
C  7( 7):have  matter  spoken  have  you  there  together  if  it  may  say
C  3( 8):shelter  bardie  not  galway  in  manifested  torch  letter  in  no  bologne
C  5( 9):unity  out  bearing  but  appeared  me  legislature  you  me  sign  dont
C  9(10):your  prayers  while  doubt  the  is  the  is  pedlar  draw  you
```

Decryption... unscramble to lines

L (1):Emma flood shelter weitzel unity I have seen your dispatch
L (2):to paradise bardie abe out the matter of prayers zebra
L (3):I to not remember bearing prayers spoken of while I
L (4):was in galway pekin but I have no doubt you
L (5):have acted in that appeared to you toby the spirit
L (6):and temper manifested my me while there Zodiac is there
L (7):any sign torch walnut legislature coming together on the understanding
L (8):of my letter to you star if there is any
L (9):such sign in form me what it is pedlar if
L (10):there as no such sign you may with draw the
L (11):offer yoke bologne why dont you say what you piloted

Decryption... Decode Arbitraries

L (1):/9am/ /12/ /Genl./ weitzel /./ I have seen your dispatch
L (2):to /Col./ bardie abe out the matter of prayers /./
L (3):I to not remember bearing prayers spoken of while I
L (4):was in /Richmond/ /,/ but I have no doubt you
L (5):have acted in that appeared to you /to be/ the spirit
L (6):and temper manifested my me while there /./ is there
L (7):any sign /of the/ /Rebel/ legislature coming together on the understanding
L (8):of my letter to you /?/ if there is any
L (9):such sign in form me what it is /,/ if
L (10):there as no such sign you may with draw the
L (11):offer /signed/ /Pres of U.S./
/why dont you say what you piloted/

Long-hand typos:
to for *do*, *bearing* for *hearing*, *that* for *what*, *my* for *by*

Cryptanalysis

- Blog says never broken by Confederates.
  - Likely true.
  - Says more of Rebels than of system!
    - Rebels happily used simple polyalphabetic Vigenère with single key for most of war for their General officer cipher (See previous Vicksburg talk.)
    - Rebels likely didn't have crypto-intel staff to crack this
      - both sides broke wig-wag simple substitiutions of the other.
        - NSA Spectrum, The Gray Fox Swallowed the Bait
        - https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/gray_fox.pdf
      - Union did much better, no reports seen of Rebels doing so
- Breakable but difficult.
  - Depth needed – thus volume of intercepts
    - In theory, If this historic trove contained many encrypted telegrams matching one missing code book edition, it could be derived
      - but that seems unnecessary given content of the archive
  - Nomenclator & Codebook Codes broken before and after,
    - In theory, could've been broken
    - if intercepts and staff available

Depth needed

- To break either a transposition or a code-book requires lots of intercepted material.
- Nomenclator codes were broken in Renaisance by “Dark Chambers”
  - that copied all mail in/out of capital, including “sealed” diplomatic pouches,
  - so it was possible to reconstruct single-part code book by pencil and paper.
- Pre-radio: tapping telegraph lines was common by Cavalry
  - but only get messages on **that** circuit,
  - not everything as one gets with radio telegraphy in WW1

Aids in breaking

- Kerckhoffs' principle: only the keys are secret;
  - "the enemy knows the system" (Shannon's version).
  - Assume we know, or guess from observing multiple messages, that route transposition of codebook words, with blind indicators added.
  - We don't know the routes; nor the blind indicators; nor the Nomenclator book of Arbitraries.
- Transposition
  - Blind route indicators would make sorting messages into depths easier, as 1st Blind is number of columns. Many homophones, 9 per Route.
    - (Did they have more than one Route for a given width during a key period? If not, Fail!)
    - One-part alphabetic will suggest homophones !
  - Typically small number of factors of body size for columns x lines.
    - Blind route indicators will tattle that # columns is sometimes the same as another message of different length, removing all doubt as to which factors are which.
  - Blind column indicators serve as error correction for proper recipient but likewise will aid a cryptanalyst with a depth to do multiple anagramming once they've been intuited
- Codebook
  - Nomenclator means don't have to break the little words in each version of code first, they're given free (like word-breaks in newspaper CryptoQuotes™). Oops.
  - Single-part code-book's parallel ordering of sensitive and cover words helps infer meaning !
  - Military Intelligence has much context to provide probable words from Order of Battle and Operational Awareness.
    - E.g., if we knew addressee SHELTER Weitzel refers to a (Maj)Genl, could infer SHELTER is either /MajGenl/ or /Genl/ from context.
  - Unknown Codewords can be obvious from context once known ones filled in.
    - /Richmond/ … WALNUT Legislature
    - Which Legislature might General in Richmond be talking to? Not likely State of Maine …
    - Recently declassified, how Nazi Germany broke a US Code https://www.nsa.gov/news-features/declassified-documents/tech-journals/
- Blinds acting as nulls in last line are operator chat !

Historic Examle 2. ADFGVX (Y-100)

- Well, Y-98.
  - WW1 centenary is well underway (1914-1918)
    - Centenaries of Battles of the Somme (1916 Jul01 to Nov18) and Verdun (1916 Feb21 – Dec18) extends before I write this to after I present. *Ouch*!
  - but this cipher is March to July 1918 * .
- German near-front Army/Corps/Division cipher, Western Front.
  - Trying to break out of trenches into decisive movement before attrition; Tanks & Gas.

ADFG(v)x

- Polybius Substitution
  - Fractionated Bifid Substitution
  - Thoroughly mixed alphabet
  - Labels ADFG(V)X
    - Optimized for Morse Code Wireless Telegraphy speed & accuracy

      ·- --· ···· --· ···· -···
  - Expanded from 5x5 to 6x6 to include numerals in June
    - Avoids spelling
      - numerals become probable words!
        - eins zwei drei vier fünf sechs sieben acht neun zehn
      - or shifts to digits modes in other systems.
    - Shorter messages. less mistakes.
  - (Image from Wikipedia)
- Single Columnar Transposition
  - Ragged last row hence ragged columns
- Irregular splitting / blocking of long messages
  - To avoid multiple anagramming

	A	D	F	G	V	X
A	N	A	1	C	3	H
D	8	T	B	2	O	M
F	E	5	W	R	P	D
G	4	F	6	G	7	I
V	9	J	0	K	L	Q
X	S	U	V	X	Y	Z

Cryptanalysis of ADFGX

Mostly one Analyst: Lt Georges Painvan

(picture via Wikipedia)

- Irregular message sizes:
  - Ragged row prevents factoring for size
  - But eventually actually harmed security
- Frequency analysis says little at start
  - Only 5 (later 6) letters discloses it's a Bifid
  - Freq distribution varied day to day disclosed that Polybius is keyed daily
    - And thus likely the transposition key too

Cryptanalysis … Depth

- Transposition requires Depth to break
  - Regular blocks in one message can provide that, but avoided here
- Required depth of messages needed in same day key and similar or same size to crack
  - Initially too few messages
  - Flurry of messages prior to attack!
  - Only 10 days broken, but 50% of all traffic

Cryptanalysis … Entry

- Find Column width, lengths
  - Stereotyped military message prologue results in common pattern even after transposition
    - similar to “cribs”, but only need the pattern not the text !
      - (the text crib will help later)
  - Divide columns into long and short using prologue pattern
    - limits anagramming choices to subsets
    - Undoes the complication of where to break the columns
- Two messages with same length: Multiple Anagramming
- Different but close: Pattern similarity discloses width and length.

Cryptanalysis – matching columns

- Frequency analysis
  - Dividing columns into even/odd.
    - (Also can detect Even vs Odd number of columns if not determined otherwise)
  - Candidate pair [odd:even] columns as Polybius bifid letters
    - Bifid means only 36 not 26*26 kinds in each pairing so easier to have enough data to be meaningful

Cryptanalysis … finishing

- Once anagrammed, bifid coordinate pairs can be treated as simple mono-alphabetic substitution; routine.
  - Re-use the crib to start.
- Having recovered transposition (# columns and permutation) and substitution (mixed alphabet) keys of the day, all messages of the day are readable.
  - SIGINT Metadata will likely indicate priority of which to read first.
- General solution in between-war (de)classified text http://www.nsa.gov/public_info/declass/military_cryptanalysis.shtml later; only special case depth solutions during war.

Critique

- At a post-wars history conference, cryptanalyst Maj.(then Lt.)Painvin and cryptographer Col.(then Lt.)Nebel met.
  - Double Transposition would have been too hard to get right in transmission, but would have blocked timely breaks if used properly.
  - Using it wrong would have transmitted errors more useful to breaker than recipient and many retransmissions, likewise !
- Illusory Complications
  - Same chars in row & column labels – but can tell 'Ax' from 'xA'
  - Lack of 'Russian copulation' (nor free re-wording) to hide stereotyped beginning flagged width and column size in common patterns
  - Varying column lengths leaked by stereotype leaking patterns through transpostion
  - Sorting into long / short columns reduced anagramming
  - Fractionated letters actually makes frequency testing candidate column pairs more useful

3. GPG/PGP Key Signing

- A quick HOW TO