Part V
Grid-based ciphers

Unit 69
Polybius cipher

If we cram the alphabet into a 5×5 matrix, we have a *Polybius square*. Unfortunately, the English alphabet has more than 5^2 letters, so we may have to jettison one of them. Usually, we will put ‘I’ and ‘J’ in the same spot.

Now, if we add labels to the rows and columns, we can use the Polybius square to make a cipher, which we will call the *Polybius cipher* or *Polybius-square cipher*.

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

The application of the cipher is obvious: we replace a letter of the plaintext with the row and column labels of its location in the grid. For example, with the matrix above, we can encipher this short message:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
33121332 21043232001104 410032 042202314324330403 41133312 00 11311303 021324120431
```

The ciphertext is

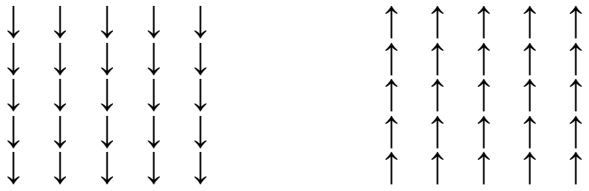
```
331213322104323200110441003204220231432433040341133312001131130302132412043l
```

We are not forced to use the digits 0, ..., 4 as our labels, and we are not constrained to use the same labels for rows as for columns. The only constraint is that all row labels must be different, and all column labels must be different.

The cipher can be keyed by using a mixed alphabet. In Unit 26 we saw several ways to construct mixed alphabets from keywords. With this new cipher, we add a new dimension. There are many ways to lay the mixed alphabet into the matrix. Here a just a few:

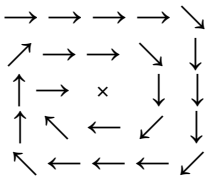
- by rows

- by columns



- boustrophedon (by rows or columns in alternating directions)

- spiral, outside-in or inside-out, clockwise or counterclockwise



At this point, you should realize that no matter how we mix the alphabet and no matter how we place the mixed alphabet into the grid, all we have done is replace each letter with a two-character string (a code word). By listing all two-character strings in the ciphertext and assigning a letter to each, we convert the Polybius cipher to a monoalphabetic substitution cipher. In Unit 28 we saw a method for solving monoalphabetic substitutions automatically.

Reading and references

Practical Cryptography, practicalcryptography.com/ciphers/polybius-square-cipher

Fred B. Wrixon, *Codes, Ciphers & Other Cryptic & Clandestine Communication*, New York: Black Dog & Leventhal, 1998, pages 190-191.

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, page 83.

Programming tasks

1. Write a function to fill a Polybius square. Allow for many options on how to generate the mixed alphabet and on how to fill the grid.

2. Write a function or script to encipher a plaintext with the Polybius cipher with a keyword, an alphabet-mixing method, and a grid-filling method.

3. Write a function or script to decipher a ciphertext with the Polybius cipher with a keyword, an alphabet-mixing method, and a grid-filling method.

4. Implement the attack mentioned above.

Exercises

1. Decipher this ciphertext with the keyword `POLYBIUS`. The mixed alphabet is constructed by adding letters that come alphabetically after the last letter of the keyword (in this case, start with 'T'). The grid is filled by columns. Labels are as in the example above.

```
24100231433231023221243121104332440302322101310010203040
40011121420100431344213244131332213031104244324204322020
20301011241313030121324201004313443113123131433231012120
20102433132410113343231044301011311040441332043143131400
10241032200043324013310142211402131013111310110244201000
431344
```

2. Break this ciphertext from the 2019 British National Cipher Challenge:

```
FBGAI AGCFE KEFEK CIAGC FCGAF CIBHD HEFCF AFBFA GDFCH
DFEKC IAKCI BGBGC IAHAF EKCFA KAIAG CFBFA GBFBI AFBHE
IAGCK CIAFC IBHDF EGAGA FCHDI AHEIA FCKDF CFAIA KCFBF
AIAGC FEHEF CICFB FEIAH EFDKA HBHDF CIEKA IDKCH DHEFB
HEKEF CFCHA FEKEK CHEHA KAGEF CKCIA GCFBF AGBFC GAIAG
CFEHE FCICF BFEIA FEHAH BFBHD FEIDK CHEHE IAFCG DFEKE
FDKAG CFBHE KEFEK CIAGC IAGCF EIBHE HEHDG AFEFE KEHEF
CFAIA GCFEK CFAGB FEHDI AGCKC IAIDF EHEIA FBHDI BHBID
FBIAG CFEKC KDGCI DKCHD IDFEG AFBGB GCIAF BFAFB IAHEH
BIBHB HBFEI AHEIA KCIAF EHEID FEGCK CICFE IAHDF BFEKE
IAFCK DFCFA IAKCF BFAFB IAFDI BIAFB FAFCI DHDFE KCGEF
BHEFE IAGCK CIAID FEKDK CFAFC FAGEK AKEFE GAFEK CIAFB
IAIAG CFEID KCKAI DFEGA FCIBG BGCIA GAKCH EKDFB HEHAF
DKAIA KCGDF BFAGB FCFAF BIAHE HAFBG BGCIA FBFAF CHBFE
FAIDK CHDFC IBHDH BFCGE FBIAF BKDFB KCFAH EGCKC ICFEH
EGCHD IBFAG DGAHD FCHAI AGCFE KDFCF AGAGE FBKDI AKCFA
KEIAG CFEKA FAFEF EKEKC HDFEK CHEFC FAIAF CKDFC FAGAH
DFCFA IAIAG CFEFE ICFBG E
```

Challenge

Unit 70
Playfair cipher

The *Playfair cipher* was not invented by Lord Playfair, but rather by Charles Wheatstone. At any rate, it is a *digram substitution cipher*, which means that it makes substitutions two letters at a time. It has little tolerance for double letters, so before we can apply the cipher, we have to prepare the plaintext by putting an ‘X’ between all adjacent pairs of identical letters. Since it works on pairs, we also need to add an ‘X’ to the end of the plaintext if it has an odd number of characters. (We do not need to put an ‘X’ between letters if they are in different digrams.)

The main engine of the Playfair cipher is a Polybius square. We fill it with a mixed alphabet that was generated in whatever way we like. Typically, ‘J’ is merged with ‘I,’ but some prefer to merge ‘Z’ in to ‘Y.’ The plaintext is processed two letters at a time, according to these rules:

- If the two letters appear in the same column of the Polybius square, then each is enciphered to the letter below it. If the letter is on the bottom row, then we use the letter at the top of the column.
- If the two letters appear in the same row of the square, then each is enciphered to the letter to its right. If the letter is in the last column, then we use the first letter in the row.
- If neither of the previous two cases hold, then a rectangle is observed in the grid such that the two letters are at two of its corners. They are enciphered to the letters in the other two corners. Each is enciphered to the letter in the other corner in the same row.

(Mathematicians in the audience recognize a torus when they see one.)

Now for an example. Here is our plaintext:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

First, we prepare it with nulls, one between the two ‘S’s and one at the end.

```
TH IS ME SX SA GE WA SE NC RY PT ED WI TH AG RI DC IP HE RX
```

Let’s use the keyword `POLYBIUS` to mix our alphabet, and let’s not do anything fancy about how we lay it into the square:

```
P  O  L  Y  B
I  U  S  A  C
D  E  F  G  H
K  M  N  Q  R
T  V  W  X  Z
```

The first two letters of the ciphertext, `TH`, are enciphered to `ZD`:

```
P  O  L  Y  B
I  U  S  A  C
D  E  F  G  H
K  M  N  Q  R
T  V  W  X  Z
```

The next two, `IS`, are enciphered to `UA`:

```
P  O  L  Y  B
I  U  S  A  C
D  E  F  G  H
K  M  N  Q  R
T  V  W  X  Z
```

This continues, and the ciphertext is

```
ZDUAVMAWACHFXSUFRSQBIPFETSZDGQKCHIDIDFQZ
```

To detect whether we have a ciphertext that has been encrypted with a grid-based digram substitution cipher, we look to see if there are at most 25 different letters and whether the length of the ciphertext is a multiple of two (to disguise the cipher, however, one might change some ‘I’s to ‘J’s, so be careful). If there are any long repeated sequences of characters, then the starting character of each needs to be an even number of letters apart. Furthermore, if we plot the index of coincidence as a function of period, as we did in Unit 31, we often see a slight increase in the even periods over the odd periods (do not take this to mean that the cipher is periodic, just that this is a differential tool).

Reading and references

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain; chapter XXI.

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/Playfair.pdf

Wikipedia, en.wikipedia.org/wiki/Playfair_cipher

Practical Cryptography, practicalcryptography.com/ciphers/playfair-cipher

United States Army, Field Manual 34-40-2, chapter 7, “Solution to Polygraphic Substitution Systems,” Basic Cryptanalysis, U.S. Department of Army, www.umich.edu/~umich/fm-34-40-2/ch7.pdf

Fred B. Wrixon, *Codes, Ciphers & Other Cryptic & Clandestine Communication*, New York: Black Dog & Leventhal, 1998, pages 217-219.

Fletcher Pratt, *Secret and Urgent: The Story of Codes and Ciphers*, New York: Bobbs-Merrill, 1939, chapter XII, section I.

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, pages 198-202.

Joseph O. Mauborgne, *An Advanced Problem in Cryptography and Its Solution*, Fort Leavenworth (Kansas): Press of the Army Service Schools, 1914, www.marshallfoundation.org/library/digital-archive/advanced-problem-cryptography-solution

W. W. Smith, "Solution of the Playfair Cipher," in part IV of André Langie, *Cryptography*, translated by James C. H. Macbeth, London: Constable & Company, 1922, HDL: 2027/uc1.32106002774104 and 2027/uc2.ark:/13960/t0tq62t29

Programming tasks

1. Write a function that returns a boolean value representing whether it is likely that a given ciphertext has been encrypted with a grid-based digram substitution cipher.
2. Implement an encryptor for the Playfair cipher.
3. Implement a decryptor for the Playfair cipher.
4. Implement a dictionary attack. Remember to allow for many possibilities for the method of mixing the alphabet from a keyword and for the method of laying the mixed alphabet into the square.

Exercises

1. Encipher this text with the keyword `TRENDING`. Fill the square with whatever method you like.

   > The point I advance, if it need confirmation,
   > I'll prove by a witness that few will dispute,
   > A pink of perfection and truth in the nation
   > Where fashion and folly are all of a suit.
   >
   > (from *Nothing to Eat* by Horatio Alger and Thomas Chandler Haliburton

2. Decipher this ciphertext with the keyword `GROCERIES`. The alphabet was mixed by starting at the beginning of the standard alphabet after the keyword. The mixed alphabet was laid in by rows from left to right.

```
MDSOASOGTGKCDRBZEQVSKYMHFVIBDSKYMHCOROCEGODGABUICQMROR
AOEAIHPEVFHPDMQCXCNDPUMRKBBPASZKGQPLABKENPNBVIQCASYQWB
GZGUAEKYKBSHIQBUFSCPVLEQOEGUPBBNEQRFQYQCKSZGDCGUQSSIDC
KGOGKRXZEQDKFVSAUCOCLNMRRCHWCMOBVFPDNBLVXCPEDRMHFVPDFV
OVRCEAHRFSRLXCZMGQUQBXKGGSOBPUNPMDSHQBUIFNSGDUDUDCOWGS
RFYTCYMRDSLTRDBXARZRQGKDQITVPLFVOIASDPQWQRDRXCPEGECRVF
EDPLCDSDMCBAIQDQPLCOBNVBOZURBYXCNURQBXNQWSEKQUTCIQAELT
FICZEQSHOGHWGENLTMTCPLEKBAUNAEOW
```

3. Apply a dictionary attack to break this ciphertext.

```
CQAHUBVNTIZNTODRBAFRCEAWRKKRNODRVTMCNZITVTUBKHQCXEPRBN
TZFRZHMBABNOXEQGBTWRTZPODRCUQZOPKVUFDWONTZDRNKFWFKDEDR
BANOPGVBIWMTAWRKXEPRVTLQPUDKOMKATZMXZIKDVTLUDARPTBISBA
QCTPMKCKDBZNBTYCGNRLXVBNRABHFRLZKRQFKHQFPDOPZNDKMOQRTZ
PVBLLHBFOTVRADTBZNVPYCDVTOMBADTBISCLOTEVILTODRBNRAVNMC
NZFRRAEARKNKTOELRKCQBVKRIQMHRQDKQKBLITETKBDBQCPQRKQFKH
ZNVPZBLFDBQCZNVPITZDABDEVQHASIAWQPOYBAOPUKKHRLGPZIVQFR
EHVQQERAKVTZ
```

Unit 71
Hill-climbing attack on the Playfair cipher

We are going to begin with Cowan's attack ("simulated annealing") and make some improvements. In his method, fitness is measured as the sum of tetragram frequencies. A parent key (in the Polybius square) is set, and from it a child key is generated by swapping individual letters, swapping two rows, swapping two columns, or flipping the entire square. If the fitness of the decrypted plaintext from the child key is greater than the parent, then the child becomes the parent. This is a step upwards. However, it is easy with the Playfair cipher to become trapped in a local maximum fitness. To allow the algorithm to escape such a fate, a "temperature" is added by allowing a step to go downwards in fitness if the distance down is smaller than a random variable that drops off exponentially and which depends on temperature. As the temperature is reduced, the jitter in the motion in key space gets smaller and the distance downward that is allowed gets smaller. The temperature is allowed to slowly decrease to zero. If the algorithm has not found the global maximum fitness at that point, then it starts over with a high temperature. The algorithm actually does not know if it has found the global maximum, and requires human interference to stop it.

The first improvement that we make on this algorithm is to use tetragram fitness as described in Unit 9. Our definition of it is an average over all tetragrams in the decrypted text. As an average, it is not dependent on the length of the text. Therefore, it can give the algorithm a clear indication that it has found the maximum and can stop. A threshold above which we are confident that we have English text was found in the exercises of Unit 9. For the Playfair cipher, we remove all 'X's before evaluating the fitness, since they would have been added between any double letters.

Our second improvement is to use a constant margin of error for downward steps. In our algorithm, a downward step is allowed if the distance downward is less than a fixed amount and if a random variable is within a predetermined interval. That margin is 0.5, and downward steps are allowed only if the random variable lands in 5% of its range. The global maximum will be steep enough that the algorithm cannot walk downward out of it. So we can terminate if we have reached a point from which we cannot step upwards within a large number of tries (around 10,000).

Here is the full algorithm:

1. set the parent key to a Polybius square with an unmixed alphabet
2. set the best fitness to the fitness of the unmodified ciphertext
3. set the counter to 0
4. while the counter is less than 10,000

a. copy the parent key into a child key
b. randomly choose one of these modifications to the child key:
    i. swap two randomly selected elements
    ii. swap two randomly selected rows
    iii. swap two randomly selected columns
    iv. flip the square around the diagonal that runs from upper left to lower right
    v. flip the square vertically
    vi. flip the square horizontally
c. decipher the ciphertext with the child key to find a new plaintext
d. calculate the new fitness of the new plaintext
e. if (the new fitness exceeds the best fitness) or
   ((the new fitness exceed the best fitness minus the margin) and
   (we roll a 1 on a 20-sided die))
    i. copy the new fitness to the best fitness
    ii. copy the child key into the parent key
    iii. set the counter to 0
f. increment the counter

5. output the parent key

Reading and references

Michael J. Cowan, "Breaking Short Playfair Ciphers with the Simulated Annealing Algorithm," *Cryptologia*, 32:1 (2008) 71-83, DOI: 10.1080/01611190701743658

Programming tasks

1. Implement the attack. If you used a different logarithm base, you will want to experiment with different values for the margin.

Exercises

1. Break this ciphertext. What is the keyword?

```
UDSDAEEPVFHPKNNMPILPBMNGDOOGHPGDVFHIVQRSURBETIREAFHPAV
KFREHRRMFANFPUDMRAAUPIAGPEXFTGRUODWRBNFNDOTGPWQGDMNLQV
WEUWHGLDFSAUNOQPUALZSDZDGUFABEZDRBDFDVVQRSGMBEIZTDFNOP
PLPUUVRBAUGTVEHRARFKDRBEODUDVEUCAWRBPRDSNEBXRSLTPWQGRA
FAKGLPUWHGLZBFREIEREZLRETZWGYNLPDUFPECPZZDMUGUUTICGUIA
RAODOQGDUGIZGHUALZMUBVZDDMZDRBGUFAEFBRDMARDFOPBRPRNLOM
SDSRXNOREBRADMGKANMHKIDZUMOAPLOAAFUNRZARSIGHUSMGZDRDEP
UWBEIFREOPLSFNBWAUMPTLMGNLRZARSIPIAUXGZDPR
```

2. This ciphertext is from the British National Cipher Challenge before it was national (2001). Figure out how it was disguised. Break it. Make sure your decryption is a clean one; otherwise you may have made a mistake with its disguise. Can you find the keyword?

```
NZTFM YKDID MYLCY NSGZK VXKMX ALZDP MYLCY NSGYK VXKMX
AGKOG LCYUR EGPNY TFMZK DMNGL HWCLL DKYAB IYYKV XKMXA
DYOSJ PCDHU GDKIK UVXKM XADYO SJPCD KUJAS DLBEU VTNZT
FMZKD ZIKMG JLCEU DAYNV XKMXA IYGKP EJGHL HMAII YYKVX
KMXAI ZQSNJ OLHKJ VIKVX KMXAL YNJYG PDHLI YMCBS YLKCE
GYOSX XANJD NLKDP LIQZD KHGJG XANJD NLKDP LIQZL YDSGK
DWDOE JANEB SDAVV GKDCT GIZLY LSDFG DOEJA NEBSD AVXAG
LXADS TFEKI MCDMX XAOSD SJELX KMPEH CQDKS GZKDQ SIZGI
VMDSJ EGXKC ZMGPG LKUYM JGKYK IMZFN XADPN YKIZK IMKZY
GELJN YMIDN JDMOK IKYOL HDPOL LEDPC LSDYJ EUAGK DQISO
QDMGJ ZGEGO SDGLH FGPMC SBPEJ GUGXE JKSII MXAKY KZCMG
FWKKN PHJSK DSMBS FKHMD GQYKD MGMZG JIKJT GIZGE BYNAG
KDSNB DEDGL AWKDJ NIGYG GIXAK OAGBQ XKGIM TGEKB ZKJTG
IYNGJ CHYGX RKYOL LEHQK IBGEW GJQOK THCBS XALKB SMZNH
PDJMG FWKKN SMGMB GSDYQ NZTFQ IZIBX NEAXJ QBJZN GWKDK
USMVX DPDET FXD
```

3. Break this ciphertext. What is the keyword (hint: it is a name)?

```
BIPAFKWLIFETHACPEGKWCKKPIUDQCWPMLKBIAMSFFSAFQDANHOBQTB
BOKOSCQBTBQCFWUHHACPATIRFYKWUBQOIRHOOKUPZPQVONLCPKWOMK
GRCRKQVIPUBICMHACPATNLHWHFPMHOIQQTQNKNWOIXSFRCCRKQPRHI
OQQTQNEHQOOBQBUQGICPKPAPBTBTQOWOBIKUEFKMRCCRKRQYQYUQKT
CBCPKPAFGYSLPKCMQEKPUHAUDAIFKQBIAQQMINQCBICUKUOKMROWGY
FSAFQDHORFPUPKKFAIXBCPGARUZCUHXBKIMKWOFHQTRABNWOARTAOB
OUINTGUCQYOKMRQBCPKPFEKLPKCMQEKPUHAUMIHACPTQAQNEQKPAKP
UKQHHOFXQALNQAPZPUHDKRUKOKVNBIKUAZBFFKFYKWYLAMQNVNHOFS
QDUCQYOKMRQY
```

Challenge

Not square.

```
G0IJVEFCDLZMDECBNAV4VIWGBRCEACKTVETFCKEWDBIZPMRFNETSZOVCJPL
KIEIPYCICKTDIZUHTNBUEFTGTCAFCNTIJTSGFCGATKLVFVE2FUY2FGAJTNZ
GZKTCIFVTFEXACKTJCUYUVNUTCRFRFKT2FJBENIVGLJEGDDLCTPOOBCACBV
GJCCKVIFCEAILFCUFNELFIEFCPL2FTQCENGIRFCUFNELFSFVNCEGNBGNAQC
TFGAFCCIKTEYSA2FCFBJFBGAFCFBETBFIVKLPHNGPLFATAG0NGPL2FTQCEF
RFBRKZFCKFVJZEXVIWCIVKLNGHRDTH3FYANGTF2HPECWNODBCFJVENGTCVJ
NZGONJTFANK0FBNEYFNBBCENRKFJKYFGAQGFNJCNNZOZ5JGTFSDLCIFVNBO
PVEXCLHEXTHHZZEVMTKGACEDBCAKTAYJCAVF2NSCRVCVILK5JK0FBNEVEJC
NVCICNNZOZ5JGTGFRJFSDLCIGFILJPLKIEFCPL2FTQCEJCUFVIFCEAPLNSC
GLIHLCQFREJNTLISTEBKZPMRFRCTNVUTFBKENTAHTCNNZOZE0CESTEQUFNE
CGCNEBVGFCWEFGOPIVKLCINAPHCINSCNEAIDMUVFTNEZJBTCNGIRJOCNECH
```

PXCIRPLCTOZ2FGZLPXCHQJ0VIICIJYFILJPLKIEFCPL2FTQCENGFPGBWGGN
OPBDIPVULHPGKTNAJPLKIEFCAVPJZEFSIVCKCECGIVGAFCNSACEGNBZJEBJ
QFCEXJBTCNGIRJOCNECECBCLNACIRILFCDTDBPDCEZFQCTCCILFE0CESTEA
FCZJEBFPKENAQCASIJHUECJGKTWEK0FBNEUYVEENGLCBZVEKGJOTJTERVCV
IFVKTECNBVIZUJOOBJHFTJRRKCICSRKCEGZKTCYTKGVPHCIBFTDGTJDNBDI
CGPOCGTJXEJZTBCNEBQGTSCNBCKQ

Unit 72
Vertical two-square cipher

The *vertical two-square cipher* is a digram substitution cipher that uses two Polybius squares, one above the other. The plaintext is padded to an even length and divided into digrams. The first letter in each pair is found in the upper square, while the second is found in the lower square. The ciphertext letters are taken according to the rules:

- If the plaintext letters are in the same column, then the ciphertext letters are the same as the plaintext letters.
- If the plaintext letters are in different columns, then we find the rectangle that has them at two of the corners. The ciphertext letters are at the other two corners. The first ciphertext letter of the digram is taken from the upper square, the second from the lower.

  An example couldn't hurt. Take this plaintext:

  ```
  THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
  ```

It has an even number of letters, so we do not need to pad it. Let's use the keywords `POLYBIUS` and `KEYWORD`, and fill the first square by rows and the second by columns.

```
P O L Y B
I U S A C
D E F G H
K M N Q R
T V W X Z

K R F M T
E D G N U
Y A H P V
W B I Q X
O C L S Z
```

The first plaintext digram is `TH`. It defines a rectangle and we find the ciphertext digram `WY`:

```
P O L Y B
```

```
I U S A C
D E F G H
K M N Q R
T V W X Z

K R F M T
E D G N U
Y A H P V
W B I Q X
O C L S Z
```

The last plaintext digram is ER. They appear in the same column, so the ciphertext digram is also ER.

```
P O L Y B
I U S A C
D E F G H
K M N Q R
T V W X Z

K R F M T
E D G N U
Y A H P V
W B I Q X
O C L S Z
```

The full ciphertext is

```
WYAOKDALSNDBASGDUTYPTEDWCKEVEMUESXLYER
```

Decipherment with the vertical two-square cipher is the same process as encipherment.

Reading and references

Félix Delastelle, *Traité élémentaire de cryptographie*, 1901.

Wikipedia, en.wikipedia.org/wiki/Two-square_cipher

Crypto Corner, crypto.interactive-maths.com/two-square-cipher.html

Warren Thomas McCready (“Machiavelli”), “The Twosquare Cipher,” *The Cryptogram*, Nov-Dec 1972, 152-153.

Programming tasks

1. Implement an encryptor. Remember that there are many ways to mix an alphabet with a keyword and many ways to lay a mixed alphabet into a Polybius square.

2. Implement a decryptor. Remember that there are many ways to mix an alphabet with a keyword and many ways to lay a mixed alphabet into a Polybius square.

3. Implement a dictionary attack. Remember that there are many ways to mix an alphabet with a keyword and many ways to lay a mixed alphabet into a Polybius square.

Exercises

1. Encipher this text with keywords `HUDSON` and `EXPLORE`. Use the same methods for mixing the alphabets and for laying them into the squares as in the example above.

   > I take for granted that you are tolerably well acquainted with the different modes of life and traveling peculiar to European nations. I also presume that you know something of the inhabitants of the East; and, it may be, a good deal of the Americans in general.
   >
   > (from *Hudson Bay* by R.M. Ballantyne)

2. Decipher this text with keywords MAPLE and LEAVES. Use the same methods for mixing the alphabets and for laying them into the squares as in the example above.

   ```
   XCSOKGSOMYHBMQBWSOLYEWLYMXPRHZSTNZQCMZLGMBMPWILWQQBPVG
   ICHHVPPRQKIQMAMHMZXBHZAYHUHDBWVDTIMBAYNYVDNTIYUHHTKEHP
   PGCNSCEVXCSOSMKXPWIRACTTHEQCVDSNNZELDBIYPGYTKEITKGSOLZ
   OWHTMFLZHELOITDIITWRACTOSCMZSOLGFLRDLYAXSOLYHFLYSOAZTB
   TWIYDBMXMKIQBXRXVTNLMNKZSOPYPCHTTRMWQQIQTBVGTWKZTBVGIY
   YBIXPZNLQZMZMBPPBINTICMBKGBISIDZVDMOKGDWNTHEKEDUVDZQ
   ```

3. Perform a dictionary attack on this ciphertext. The keywords are short.

   ```
   DUDAMXTENUICFGMPRLUBGGAMFQQIMXOLLWQQOMESITRSSGLQLIHMES
   DAXQOIRXTMBDNHKDOUMODUWCRLFGGSBPILBOSXECTERWECNLVPNSMK
   QDOFESQQLWHMESBALMQQBOSZDALOMNDOXGSPEGREFGECGXCBAFVUMI
   DNNCGGQQSPKDATDBXDSPGSOUHCNXASHTFQSINITSFEKIASLISPGGBH
   FFBPDZGCDGTLQXHTFQMNQNREMTDHHDRXOMLSAZQBFGIXGGSPEGREAT
   LPECQDHMFQMNQNMISPHFLQSPMTSQMEDGSIPKBWSXFRCPEGLNWEDAVG
   YTESELVETGMBQIELBPSPSPATESMOSPHEQQMLGGLWAEHEBZQEFEWTCB
   FFGGTYHEDUECLAOXEDDQWEWCUDESLNRLBWMIBOSXECQBNSMCEOPQPI
   BPFOLNLGNNDBLVDEAEFEYSGFGEBPQQAFTHREECIXTLLPGUHKSYGCED
   GGQQSPKDATDBXDSPBPTXHTDUQPHEOUMIEDBSQDTLGUDABVOSRMQDOF
   ESDIRETMNUFDSPDBBALM
   ```

Unit 73
Horizontal two-square cipher

The *horizontal two-square cipher* is a digram substitution cipher that uses two Polybius squares, one on the left and one on the right. The plaintext is padded to an even length and divided into digrams. The first letter in each pair is found in the left square, while the second is found in the right square. The ciphertext letters are taken according to the rules:

- If the plaintext letters are in the same row, then the ciphertext letters are the same as the plaintext letters but in reverse order
- If the plaintext letters are in different columns, then we find the rectangle that has them at two of the corners. The ciphertext letters are at the other two corners. The first ciphertext letter of the digram is taken from the right square, the second from the left.

  An example couldn't hurt. Take this plaintext:

  THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER

It has an even number of letters, so we do not need to pad it. Let's use the keywords POLYBIUS and KEYWORD, and fill the first square by rows and the second by columns.

```
P O L Y B   K R F M T
I U S A C   E D G N U
D E F G H   Y A H P V
K M N Q R   W B I Q X
T V W X Z   O C L S Z
```

The first plaintext digram is TH. It defines a rectangle and we find the ciphertext digram LD:

```
P O L Y B   K R F M T
I U S A C   E D G N U
D E F G H   Y A H P V
K M N Q R   W B I Q X
T V W X Z   O C L S Z
```

Then IS → NT, ME → WU, and SS → NW. But then AG is on a single row, so it is enciphered to GA.

```
P O L Y B   K R F M T
I U S A C   E D G N U
D E F G H   Y A H P V
K M N Q R   W B I Q X
T V W X Z   O C L S Z
```

The full ciphertext is

```
LDNTWUNWGAYMNXPUDBMGOIYKUPAHAYDIGRFDAO
```

Decipherment is the same process as encipherment, with the two squares swapped.

Reading and references

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/TwoSquare.pdf

Wikipedia, en.wikipedia.org/wiki/Two-square_cipher

Crypto Corner, crypto.interactive-maths.com/two-square-cipher.html
(Note: They reverse the order of each digram, compared to our method of encipherment.)

Fred B. Wrixon, *Codes, Ciphers & Other Cryptic & Clandestine Communication*, New York: Black Dog & Leventhal, 1998, pages 219-220.

Programming tasks

1. Implement an encryptor. Remember that there are many ways to mix an alphabet with a keyword and many ways to lay a mixed alphabet into a Polybius square.

2. Implement a decryptor. Remember that there are many ways to mix an alphabet with a keyword and many ways to lay a mixed alphabet into a Polybius square.

3. Implement a dictionary attack. Remember that there are many ways to mix an alphabet with a keyword and many ways to lay a mixed alphabet into a Polybius square.

Exercises

1. Encipher this text with keywords `BACON` and `CIPHER`. Use the same methods for mixing the alphabets and for laying them into the squares as in the example above.

   > For months and months the eye has been assailed by paragraphs and pages in the literature of two worlds, contending for or against the existence in the Shakespeare plays of a cipher that would assign the honor of their authorship to Lord Bacon.

(from *The Little Cryptogram* by J. Gilfin Pyle)

2. Decipher this text with keywords `POLYBIUS` and `SQUARE`. Use the same methods for mixing the alphabets and for laying them into the squares as in the example above.

```
FLHSHXESUORPOHLSVUAMYBIVMFQONAXPQYTDQVQFGHCELDBSEGMOSK
KHKLLIOOSOFTNYSEBLPMQTUOLSBDORDBBBCPUKDNLSBDICWYCUCOPW
CBUNTEQVNTOVCBDONFISQPTDKHNAQNDNDOQYQVNIOXCBYUNTOZCBQF
EPKHSVUXUMTIUONFUWMOOVCBDBQXCUNVLIDBOVURFKUOUVFOXOOUTD
EBNFNHPMQXCMNAOPUMQFDBUKDNLIXMQXOVCBBLLIOMUVHFNABWSVBG
UVRKNIELKLLIEVLDDOFLDBMDQLUOBLODUNUXUMFPPMQTUMDNODKEKF
MULIIVBGCMBYPEKFNAQNOWUVNHPWOUIDKLOFABNMDBAMWRNIUXCOBB
OFPBNAGYOUUVNXNDALLSOULIXMIDIPOVNTCBENNTLFLISEFKQPSDFP
OFDCQXIVMXFLVLXMUMABLIOOBGCMMUQKALEURKNICMODKEKFMUNIUE
PHEPUWMOLIIVNAUPMHDRUVNIOGPWCBBQKHNXBDTDLICMNABUUMDNVR
LICMUORTBELDMUEVLIOMUVHFNAOOGDDBLIXMBXFPYCQXUPBQCPOTMV
URTTCBODKEKFMUEVQYQKLIUVMONANHASBONWMULIOELIUVURDNRNNS
MVSKPZQKVF
```

3. Perform a dictionary attack on this ciphertext.

```
NIUGOTANORETOTQLWAQNLATSKAASARQNTHSARPQVLTCIEMXUNELTLA
NTPMQDLGKTDEBBDEESSHINKGADXSSEINKGMMLPTSKAASKCSFKBNDAO
DRLTHRRFZUSLXSRGBKUOUDNELSFHGOIBWFRGWAKZNPNOKARFLEONDN
STSASUUPPDBKTZNPEBHRLATSEMAENEUOSEGDGOLZNPIHNTKAWBLNUG
AETTDNQNTHSAUGONFORFUDNEUGBGPDSSOTZUSLROOELROTQFTHECNT
ARRGODNTKAVHQLSEHDKGFORGDKSURGNTGOLZMMRFFHHVNICNLZLEUD
NETSKUMLROAEAMVNNGHUBREOMPOOHHRBEMDESEUGANUHLUEOPOOMLP
```

Unit 74
Hill-climbing attack on the two-square ciphers

A hill-climbing attack uses two mixed alphabets and the parent key/child key paradigm that we saw for the Playfair cipher. When it comes time to modify the child key, we randomly choose to swap two characters in the first or in the second alphabet. It is not necessary to flip squares or swap rows or columns. To avoid being trapped in a local maximum, a margin of 0.2 works well.

Here is the algorithm:

1. set the two parent squares however you like
2. set the best fitness as the fitness of the unmodified ciphertext
3. set the counter to 0
4. while the counter is less than 10,000
    a. copy the parent squares into two child squares
    b. randomly choose which child square to modify
    c. modify that child square by swapping two randomly chosen elements in it
    d. decipher the ciphertext with the child squares to get a new plaintext
    e. calculate the new fitness of the new plaintext
    f. if (the new fitness exceeds the best fitness) or
    ((the new fitness exceeds the best fitness minus 0.2) and
    (we roll a 1 on a 20-sided die))
        i. set the best fitness to be equal to the new fitness
        ii. copy the child squares into the parent squares
        iii. set the counter to 0
    g. increment the counter
5. output the parent squares

Once a key is found with a hill-climbing attack, we can recover the keywords by swapping rows and columns. For example, if we find this (half) key:

```
T P R Q O
E M S U A
N I L K H
G B F C D
```

```
Z W Y X V
```

then we can rearrange columns to make the last row more orderly.

```
O P Q R T
A M U S E
H I K L N
D B C F G
V W X Y Z
```

Now we can reorder the rows:

```
A M U S E
D B C F G
H I K L N
O P Q R T
V W X Y Z
```

It appears that one of the keywords is `AMUSED`.

Programming tasks

1. Increment the attack for the vertical two-square cipher. Remember that there are many ways to mix an alphabet with a keyword and to lay the alphabet into a square.

2. Increment the attack for the horizontal two-square cipher. Remember that there are many ways to mix an alphabet with a keyword and to lay the alphabet into a square.

Exercises

1. Break this ciphertext which was encrypted with a vertical two-square cipher. What are the keywords?

```
MEXESAEPQHNPLAOKMGBSUNUTXTDCALPTOUERPTGHNVGHNBOQISPQFT
REFOIHREKLFAIHREGRDHQFOQISQXMEIBHUMQLHNAUNNACEIHMTIHRE
WEREALPQRDRESADCRDREPQNFMNHSDKKLEQNWHIBTPTFOUNRHCAREHS
CPDIFOSLYTHISLKLNXCQBSWHRENXMEHHDHPTGHEPTYFHOKDMIZGHKL
NXMEHBAERMGIVEICIVCQALREADWSTRPMGCONMESATRTNGCHQCWMGWT
LLIZKLGADBNEMEIHCEIHKHRDRRGKORPTEHDHPTGHHMDCDBPTEISNVT
DHPFTRPTEBTRQTCCHLFOPTOUERPMSTUTMCIAUNBSMFORSTAIDHDCLT
NAESCEIHAMTNTOMGUTNHSADCHQINDBHQGCOKDNXTDCREGRFHGSLLXT
QYLHPTADRHGIKLHNTXAHBBHLGCHLTTIAKHHUBGTRXEULIZADCWKLFQ
PSFWBTKLNELDFOGHQTNAWHECYTIHGAKDONDMIESX
```

2. Break this ciphertext which was encrypted with a horizontal two-square cipher. Can you untangle the keywords?

QMHCPVUNGIPBYNTNDKCIXGCITHMBKNVLQMEBGITRBPKNTSSFGPAPIS
HPTSMFQMFNMVFNHCMDSNICHCOPFHMOESFCPETIRRHCQINGBATIESWH
SXNITQCNLPNAIMPBGDBPBOEDQPDGEWTIPPCRADLQPPWRKPPIDDCTOC
WHMBKNQMDHRPUAYPHPGDPSILWHBWESSNDHEDMEPBLIEHRIPSBHMDQA
QAEBICDFILGHCTOYDISOWNECESQMDHWYILWHADIHHPDGEYYSGNMDQA
DFGNSHCOOCPSBDEQPBGAXCBIMBESASUCTMDQTSQSPIBDEYZSQSMHID
QPSXIDCSMVFPEIEXEAESRBPEZEIHTICQVPAPCRKNFUFPTYRAPEHBPV
MCUPEHAPTSQMYNWYMFPIQEHPMBSTIADIAHPTCVRBBNADAPUSCIZEIH
AHEBLFDHKUHPSRXCOIPKQAHPWHMBQIDKFPFUUFZPEDUPAHQIDGTIER
MBSPETOYAKIVKCGPMNDAHCGUQMDHDFDYEHLCRMCIKNOCSNMIYPPIBD
ELVPHHQMFPAKIVKCGPPCWHUSRHPVQPUCQMDHQAQMFEEIDLQMYNDEHP
PSNMBOERURPEWNQMFNSOQIDRUCNAQMIHWHTSQMDHAHESWHPSMPCIEH
DIEHODHIADMFCSEISPHU

Unit 75
Four-square cipher

The *four-square cipher* uses four Polybius squares, arranged in a two-by-two layout. The upper left and lower right are the plaintext squares; their alphabets are not mixed. The other two are the ciphertext squares and contain mixed alphabets. The plaintext is padded to an even length and divided into digrams. The first letter of a plaintext digram is located in the upper left square, the second in the lower right. They form the corners of a rectangle. The other two corners hold the ciphertext letters, the first in the upper right square and second in the lower left.

Let’s encipher this message:

```
this message is encrypted with a grid cipher
```

Its length is even, so no padding is needed. We will use the keywords `POLYBIUS` and `KEYWORD`, and fill the ciphertext squares in an unimaginative manner:

```
a b c d e   P O L Y B
f g h i k   I U S A C
l m n o p   D E F G H
q r s t u   K M N Q R
v w x y z   T V W X Z

K E Y W O   a b c d e
R D A B C   f g h i k
F G H I L   l m n o p
M N P Q S   q r s t u
T U V X Z   v w x y z
```

The first digram `th` is enciphered to `NB`.

```
a b c d e   P O L Y B
f g h i k   I U S A C
l m n o p   D E F G H
q r s t u   K M N Q R
v w x y z   T V W X Z
```

```
K E Y W O   a b c d e
R D A B C   f g h i k
F G H I L   l m n o p
M N P Q S   q r s t u
T U V X Z   v w x y z
```

This continues, and the final ciphertext is

```
NBSQHENPOROZLMLLOPZIRWOXAQIYUNAWYAFCOS
```

Reading and references

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/Foursquare.pdf

William Maxwell Bowers, *Digraphic substitution: the Playfair cipher, the four square cipher*, American Cryptogram Association, 1959, page 25.

Wikipedia, en.wikipedia.org/wiki/Four-square_cipher

Practical Cryptography, practicalcryptography.com/ciphers/four-square-cipher

Crypto Corner, crypto.interactive-maths.com/four-square-cipher.html

Fred B. Wrixon, *Codes, Ciphers & Other Cryptic & Clandestine Communication*, New York: Black Dog & Leventhal, 1998, pages 221-222.

Programming tasks

1. Implement an encryptor. Remember that there are many ways to mix an alphabet with a keyword and to lay an alphabet into a square.
2. Implement a decryptor. Remember that there are many ways to mix an alphabet with a keyword and to lay an alphabet into a square.
3. Implement a dictionary attack. Remember that there are many ways to mix an alphabet with a keyword and to lay an alphabet into a square.
4. Implement a hill-climbing attack. Except for the decryption routine and margin, it can be the same as for the two-square ciphers. The margin should be about 0.2 when the fitness is lower than a threshold, but near zero above the threshold. Experiment with it until you find a threshold that works well for you.

Exercises

1. Encipher this text with keywords `WINDY` and `WEATHER`. Use the same methods for mixing the alphabets and for laying them into the squares as in the example above.

   > We all held the string as fast as we could, and tried to pull down the Kite; but it was impossible, for instead of bringing her down, we were all three dragged along down the meadow slope.
   >
   > (from *Adventure of a Kite* by Harriet Myrtle)

2. Decipher this text with keywords `NUMERAL` and `CIPHER`. Use the same methods for mixing the alphabets and for laying them into the squares as in the example above.

   ```
   CTBTLONUTEISIVRHSBOINKEUHTMNMMPNUUNGSBISDPEKEYFDMCDMDP
   PKMUOPDITPZCOIHCDMDPQQXTTHHQGUMUUSLHEUAPOHFGKSKIOIHOBM
   QDUEIHYMACKIQSURUNQUPHMUKEFGEEKTOHIPXAAMEUDPTIBTILEMPE
   PHSUQDEOQDBTBMTSTIPBTIEOUUMCRSOIEXCTNGSLLQNEOMYDHPTIMO
   MUQDNNMNCQCLBOQELLMUOPDIQX
   ```

3. Perform a dictionary attack on this ciphertext.

   ```
   EQVOMWHHQSPEHMLWCGEINSBEPEILCQFDCDXCSBAIROTWTBPPPLQCRW
   XCGLFHQPFTYTCDIPLARQROMWROQPOKBRMITABAFWSKGGUKHMGLHMNS
   IZLAPNFHROPEGGHMFQAWQNUKGSPEGSILLHGGTWBEROFLRWPEGSLAVO
   MIAELAPDTAQKAMFWMLHMSKUCBRPPIRROTZGFHRTOGLGZKAHPHATNQE
   FWLFOBDWHLARZIGAMBQEDKEQOWGKFQHIKOQIPEIABBNKGLZOROCBFT
   AOHQKQRWPEHFQHIMQPAWZQRWHQAWCVLLDTCYLZISSKQIKNGDPEHMPE
   LLGGTBROFGCDTGKAIMHAFTAAIRKMLLSKHLFPAWEIQCYLFPAWCWGAIG
   HSROKNFGPSGGHEFWSQQEDWMBFWETBWBGVYGGSQAWHEFPAWFCQPQIUG
   CQFDCD
   ```

4. Perform a hill-climbing attack on this ciphertext. What are the keywords?

   ```
   DSVNOOSGDPFOHMLETLEOLWSFFLMHSTCIAKNSMRSVACAILZRGGKUNAM
   THTNGKCIENSFRMGSEOSAMHNOISACMSFOTFHKUORALTLZAPLCACLUCS
   LMACUEMHVFGLFNLKNKKILZDHTOYFSNACLWTNGPBXAPAMNSCDSIFOPC
   PZLTYINOXDKAGKUNAMCIFKGRGLYDRARAUMATSANKKOPLMOAPTRAGNO
   XQYFOMLAMSBRNSCDRAPMACPWMOPZLTYINOYFOMGSPCELGFSTDSHNMX
   YFOMLWPMFWZKHNMXYFOMGWNSGQUQQIACWYNSMKFNSIMRFOBSVNVWRR
   MIHOTHKSSGPFGTKSULDTFOYDTOHNMRFOFONCLTFSSRMEFLRACSRACS
   MVRAONMRBRNSCDRAPMACGSEOOAONBQACQIYSDHBEMSLCGPFOUQGWEO
   RALZCSLMACHARAPBLCEIYICPUEVWFOMMRRATTOASMSFOUNMEPZLTRR
   GEGSFODGCDATTWHHBADRAMNNMRFOTNNNINLTGLDGTHTNYENSOHEYAT
   FOEOLSPLAGGLRAAMBSVKHOACAIPZLTTNTSRFGLCISIRAALXWNKVNRH
   PZLTLEGEKRQLNNQDGLCIRALMQTDZSDZKSFFCDXSGPOHEISKQHNMXYF
   MOLTFPHKMORMUNMEPZLKNKRACICQZNTNTNMMSQGLHADGKDABGKNLOD
   ISNNLIBSAKNKRGGKHYLTGHNNRAGLPZEIEOASMMFLMRMSFODFASUQRA
   CSAMLMFWOOMOGAQOPMFWZKRQOODWRACSDFOWHNVNOOVKCITOUSUORD
   LZNSMKTHAMRACSPWXSCINPZRSVROISNOGSFOHAFKSDIGQXAPYDRANS
   OIPLRFCIENMOCMLZNODSFOTNZORNCSATMHRQPMCKAPSAENSAKI
   ```

Unit 76
Phillips cipher

In the *Phillips cipher*, a Polybius square is filled, and from it, seven more squares are generated. Each square is used to encipher five letters at a time. The second, third, fourth, and fifth squares are generated from the first by shifting the top row downward one, two, three, or four rows. The sixth, seventh, and eighth squares are generated by shifting the top row of the fifth square downward one, two, or three rows. A square enciphers a letter by replacing it with the letter that is in the next column and next row, with wrap-around.

An example is essential when the explanation is as poor as the one above. Let's begin by filling a Polybius square with the keyword `POLYBIUS` and generating the remaining seven squares.

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

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

Notice that squares 0 and 4 have the same effect, as do squares 1 and 7. Now let's encipher a short message. The first letter enciphered with each square is highlighted with pink in the square and below. Notice the wrap-around used in enciphering 'T' to 'O' in square 0.

plaintext:	THIS MESSAGE WAS ENCRYPTED WITH A PHILLIPS CIPHER
square:	0000 0111112 222 233333444 4455 5 55666667 777700
ciphertext:	OKEG WNYYBRL AHG LYDPZVONM YEOI R EIVGGVEY POEKNT

Reading and references

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain; chapter XIX.

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/Phillips.pdf

Programming tasks

1. Implement an encryptor for the Phillips cipher. Allow for several choices on how to mix the alphabet and how to lay the mixed alphabet into the square.

2. Implement a decryptor for the Phillips cipher. Allow for several choices on how to mix the alphabet and how to lay the mixed alphabet into the square.

3. Implement a dictionary attack.

Exercises

1. Encipher this text with the keyword `EDGAR`. Use the same method for mixing the alphabet and for laying it into the square as in the example above.

   > Now the irony is this. In this walk, so many times repeated, the world's greatest master of the terrible and the bizarre was obliged to pass a particular house on the eastern side of the street; a dingy, antiquated structure perched on the abruptly rising side hill, with a great unkempt yard dating from a time when the region was partly open country.
   >
   > (from *The Shunned House* by Howard Phillips Lovecraft)

2. Decipher this text with the keyword `RHYMES`. Use the same method for mixing the alphabet and for laying it into the square as in the example above.

   ```
   UBSSOOWGUHWHTWFUVHVYDIVLSPGFOWPGFWSNKHAXSAQWAUWUIFKNGU
   HQLRQYVGWOIAWGLFGWPFSIYUWNFMQYSHUYNFGIONVYRGYVSIFQNKUW
   SFGWSFUYHUIFCMSASQVUQLNGXIGRCUEASGUQWVMIFUIFGWAKWVFQVU
   BSGFRYKHGIBNIBUVXPAIYSIVUCZHWGKZBANRGFIFUMWEIYXUNOGWHR
   WUZYAUSIAUIHGFMQSIBAUYKYMV
   ```

3. Use your dictionary attack to break this ciphertext.

   ```
   RAPSZUHLHMRIXQGAPPHIZURAQKOHXLGHLYGOLKAUPSFALURHMSZUXN
   KAESXZZBRAYHUBHIKCLYDCDOZUDKALSBSMHMNTUSZVBVZIXAIZARIB
   UKXHFCAVPSHMIFLZAXBSIHLKHSTVUIZAGIBUCXHXUBSFGHWLUGKLDV
   DPHKEIKAXZQKAEIZVWAZZIXQKLHYSTHYRHUHPHVRDFAZHXBSRQNUDI
   MSZERAVCKYDIZSHFYSLUHXHZUZ
   ```

Unit 77
Hill-climbing attack on the Phillips cipher

Our hill-climbing attack on the Phillips cipher is similar to the one for the monoalphabetic substitution in Unit 28. The parent and child keys will be mixed alphabets, not sets of filled squares. To avoid getting stuck in a local maximum, we will use a margin, as we have done before. A good value for the margin is 0.5. Here is the algorithm:

1. calculate the best fitness as the fitness of the unmodified ciphertext
2. set the parent key to the alphabet without 'J'
3. set counter to 0
4. while counter is less than 10,000
    a. copy the parent key to the child key
    b. randomly swap two letters of the child key
    c. generate the eight squares from the child key
    d. decrypt a plaintext using the eight squares
    e. calculate the new fitness of the plaintext
    f. if (the new fitness exceeds the best fitness) or
       ((the new fitness exceeds the best fitness minus the margin) and
       (we roll a 1 on a 20-sided die))
        i. copy the new fitness to the best fitness
        ii. copy the child key into the parent key
        iii. set the counter to 0
    g. increment the counter
5. output the parent key

Once we have a key, we may not have *the* key. The reason for this is that if we roll the entire square to the left or right, then the cipher has the same effect. For the example in the previous unit, these versions of the first square (square 0) are equivalent. No matter which of these you choose, when you generate the remaining seven squares and encipher a text, the ciphertext will be the same.

```
P O L Y B    O L Y B P    L Y B P O    Y B P O L    B P O L Y
I U S A C    U S A C I    S A C I U    A C I U S    C I U S A
D E F G H    E F G H D    F G H D E    G H D E F    H D E F G
K M N Q R    M N Q R K    N Q R K M    Q R K M N    R K M N Q
```

```
T V W X Z    V W X Z T    W X Z T V    X Z T V W    Z T V W X
```

If we find, for example, that the key is `LYBPOSACIUFGHDENQRKMWXZTV`, then we can lay it into a square and roll it until it appears to be in order, and thereby recover the keyword.

Programming tasks

1. Implement the attack. Use tetragram fitness.

Exercises

1. Break this ciphertext. What is the keyword?

```
DWCFPHQAZAXMZZLZPLYARDZDMEHHDUUGLFGZPSKMFDWLHOIKIHRFOM
TLCQXCDZPCSLBREHQQZKDLNMAQLFEABIGVZHSMTNMWXBSASBZCWUKU
DGHSOZFHQAFQDHFLOAKRATQSLZLLZTZKMLQLFKAAIVBDFHULICCGZF
CBOAKFCATTILKVTALQLQDHIUULRIKUSLPZIQGKHCFQSZUGLZMZGMSO
WQVWQSZQLGDHCCGWPSOALCGFDFHMLTHQSWCLMAMZHZLYOCVZZICUDU
VHGDLHAWGHQCWLBICGHNRMGPLYWQLQSELHWULGLPHIHGUANGKACGBQ
LTGKWCRNTLRLWYVBLMLHGGKGRGAHIGDZHKGMSDBCOSZSHQNZKQVASZ
AVFHQDOUGBIIWKZFH
```

2. Break this ciphertext. What is the keyword?

```
BVGHUUWZKGDQLDDFZUFYVMUIVLNZKUXALMRWGHKWGHVABNNSNGHERZ
FYFOBFRBCBILBPNVMHPMUZIKSZFVMULFZZWOUWETFPXIFZAMZECGHM
MVFMRXEIFVHKFABURURHVQRQIPNOZYZUVMURHZPFVHKUGHMRURHVQC
XIKNHODARQVFRYVXNNZFGHBVIVLFAUHPBADNHOKICBVWKKZWGHQVRA
IZUIFMZEFZQVLCXEVFAEGHNNVMUPNFAZHKDQINZZFOHIERHZGFVOLF
AFMPNFAZHKRNHAHVLHAKUQLFPXNNIUUHUUHHVUCNHEUALKHPNSAHVE
BAKUHOFTNVNWHWWHBVURFHZNVLKMRUBWFXNWABNNKWAVSDWFUNGUBF
RHVEMZPFFUUCUGHKUISVURFZFPMZWPZSGFRDQYZFPXVBUBMVKUFZUQ
INXUWRHKCXFFLRSVLRQRRXFFLRWUZFQINQUNCHKXZMHFVKRWBCVFSW
ZZWOOWFRRXIRXYLRMBLNFAGFELK
```

Unit 78 (optional)
Phillips-RC cipher

The *Phillips-RC cipher* is a modification of the Phillips cipher in which rows and columns are shifted when generating the eight Polybius squares. The encipherment proceeds as in the Phillips.

Here is an example starting with the same first square as our example for the Phillips cipher:

```
    0           1           2           3
P O L Y B   U I S A C   U S I A C   U S A I C
I U S A C   O P L Y B   E F D G H   E F G D H
D E F G H   E D F G H   O L P Y B   M N Q K R
K M N Q R   M K N Q R   M N K Q R   O L Y P B
T V W X Z   V T W X Z   V W T X Z   V W X T Z

    4           5           6           7
U S A C I   F E G H D   F G E H D   F G H E D
E F G H D   S U A C I   N Q M R K   N Q R M K
M N Q R K   N M Q R K   S A U C I   W X Z V T
V W X Z T   W V X Z T   W X V Z T   S A C U I
O L Y B P   L O Y B P   L Y O B P   L Y B O P
```

If we can break a Phillips-RC ciphertext, then the keyword may not be obvious. We can roll the square until it becomes apparent, as explained in the last unit, but for the Phillips-RC we must roll horizontally and vertically.

Reading and references

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/PhillipsRC.pdf

Programming tasks

1. Implement an encryptor for the Phillips-RC cipher. Allow for several choices on how to mix the alphabet and how to lay the mixed alphabet into the square. Feel free to copy and modify your implementation of the Phillips cipher.

2. Implement a decryptor for the Phillips cipher. Allow for several choices on how to mix the alphabet and how to lay the mixed alphabet into the square. Feel free to copy and modify your implementation of the Phillips cipher.

3. Implement a dictionary attack.

Exercises

1. Encipher this text with the keyword `STORY`. Use the same method for mixing the alphabet and for laying it into the square as in the example above.

   > Once upon a time there lived a cat of marvellous beauty, with a skin as soft and shining as silk, and wise green eyes, that could see even in the dark. His name was Gon, and he belonged to a music teacher, who was so fond and proud of him that he would not have parted with him for anything in the world.
   >
   > (from *Japanische Marchen und Sagen* by David Brauns)

2. Decipher this text with the keyword `FRIENDS`. Use the same method for mixing the alphabet and for laying it into the square as in the example above.

   ```
   ZQCUBXHDEFKYZOHTOVMLZZQCBQMPXKSUHOAWFMNMBDPLMUMZXOUNXI
   OPFQLFQCUBSZMQVYULZCYDEHIUCZQBOQXFXPUZORULZFVXZQCUBXGE
   PTVYDQUZLHEZALXLDIZOMOWPZUQKAQNMCKBACQZXOPMMRULPEULACZ
   WZQMTLHQZOULIYPFNLZACCIBHCMZUHRNHHZLHFCLAGQXKEDEEEYPZN
   HLXXNQBOWGHVTZSUHGSOMULZZUCOWWFMOEXXUPUMFNILKKMNLGQTMM
   LGQSUMFEIVUBPQZLHDOLHIZIUOYNWALKICDZVYZXULOYGIFXXHPDLI
   CIEDECZIUQYIVKFQLZMWVGQZBMTLGQAKZOMNCLKZK
   ```

3. Use your dictionary attack to break this ciphertext.

   ```
   NGQFUQBVQLVAVWKHKTXAEPGFZETVMHMRUOVYQZZVSPZQOQMQZZRPOA
   MAQDKWUSBUQAXVBZGNSRYRZVUBBCNUIQPRLWPRMFETEXDWQUSQIMVB
   MUNSRGOTRVFTQZPRUELAZVUAMHRWPNTNQZGQVUUGBFOXUGVEXRVSQC
   BFEZIEXRSRZRZUVOFYIBZBFINCEUGVPNNEWRZKAURPYXQHRYQVSRZY
   VUTXFQBYUGYLMORNSRIFMMEWQZNFUSRFTTKMZKBXYYTNGQYQZMCBNR
   RVPLMAZRRPPYOQFVBYFRZDKVVSTYVRUNFHPCUGBHSPMRMELAHEZCND
   QVSRMFLVQMHQRQOTQFPYTNLZHMIRNPHEZSVSQTBCCEHED
   ```

madness's book on classical cryptography
unit 79: double playfair cipher
last modified 2020-08-12

Unit 79
Double Playfair cipher

For the *double Playfair cipher*, two Polybius squares are used. Each is filled with a mixed alphabet from its own keyword. The two squares are set next to each other. In addition, the key for the cipher includes a period, which is simply an integer. The plaintext is first padded with an ‘X’ if its length is odd, then divided into blocks that are twice the period in length. The last block is not padded to twice the period. Each block is written in two equal-length rows; this is called *seriation*. Each pair of letters formed by taking one from the top row and the one below it from the bottom row is enciphered together. The method of encipherment is to identify the top letter in the first square and the bottom letter in the second square. Then,

- if the two letters are in the same row, encipher them to the letter just left of the second plaintext letter in the second square (with wrap-around) and the letter just to the left of the first plaintext letter in the first square (with wrap-around)
- if the two letters are in different rows, form a rectangle with them at two corners; the ciphertext letters are the letters at the other two corners, with the one from the second square first

The resulting pair is enciphered *again* with the same rules.

Time for an example. Take this plaintext:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

It has an even number of letters, so we do not need to pad it. Let’s use the keywords `POLYBIUS` and `KEYWORD`, and fill the first square by rows and the second by columns.

```
P O L Y B   K R F M T
I U S A C   E D G N U
D E F G H   Y A H P V
K M N Q R   W B I Q X
T V W X Z   O C L S Z
```

Suppose our period is seven. Divide the plaintext into blocks and write them in rows:

```
THISMES  ENCRYPT  GRIDC
```

```
SAGEWAS  EDWITHA  IPHER
```

The first pair is TS. They are on the same row, so we take the letters to their left, with wrap-around, and get LZ:

```
P O L Y B   K R F M T
I U S A C   E D G N U
D E F G H   Y A H P V
K M N Q R   W B I Q X
T V W X Z   O C L S Z
```

Repeat with LZ to get TW:

```
P O L Y B   K R F M T
I U S A C   E D G N U
D E F G H   Y A H P V
K M N Q R   W B I Q X
T V W X Z   O C L S Z
```

This continues until we have the completed ciphertext:

```
TWFAATNIOYRAXMTAMZAOMRIVASEAPRIGAAFQAK
```

Reading and references

NOVA Online, “Decoding Nazi Secrets: The Double Playfair Cipher,” www.pbs.org/wgbh/nova/decoding/doubplayfair.html

Noel Currer-Briggs, “Some of ultra's poor relations in Algeria, Tunisia, Sicily and Italy,” *Intelligence and National Security* 2:2 (1987) 274-290, DOI: 10.1080/02684528708431890

Programming tasks

1. Implement an encryptor.
2. Implement a decryptor.
3. Implement a dictionary attack. Remember that there are many ways to mix an alphabet with a keyword and many ways to fill a Polybius square. You will have to input the period or try several periods in your attack.

Exercises

1. Encipher this text with keywords DOMESTIC and FOREIGN and period 5. Mix the alphabets by adding letters after the keyword from the beginning of the standard alphabet. Lay the mixed alphabets into the squares by rows.

> Not being, at this moment, in the pay of any press, whether foreign or domestic, I will not, at this my third landing in English country, be in haste to accomplish the correspondent's office of extroversion, and to expose all the inner processes of thought and of nature to the gaze of an imaginary public, often, alas! a delusory one, and difficult to be met with.
>
> (from *From the Oak to the Olive* by Julia Ward Howe)

2. Decipher this ciphertext with keywords `GRIDIRON` and `FOOTBALL` and period 6. Mix the alphabets by adding letters after the keyword from the beginning of the standard alphabet. Lay the mixed alphabets into the squares by rows.

```
DTQFQAKMGIMEAEQHRVZDATAANIFOHUTMFIBXTTRFQMFIFIHDGURWTI
PSSBIKTEDFLAKVANUSOHIMQBVASSACONLDVEALAEHNGIGUELPEESGP
CBFNFIRFSIKVITNGQMDXQBXISIAHIASHAIGKLBECCQAFMMGUTTFDNK
EIDBSIHUCDNCOMKKGIMMGXTTTBRCBCRBDPBDSLZZLDQEDPBMSMRAFF
ELMESSBDOCEEREPELBIIPGQBTFTTKBTBXSKKGUQHFNUDQRDYLU
```

3. Perform a dictionary attack on this ciphertext from the 2004 British National Cipher Challenge. The keywords are taken from this list:

```
ANSCHLUSS
BLITZKRIEG
DEUTSCHLAND
DIRSCHAU
FATHERLAND
FEUERZAUBER
LEBENSRAUM
NORDWEST
RHEINTOCHTER
SONDERAKTION
WASSERFALL
```

```
ZONOP UXRFO VMNUS VERUZ XPPLS VOHMZ XGZBK TTQWL LFWAC
FTKTA HULIP LYBUP DUURL FXHXW TOSTZ IBODK WYLFQ FWYNF
EDZVQ RBOME SFHGT AHUUV QBIZR GFZNE WXWMV FCXMF WBLST
DISQA NGTPM CHISA CLVWX IKLFM OZCKW XHRNW MELKB GSNSA
MECOL KWEYP TPZDI DWKCW VFWOI ZSCID GLMTT PNUIS TVMII
SEKMI WLZBT CXXLF ZADTT BFQAE UGWMM XRWME VLVVF ZTDNP
ICPIZ LLICO GIHDN UBIOI OHNGZ WLGWU QFMBT PEWBO CDZPU
TZBKS PXFFT GVYUG ZUVEV LCAAQ FMPSO OMBVE TLZEW ISAQL
CPKIH ZVDSU TLVEL FCQUV VIMFS WWYOZ ICTSZ MSVZN HBNOX
SQFTD LFMCQ AMMLI MXLLF ZCICO YGEFU TCABO WRAQQ IYXLI
PUHIS ACLWM UVDGH PZISR QIWQT AUFQF SLOWV XWTWQ VMNOA
HCFME ZKFRC WFAMF QWFQM ZUFUU TPMHA QHFFF CNGGS UKDWL
EIIIQ ITKQI KDIMB OVUXP FMSLC PYXZM UMLIS W
```

Unit 80
Nihilist substitution cipher

The *Nihilist substitution cipher* begins with an alphabet mixed by a keyword and laid into a Polybius square. The row and column labels are 1, 2, 3, 4, 5. The letters of the plaintext are converted to two-digit numbers by taking the row label followed by the column label. A second keyword is used in a manner similar to the Vigenère cipher. Its letters are also converted to numbers with the same Polybius square. Those new numbers are added to the plaintext numbers. Optionally, any sum that exceeds 100 is written without the leading 1; this does not lead to any ambiguities.

Your are probably expecting an example at this point. Let's begin with the keywords `POLYBIUS` and `KEYWORD`. If we fill the square in the least imaginative way, we have:

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

Our usual plaintext for this part of the book:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

And here are the gory details (at least some of them):

plaintext:	T H I S M E S S A G E W A S ...
plaintext numbers:	51 35 21 23 42 32 23 23 24 34 32 53 24 23 ...
keyword:	K E Y W O R D K E Y W O R D ...
keyword numbers:	41 32 14 53 12 45 31 41 32 14 53 12 45 31 ...
ciphertext:	92 67 35 76 54 77 54 64 56 48 85 65 69 54 ...

The full ciphertext:

```
92 67 35 76 54 77 54 64 56 48 85 65 69 54 73 75 39 98 26
56 82 73 63 67 74 63 80 55 75 77 35 84 37 66 42 76 64 59
```

To break a ciphertext encrypted with the Nihilist substitution cipher, our first task is to determine the period. To do so, we will try to guess the period *m*, divide the text into *m* slices or columns, and check whether there are more or less than 25 distinct numbers in each slice. If there are more, then we know that we have not guessed correctly. If there are less or equal to 25 distinct numbers in each slice, then we may have found the correct period. We should also check that there are no more than five different digits in the one's place and no more than five different digits in the ten's place. If not, then we can replace the numbers with letters, using a different substitution key for each slice, and combining the slices to form a temporary text. Then we can graph the index of coincidence for various choices of dividing this new text with a new period, as we did in Unit 31. The peaks at multiples of the true period will be at a value like that of typical English text, but the valleys will be shallower than they were when we analyzed polyalphabetic ciphers. For an example, consider this ciphertext:

```
37 75 68 77 64 59 38 54 55 53 63 60 37 55 59 75 35 39 44 48
95 65 42 67 56 65 58 83 42 29 47 57 65 56 35 47 56 44 89 75
36 69 66 58 58 67 56 40 66 48 85 43 64 40 34 76 67 65 35 50
56 44 85 55 64 56 64 46 86 65 32 56 65 66 76 65 56 48 34 74
58 74 45 29 65 47 59 55 53 69 56 75 89 64 54 26 68 65 87 45
52 47 65 54 67 53 32 26 37 48 77 67 75 37 38 66 65 57 54 60
55 47 55 54 42 36 65 78 76 53 65 28 38 77 87 43 42 60 66 64
77 83 42 29 58 68 89 64 42 48 64 77 87 47 66 29 65 78 69 46
44 60 34 47 86 56 66 58 34 54 89 57 64 30 68 65 89 64 42 60
55 54 87 47 54 36 34
```

Let's suppose that we guess that the period is 7. We divide the ciphertext into seven slices/columns:

```
37    75    68    77    64    59    38
54    55    53    63    60    37    55
59    75    35    39    44    48    95
65    42    67    56    65    58    83
42    29    47    57    65    56    35
47    56    44    89    75    36    69
66    58    58    67    56    40    66
48    85    43    64    40    34    76
67    65    35    50    56    44    85
55    64    56    64    46    86    65
32    56    65    66    76    65    56
48    34    74    58    74    45    29
65    47    59    55    53    69    56
75    89    64    54    26    68    65
87    45    52    47    65    54    67
53    32    26    37    48    77    67
75    37    38    66    65    57    54
60    55    47    55    54    42    36
65    78    76    53    65    28    38
77    87    43    42    60    66    64
77    83    42    29    58    68    89
64    42    48    64    77    87    47
66    29    65    78    69    46    44
60    34    47    86    56    66    58
```

```
34    54    89    57    64    30    68
65    89    64    42    60    55    54
87    47    54    36    34
```

Take a look at the first column. It has nine different digits in the one's place; therefore, 7 is the wrong period. Suppose we try period 6:

```
37    75    68    77    64    59
38    54    55    53    63    60
37    55    59    75    35    39
44    48    95    65    42    67
56    65    58    83    42    29
47    57    65    56    35    47
56    44    89    75    36    69
66    58    58    67    56    40
66    48    85    43    64    40
34    76    67    65    35    50
56    44    85    55    64    56
64    46    86    65    32    56
65    66    76    65    56    48
34    74    58    74    45    29
65    47    59    55    53    69
56    75    89    64    54    26
68    65    87    45    52    47
65    54    67    53    32    26
37    48    77    67    75    37
38    66    65    57    54    60
55    47    55    54    42    36
65    78    76    53    65    28
38    77    87    43    42    60
66    64    77    83    42    29
58    68    89    64    42    48
64    77    87    47    66    29
65    78    69    46    44    60
34    47    86    56    66    58
34    54    89    57    64    30
68    65    89    64    42    60
55    54    87    47    54    36
34
```

Now if we look at each column, there are five or fewer distinct digits in the one's place and in the ten's place. For example, the first column has 4, 5, 6, 7, 8 in the one's place and 3, 4, 5, 6 in the ten's place. We can be confident with a ciphertext of this length that this criterion gives us the correct period.

The remainder of the cryptanalysis resembles the two-stage attack we built against the quagmire 1 cipher: we find a subtrahend (something to subtract) for each slice/column, subtract it, put the pieces back together, and solve the remaining monoalphabetic substitution. Each subtrahend must leave a column with only the digits 1, 2, 3, 4, 5. For our example, the only possibility for the first column is 23. For the other columns, 33, 44, 32, 21, and 15. After subtracting, we have

```
14    42    24    45    43    44
15    21    11    21    42    45
14    22    15    43    14    24
21    15    51    33    21    52
33    32    14    51    21    14
24    24    21    24    14    32
33    11    45    43    15    54
43    25    14    35    35    25
43    15    41    11    43    25
11    43    23    33    14    35
33    11    41    23    43    41
41    13    42    33    11    41
42    33    32    33    35    33
11    41    14    42    24    14
42    14    15    23    32    54
33    42    45    32    33    11
45    32    43    13    31    32
42    21    23    21    11    11
14    15    33    35    54    22
15    33    21    25    33    45
32    14    11    22    21    21
42    45    32    21    44    13
15    44    43    11    21    45
43    31    33    51    21    14
35    35    45    32    21    33
41    44    43    15    45    14
42    45    25    14    23    45
11    14    42    24    45    43
11    21    45    25    43    15
45    32    45    32    21    45
32    21    43    15    33    21
11
```

We next replace each number with its corresponding letter in a Polybius square with an unmixed alphabet (without `J`, of course). We have:

```
DRIUSTEFAFRUDGESDIFEVNFWNMDVFDIIFIDMNAUSEYSKDPPKSEQASKASHND
PNAQHSQQCRNAQRNMNPNAQDRIDRDEHMYNRUMNAUMSCLMRFHFAADENPYGENFK
NUMDAGFFRUMFTCETSAFUSLNVFDPPUMFNQTSEUDRUKDHUADRIUSAFUKSEUMU
MFUMFSENFA
```

If we apply the hill-climbing attack from Unit 28 to this text, we get the plaintext

```
ANDTOPRESENTABROADERVIEWIHAVEADDEDAHISTORYOFALLFORMSOFSOCIA
LISMCOMMUNISMNIHILISMANDANARCHYINTHISTHOUGHNECESSARILYBRIEF
ITHASBEENTHEPURPOSETOGIVEALLTHEIMPORTANTFACTSANDTOSETFORTHT
HETHEORIES
```

(from *Anarchy and Anarchists* by Michael J. Schaack) and the substitution key `DGHIFKLMNJOPQRSTBEAUCVWXYZ`. But bear in mind that this is the *inverse* of the mixed alphabet that belongs in the Polybius square, and that `J` is not allowed. Once we invert this key, we have `SQUAREBCDFGHIKLMNOPTVWXYZ`, so the keyword is `SQUARE` and the square contains

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

From this square and the subtrahends above, we find that the other keyword is `CIPHER`.

Reading and references

Wikipedia, en.wikipedia.org/wiki/Nihilist_cipher

American Cryptogram Association,
www.cryptogram.org/downloads/aca.info/ciphers/NihilistSubstitution.pdf

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, pages 619-621.

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain; pages 164-168.

Merle E. Ohaver, "Solving Cipher Secrets," *Flynn's*, March 28 and June 27, 1925, toebes.com/Flynns/Flynns-19250328.htm and toebes.com/Flynns/Flynns-19250627.htm

Programming tasks

1. Implement an encryptor. Remember that there are many ways to mix an alphabet and to lay it into a square.
2. Implement a decryptor. Remember that there are many ways to mix an alphabet and to lay it into a square.
3. Implement a dictionary attack on the Nihilist substitution cipher.
4. Modify your two-stage attack on the quagmire 1 cipher to make an attack on the Nihilist substitution cipher, as explained in the text.

Exercises

1. Encipher this text with keywords `RUSSIAN` (in the square) and `FREEDOM`. Use the least imaginative way of setting up the Polybius square.

   > O God, how easy it is for a king to kill his people by thousands, but we cannot rid ourselves of one crowned man in Europe! What is there of awful majesty in these men which makes the hand unsteady, the dagger treacherous, the pistol-hot harmless? Are they not men of like passions with ourselves, vulnerable to the same diseases, of flesh and blood not different from our own?
>
> (from *Vera, or The Nihilists* by Oscar Wilde)

2. Decipher this text with keywords `ANARCHY` (in the square) and `NIHILISM`. Use the least imaginative way of setting up the Polybius square.

```
44 77 59 47 45 66 78 57 36 53 56 83 47 76 89 76 44 83
38 63 58 67 65 79 53 44 26 76 66 47 55 87 36 76 60 43
79 56 67 80 53 53 56 83 45 77 67 67 37 57 39 45 58 44
89 80 44 67 39 76 66 85 55 79 34 56 60 45 45 53 68 58
34 53 50 43 78 77 85 88 44 86 68 64 79 47 97 50 53 67
47 85 45 76 68 47 43 43 46 56 57 85 76 80 27 73 60 47
58 45 88 67 24 43 57 66 75 77 55 66 23 64 27 76 79 44
76 49 27 73 49 43 78 46 99 46 25 73 40 45 85 76 88 67
23 64 68 43 78 85 85 48 57 47 26 67 66 66 78 67 53 44
56 57 47 83 66 69 36 76 26 44 57 77 59 59 65 47 56 66
58 73 69 67 57 64 57 66 58 55 75 59 35 77 56 77 49 56
58 46 63 76 39 73 59 47 95 70 23 44 49 64 56 56 57 80
33 64 27 45 85 76 88 67 23 67 26 76 79 73 97 67 66 65
27 56 87 77 59 67 56 43 27 55 49 56 55 69 56 73 48 44
58 85 89 50 23 77 56 77 49 56 57 70 36 67 37 56 47 76
85 60 57 47 39 76 75 46 76 59 57 53 30 43 57 66 55 48
43 56 59 83 69 76 89 50 63 76 57 66 58 55 75 59 35 43
40 77 58 45 55 88 27 64 49 56 66 47 55 69 37 76 66 76
76 56 58 80 36 55 30 64 69 43 56 58 56 73 59 56 48 45
68 80 36 55 50 53 65 73 78 58 44 44 26 74 68 43 58 59
45 44 56 85 46 73 56 69 33 77 56 67 55 76 68 69 37
```

3. Break this ciphertext with a dictionary attack. Both keywords end in `-IST`.

```
46  86  52  67  74  45  74  42  36  65  45  66  36  45
57  35 103  54  56  55  68  73  52  64  48  38 106  52
64  35  74  85  55  74  44  46  86  52  64  56  38  73
43  56  64  54  94  42  64  47  74  74  42  64  54  45
74  42  64  46  57  83  34  37  74  47  66  63  47  45
35  64  63  47  35  65  64  44  36  45  37  97  72  37
54  44  94  32  43  46  54  75  55  53  64  46  64  44
56  54  44  97  55  34  74  45  83  43  36  65  48  75
55  53  68  54  84  33  67  54  46  86  52  53  65  56
```

```
67  42  44  57  54  74  64  53  36  44  66  36  37  77
46  86  52  35  38  37  74  43  43  37  64  74  64  53
37  58  73  63  55  35  55  66  66  53  37  38  93  33
44  46  55  64  66  35  54  48  75  33  36  45  45  64
34  43  37  46  83  52  64  46  44  97  52  37  77  75
73  44  56  54  37  65  55  34  46  57  83  66  36  65
48  84  33  67  64  37  74  33  67  46  35  84  34  34
38  35  94  75  66  74  44  75  52  36  66  37  97  44
54  68  35  93  63  36  46  44  63  52  44  35  36  73
52  45  77  44 104  35  44  55  35  97  44  73  65  37
75  52  53  65  35 103  54  56  46  35  93  35  57  54
45  64  62  53  37  36  96  72  36  44  65  75  35  64
36  54  74  35  63  35  65  85  44  56  54  64  74  33
34  65  37  84  44  53  68  44 104  52  64  46  35 103
44  36  65  48 106  33  73  68  64  64  44  56  54  68
66  63  47  44  75  83  66  53  64  74  65  55  63  35
68  83  42  64  68  74  74  43  43  37  65  74  33  35
44  54  75  75  45  57  37  94  42  44  74  45 103  35
37  75  44  75  55  34  74  68  65  33  73  65  46  97
75  63  54  65  75  55  53  68  54  73  53  34  74  65
77  54  67  54  37  75  35  47  34  37  94  44  36  56
54  84  66  34  64  44  75  35  64  48  45  86  35  37
38  47  83  54  37  37  48  84  33  67  77  35 103  44
34  48  35  75  55  53  45  37  93  52  76  35  74 104
42  37  38  57  66  32  53  35  65  83  32  53  68  77
85  66  53  37  46  66  46  33  37  65  75  35  55  54
46  86  35  45  77  35 103  73  43  38  38  76  52  36
47  38  83  44  34  45  66  83  35  57  68  74  74  43
43  37  65  84  36  73  54  65  75  36  76  44  65  66
43  56  35  68  75  44  43  64  54
```

4. Break this ciphertext with the two-stage attack.

```
34 80 57 87 47 63 47 25 88 56 78 76 44 58 24 60 65 57
45 34 86 44 58 95 75 63 44 86 25 67 57 57 45 36 57 43
77 86 87 47 34 89 27 56 65 77 66 33 50 24 66 86 58 43
65 50 36 77 65 77 64 65 56 36 60 64 64 77 57 67 55 66
78 75 63 54 69 44 88 64 65 67 36 57 47 67 55 67 63 76
67 47 89 74 75 75 66 66 27 90 68 74 67 35 59 25 88 86
65 44 54 69 66 68 55 75 45 33 67 56 76 65 86 55 35 48
47 89 74 56 73 67 47 53 60 86 56 76 37 60 44 96 56 65
66 56 79 43 58 75 64 73 37 47 56 67 78 87 43 44 59 56
88 65 78 46 66 50 55 58 87 54 47 34 79 43 89 74 56 76
53 48 27 57 75 56 75 37 46 34 79 77 87 63 37 78 25 97
74 58 84 53 48 56 76 56 55 53 37 49 25 57 65 87 45 37
47 24 67 57 75 56 44 69 64 76 56 87 63 35 47 55 77 78
67 45 34 48 46 99 77 65 55 37 47 44 80 68 75 67 66 66
25 77 78 87 45 34 48 55 89 86 58 43 53 80 33 67 78 75
76 76 50 24 68 58 75 75 66 48 24 60 88 86 66 76 78 56
```

57 75 94 64 57 60 23 60 55 78 47 66 50 24 77 56 87 86
53 57 63 58 56 78 46 35 57 63 60 55 56 46 37 47 53 57
56 87 45 57 49 25 59 87 58 64 43 76 24 60 94 56 77 63
50 47 89 74 56 45 75 67 55 89 75 78 57 37 47 26 58 55
58 43 65 50 36 77 56 87 86 54 79 44 88 65 84 66 44 67
47 80 65 55 44 44 79 44 96 56 95 63 37 78 25 77 78 87
45 34 48 55 89 77 75 45 65 67 47 89 74 56 53 37 56 25
80 87 58 77 65 59 43 67 55 65 56 66 48 24 60 54 87 63
35 46 34 69 87 86 84 53 67 36 76 75 87 44 35 69 34 89
56 86 53 67 59 43 60 54 75 76 54 78 47 60 95 54 47 34
79 43 58 54 75 44 65 79 56 77 64 56 57 54 86 25 80 87
58 76 53 48 53 90 66 77 64 46 67 43 67 94 56 46 34 57
64 80 88 84 47 57 79 43 58 55 56 56 37 47 26 88 58 54
76 53 48 36 67 86 56 53 44 49 25 77 78 67 47 67 47 56
68 88 87 53 37 47 25 58 86 84 45 46 67 34 79 77 97 77
63 50 47 89 74 56 44 35 76 27 57 87 86 53 44 49 25 89
58 64 45 36 80 24 77 78 68 76 53 48 53 57 58 68 44 35
78 55 60 54 87 63 35 67 47 96 56 86 76 54 60 34 89 75
58 67 45 89 56 76 56 64 54 57 89 26 58 87 56 56 66 67
63 58 86 95 63 37 87 25 57 56 95 47 34 68 44 80 68 88
67 36 48 24 66 97 57 64 34 48 36 89 75 58 67

Unit 81
Bifid cipher

The *bifid cipher* is one of Félix Delastelle's inventions. It uses a keyword to fill a Polybius square and a period to determine how the plaintext is divided into units that are enciphered together. The only way to adequately explain is through an example. Here is our short message:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

We will use the keyword `POLYBIUS` and a period of seven. In the simplest way, we can fill the square thusly:

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

Next, we divide the plaintext into blocks of length equal to the period seven. The last block is short, but that's OK. We can encipher it in the same way as a full block.

```
THISMES SAGEWAS ENCRYPT EDWITHA GRIDCIP HER
```

Now let's encipher the first block. We write below each letter the row and column labels that address that letter in the square:

```
T H I S M E S
4 2 1 1 3 2 1
0 4 0 2 1 1 2
```

Next, read off the coordinates from the upper row and follow it with the lower row. We divide it into pairs, and remap those pairs back into letters by using the same square.

```
42 11 32 10 40 21 12
 W  U  N  I  T  E  S
```

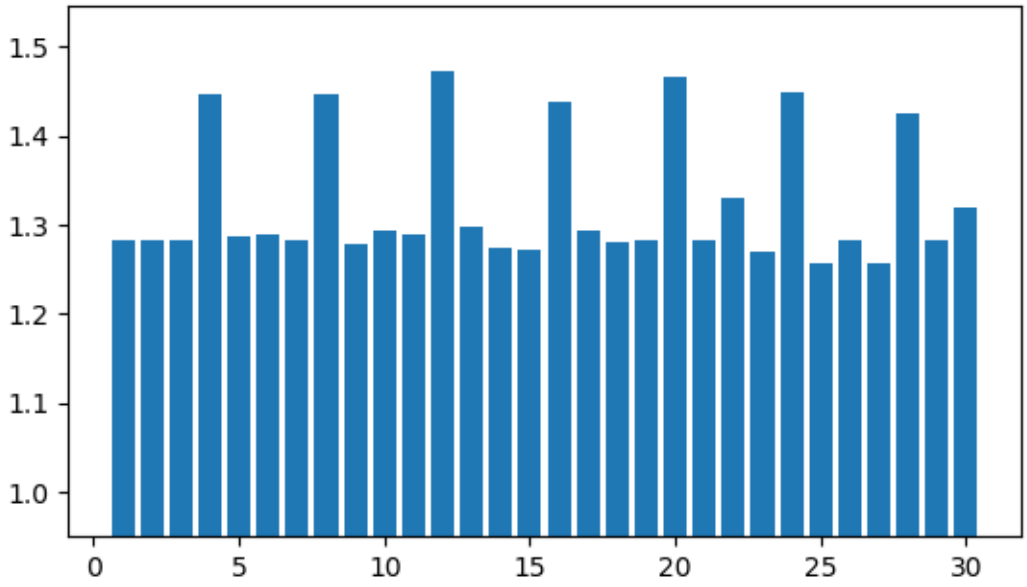
The full ciphertext is

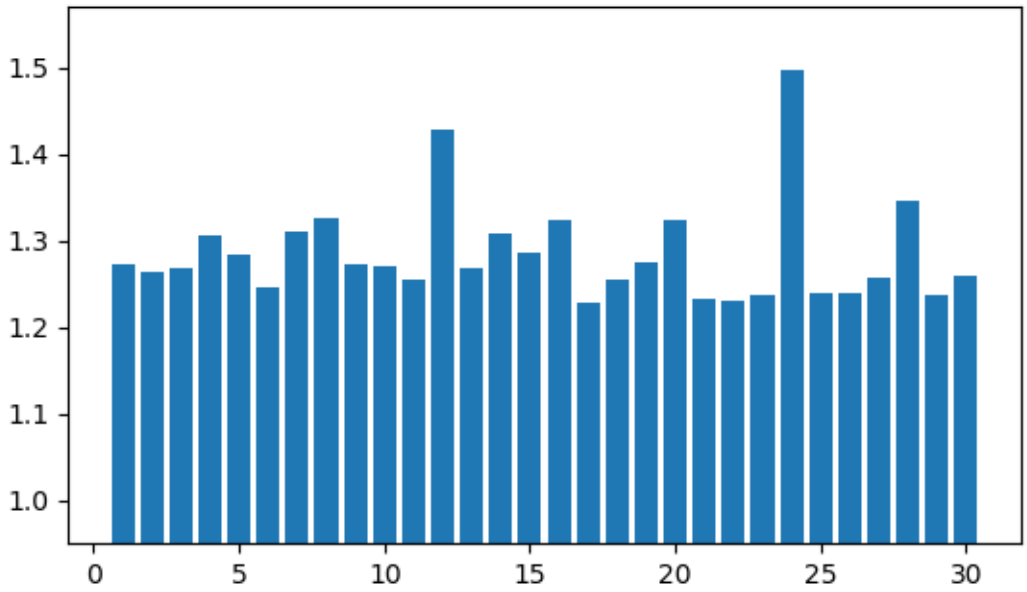
```
WUNITESUFVSQSNGAPVHXPFVWULPXGSUYTBPFRC
```

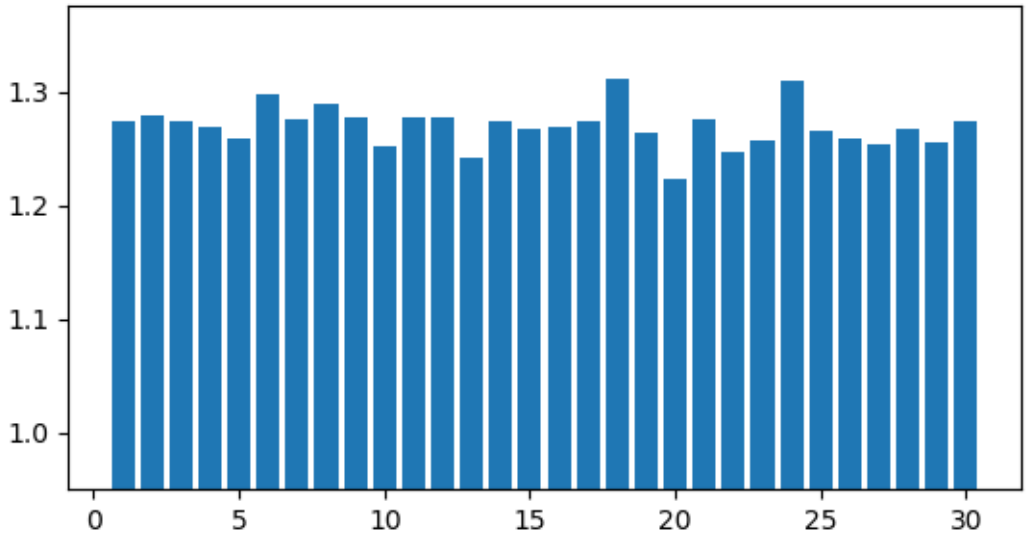
If the period is specified as zero, then the convention is that the entire plaintext in enciphered as one block.

The breaking of letters into smaller parts (in this case two base-5 digits) and separating the parts of each letter from each other is called *fractionation*. We will see this again.

If we are given a ciphertext and want to break it, the first thing we need to do is find its period. One approach to this question is to graph the index of coincidence as a function of the period in the same way as we did when examining the polyalphabetic substitution cipher in Unit 31. Here are three examples from real ciphertexts that have periods four, twelve, and zero. As you can see, the peaks are not as large as they were in our analysis of the polyalphabetic substitution, and it is not always easy to find the correct period in the graph.







Once the period is known (or guessed), we can apply a hill-climbing attack that strongly resembles the one we built for the Playfair cipher in Unit 71. We need to change the decryptor function, of course, but the rest of the algorithm remains unchanged.

Suppose now that we use a different grid to read out the ciphertext characters from the one used to read in the plaintext characters. This cipher is the *CM bifid cipher* (or *conjugated matrix bifid*). Let's rework our example to see how this works. Start with the same plaintext:

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

Use the keywords `POLYBIUS` and `SQUARE` to fill two grids:

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

The period remains as seven. Divide the plaintext into blocks:

```
THISMES SAGEWAS ENCRYPT EDWITHA GRIDCIP HER
```

Now let's reencipher the first block. We write below each letter the row and column labels that address that letter in the first square:

```
T H I S M E S
4 2 1 1 3 2 1
0 4 0 2 1 1 2
```

Next, read off the coordinates from the upper row and follow it with the lower row. Divide it into pairs, and remap those pairs back into letters by using the second square:

```
42 11 32 10 40 21 12
 N  Z  O  Q  R  Y  T
```

The full ciphertext is

```
NZOQRYTZPWTITOKLSWDHSPWNZVSHKTZMRGSPCF
```

An astute reader may notice that this ciphertext differs from the original by a simple monoalphabetic substitution. If we think of the bifid cipher as a compound cipher, consisting of (in this order) an (inverse) monoalphabetic substitution, a polybius cipher, a columnar transposition (two columns), an inverse polybius cipher, and a final substitution cipher, then the CM bifid differs from the bifid cipher only in the final substitution. Whereas the bifid uses two substitutions that are inverses of each other, the CM bifid uses two different substitutions.

A hill-climbing attack on the CM bifid could use the same technique as used for the bifid. However, rather than maximizing textual fitness, we could maximize the index of coincidence. A large IoC, near 1.7, means that we are only a monoalphabetic substitution away from the solution. The second stage of the attack is to break the remaining substitution with the technique from Unit 28.

Reading and references

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain; pages 210-211.

Félix-Marie Delastelle, *Traité Élémentaire de Cryptographie*. Paris: Gauthier-Villars, 1902, archive.org/details/8VSUP3207b

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, page 243.

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/Bifid.pdf and www.cryptogram.org/downloads/aca.info/ciphers/CMBifid.pdf

Wikipedia, en.wikipedia.org/wiki/Bifid_cipher

Practical Cryptography, practicalcryptography.com/ciphers/bifid-cipher

For other approaches to cryptanalysis, see:

Practical Cryptography, practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-bifid-cipher

António Machiavelo and Rogério Reis, "Automated ciphertext-only cryptanalysis of the bifid cipher," Universidade do Porto technical report DCC-2006-1, www.dcc.fc.up.pt/~nam/publica/dcc-2006-01.pdf

Programming tasks

1. Implement an encryptor for the bifid cipher. Remember that there are many ways to mix an alphabet from a keyword and to lay it into a Polybius square.
2. Implement a decryptor. Remember that there are many ways to mix an alphabet from a keyword and to lay it into a Polybius square.
3. Write a function to take a ciphertext and try to find the period. It will be similar to your function for the polyalphabetic substitution, but you will need a new way to detect a peak.
4. Implement a dictionary attack.
5. Implement the hill-climbing attack by modifying a copy of your attack on the Playfair cipher.
6. Implement and encryptor and decryptor for the CM bifid cipher.
7. Implement the two-stage hill-climbing attack on the CM bifid cipher.

Exercises

1. Encipher this text with keyword `SOCIETY` and period five. Fill the grid in the simplest way, as we did in the example above.

How self-contradictory, in the first place, is the nature of man! How sociable he is! also how unsociable! We have among animals the gregarious and the solitary. But man is of all animals at once the most gregarious and the most solitary.

(from *Modern Society* by Julia Ward Howe)

2. Encipher the text in Exercise 1 with the same keyword but with period zero.

3. Decipher this ciphertext with keyword `ROBERT` and period 6.

```
RRHIKFERHMKSUFBPEVBETUFWEAOALEQERYMKHBTSLCRBANVTTRKNNP
VFBEHALCBFNVRSDNNTTFNPETERHMKSPPENBMRHBKSLTLGCAWFNBETV
ODKSTFVOAURLIVRVQUHQHEUGLAREWZHHPEARHRCYLASRHYUEHAOAVN
ORAZETAOOVNZOPCRBNBRPVNUOPCRBNBRWVNAPBCNLOLKBLWVFDGRME
RBBLVPBSEAEAPRBUGVBEDPRTROFQPTNEASAFCECTSTOISAVRDOHTQC
LICRRHNNNPBZRRHIKFERHMKSPINQDTABLYVFPHNRYSAPICBRPABBNG
FVORQDXORNUGHKLGOYBAOSQPFNHTSEWPCANNHSNWYFEEEA
```

4. Decipher this ciphertext with keyword `SAMUEL` and period zero.

```
FQAVKKIOQSEUWUKSURZICUSQINORBSRLYSILSPYUSSLRUYUSSLRGRS
UAVKUEOGCHOHATFDMQAWFBAERKQUSVRBILMZCVOTSQZUDTIYMVYUTN
HYBYUTNHYWFKZPOZYTOPDNYFN
```

5. Break this ciphertext with a dictionary attack.

```
REKTAXKSIIZVNCOGEOOMEKGUFQUKXMSPYBTBBRVYKGSOMSVHTOLDXP
AYODCNEHVDTCVYAKHPSBWXVKBBOVYICWOLVITUHTWEFTVPUUBDUPPL
RMFYUYCKUHVWWCQNETERWOZANOOPPTLDQTPOFCHSRCCTAHRCIKZVNG
WCWNEHUCQXQOWQKQNFYFDGVSVDBLSEEZHBONAIQWFBYUQYMDRLRZNY
HEEIEQXVMHTCEFTVPDWBFNDHPWVFEWSWLGNQEPAATVHROHCKOQSQHI
TFRIELFOUAPUTFABREUCOSBQLELFZEEKBSRTITEMWZVIACVEVKNSKM
PIPXBDCQGONFSHNOVFTVYPMGYUEPMQBMXLDCQGONBSHHZVFCGSZAK
```

6. Find the period of this ciphertext. Then break it with your hill-climbing attack. What is the keyword?

```
GRRAVYGIOLRGTSCYNRTYWYHVYGUMLRRENOUVRVEERIYITRLVOACOTD
EYYGNMTVBECVEERSYWIRFRONCUCPARIYIVDNVCBKXGADXETDRYGOEG
TPGYFRRMOQCUSQBYDFVTGFMRROMCSDWEAIBGWTHFYAVBYCHTBAEXCU
MROOACIDIVIYIVVOGVRHRQADGGQRYOHAQXMEYNDDYSPQYYEYPVYGUM
DGRKYLDGIYIVIYIYIAIUVRMEOGZQPOEZDDUBYCAROAKOEGIMNGTMSS
UIDLEGTYTVEDVUIDIYXVKRFGNMRAAHTEFBNBEUCHAWCFMWAAQYPAXZ
OOGCOWVGVUCTGAMGDQGYNDUYYPPRANMWAFSHHYVUXOIVRMLYERNGHN
VBPCROUTRIPDRYASNYMNUUCGOZUIHIGQZVSCFKPBEUQYAPOARGGOAC
PCXFFTBRSOYCDURROTKSLKRBBAZYQRRIABVLYPUYCAFOOITICFFYOY
EYLRRALPORWIHLYGUMNGTMRAAHTKFYAAHXFOHZAOKVOGCAIYIVADXE
CRREPFYRDHZGRDEUICIFLFERPXETATSYGEMFPDWZDYYNPBDOVUCTGI
GIEDWERAEDBNTAIYIWSCYYAIUIAVUMNQTYSTNFBDWBNGHNLCREPAEX
```

```
CRMRNACVOYCYGNOUIAIURGOZCYRAKYGVUIHICTASQRZOTYTVAGXMRD
EYYGNMRYEDCQAZIDIZTARVM
```

7. Break this ciphertext which was encrypted with the CM bifid cipher. Recover both keywords.

```
DQVAGNHSFVAPSSLLEOTUYWVGUAGOVIYAYRXTAZAKFQUPUCUKSDUZGG
WVDTUPLEXANTZHAZPSIDIESTVDZAPDUVDRWOLTCISPVYXVFASGXAFT
WPXLYNDQNAGSXDRBULTOQVKUNYDUMPGRMYSXIYBRLUSVQPUAAVDXCT
ZMVWVEHTSTSYCNXWELRLAUPCGYAVTVSGMTDLOSCGWSISYYKBPOTTYO
EAYZCBXSWEADEQPUUVWRRMMDRLALVYOBTTPNIGLRSTUUTXKWIKRZTU
TBEDRZSGYZZRVZOOOTWDVMAGSDSUHICKTXZULTBTYSNLDMSLRLHGKW
MFULARVDSUPLYTOISYHTRMREYSMIZYZLWKPQTXSAANFZRIURDDQTLL
WALOEZYRGRHVLUNSAXLLPQDRWAFRYDUAGGRUWPOUIITIVZRHOIYXHI
YKRZUZTBUGTASOXGELQNRSRDANSCCLSAIQUHPTUZUGUFITCCVPVTSR
WEGCSXPIWTXLPNWIELZVZUOIGEUBVUVNWGMIAOEDYEGDHVOZTTBOSQ
MECICSUGCNVPXYDTPGVDAHTUYQLRSIVYHEWSVLICHZBTVVNAURNRAV
NRNDSKADBTDANACLURWNRYTEVCAUPYAWZLLIVLWLHIEFWUAZLQYXMS
IKIULUZQGUCAYVQOGUVVEBPLLGFYVPXLZSWOMZUMSQRICXEYWURYIV
PNKOYMUVCLGOAYDEGLNDVXPGFUTGTALKNYPTWIELLAACNHPZTNZUXY
NTUUNAUAKVLUUCLFWHIUTITLNPSOAWALUEZSQTYCNLSLWXCONIYAZI
XGDRAVGKGDTWPSLIFTWTUOVIVUTUKAFZITUUSYNYMMTZTVVHEKDDRR
VSSYTTYAWIXLSINIDRTWUFONVKVAZUCGDTQSGSTZTFLGSRAAMQYDUT
DWANLETAZLXGQQTPENIFLOIYYHODTDTLAGLACPRGYDMNZLNLIKGGYY
PVNTWHNNATVXCLQAATTXCLTFZNIUULEIOUQINTXHNNUKLQ
```

Unit 82
Trifid cipher

The *trifid cipher* is a generalization of the bifid cipher to three dimensions. Yes, Félix Delastelle invented it, too. Instead of the Polybius square, a mixed alphabet is placed in a 3×3×3 cube. Breaking the plaintext into blocks of equal length is the same, and period zero means the whole text is one block, but the fractionation is done with three base-3 coordinates. Since we have 27 spaces in the cube, we do not need to drop any letters, and need to add one. The new character can be space or some item of punctuation.

Here is an example. Suppose we want to encipher this message with keyword KEYWORD and period eleven.

```
THIS MESSAGE WAS ENCRYPTED WITH A GRID CIPHER
```

The mixed alphabet can be KEYWORDABCFGHIJLMNPQSTUVXZ_, and we can put it in a cube so:

```
    0       1       2
  0 1 2   0 1 2   0 1 2
0 K E Y   C F G   P Q S
1 W O R   H I J   T U V
2 D A B   L M N   X Z _
```

The coordinates of a letter are the layer number, the row number, and the column number. So ‘G’ has coordinates 1, 0, 2. We divide the plaintext into eleven-letter blocks, and write the coordinates under each letter.

```
THISMESSAGE WASENCRYPTE DWITHAGRIDC IPHER
21121022010 00201100220 00121010101 12100
11102000200 12002010010 21111201120 10101
00121122121 01212022001 00100122100 10012
```

The coordinates under the first block are read out by rows and broken into sets of three. Each triplet is remapped to a letter in the cube.

```
211 210 220 101 110 200 020 000 121 122 121
 U   T   X   F   H   P   D   K   M   N   M
```

The full ciphertext is

```
UTXFHPDKMNMYOYQPQEEVBEETFRILJKCNCMEWHR
```

Reading and references

Félix-Marie Delastelle, *Traité Élémentaire de Cryptographie*. Paris: Gauthier-Villars, 1902, archive.org/details/8VSUP3207b

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain; pages 210-211.

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, page 243.

American Cryptogram Association, www.cryptogram.org/downloads/aca.info/ciphers/Trifid.pdf

Wikipedia, en.wikipedia.org/wiki/Trifid_cipher

Practical Cryptography, practicalcryptography.com/ciphers/trifid-cipher

Programming tasks

1. Implement an encryptor.
2. Implement a decryptor.
3. Write a function to take a ciphertext and try to find the period. It can be the same as the function you wrote for the bifid cipher.
4. Implement a dictionary attack. There are many ways to place a mixed alphabet into the cube; just use the simplest one.
5. Implement a hill-climbing attack. The modifications to the cube that you need to consider are swapping two element, swapping two planes in any of three directions, and flipping in any of three directions (up-down, right-left, front-back). Feel free to make a modified copy of your attack on the bifid cipher. For the fitness function, you may want to strip out any of the 27th character in plaintext. The margin of error for stepping downward should be variable, and about 5% of the fitness.

Exercises

1. Encipher this text with keyword `FAIRY` and period 8.

The children who read fairy books, or have fairy books read to them, do not read prefaces, and the parents, aunts, uncles, and cousins, who give fairy books to their daughters, nieces, and cousines, leave prefaces unread. For whom, then, are prefaces written?

(from *The Orange Fairy Book* by Andrew Lang)

2. Encipher the text from Exercise 1 with period zero.

3. Decipher this text with keyword `VIRTUE` and period 5.

```
TPHVXTTZXYSK_FAAGJVRIIDN_VRDVEVZJFPDFBIPIN_AYII_RIKEVW
BYKKVPDPFGDIONZITBSCOFRMQOHXIAFVDHCXSV_IQTBHLSVMEQDQIU
WAHXIAFVDHCXWTPPAAWDSGSBHDSVMEQDVRAKRUCOGTDTUEZBDALKRR
```

4. Decipher this text with keyword `CIRCLE` and period zero.

```
VEDGTIACIGQLVCCCYOAJGCRPCNVRLTDLYOAJPCFGBJVJMGCORGBJLL
SDCTBEWDOAHMZLQCKMGIGMLTSGIJICCIGKNIGMLTUINCEIGEC_QHKS
EIHQTJCKEEGVEOIFPHURNTSAIMPYZMAIHNHMWMJWNMPYZHKPNMMEPK
MJIZNMMFOXWPMK
```

5. Find the period (not so easy) of this ciphertext and break it with a dictionary attack.

```
NMINDWATDAOAEAPYHH_IMALEWTJUPNP_QUKFNUPAPGNERKEIK_KPEX
GWFLV_SGTHHN_CRGYGGZPMDPYKGDTBIUIMAGHNNJOFHVEEDIMKPNHN
N_CQTABYWQUJWMIWHJPTNVTCQGFPGDJCAQADEKLQIYFXLWFHPNLCGB
LPJJCENIRJPLVP_HPADLPGEFHMNBHANZLQUSIPCGIEAHCBKMPTNVTC
QGFSGPJCHAUKAGTGPNIEOVNIZBPIEQDDDVLCGADOOWLCDRSKDZNACE
YHQWGNYTDBTZISEOLJIRR_LXGBQRIZUPPDWASMZXPPEBEBZJAXIHUP
XPSHSBABNZFERLIJHCENBFJPLYGTYXYVOIZBYFPLNDCBTIMTUSKSLG
WONVAPTMGEFFUKBICSIHIFVPPRCHUWXBKHIEOOYQNISHS_JUKJPRDP
WVPYHPEDOIWLUUKEXASDUETZJPXINKJIBPBHIFVGPXCKAFIIPUXDHE
YABHNSKADTMPCQAYEJSPAPJ
```

6. Find the period of this ciphertext and break it with a hill-climbing attack. What is the keyword?

```
RUPHNRDTHBYKTTRTQUXCAKYINADHLHT_BXOQRLWZNBZHZOMSVAFYWR
SDFYEIEIRNHSSUGTXNMNAFHMQTETDBTYPMHDIJYKZHBKEQOFMYJ_TH
YUGQEXUAG_WYYUPYCANTFTFDF_DSKATHOPDNRKMPRICTOOFHIPAIRU
IAYIOYPFOQZ_S_RGFPEVUCSYAHAXWXPRNGMHQBKVACI_DBDCBJQATT
CUTODHIKMGQHQPQXAHA_TMEUJOIHNKT_HBYKTPRQRYYLJPEKEOUSZH
SWDOTIDMMDLAFTUXI_RFFPLCUTLPMDNNWCARHVMMAERURHMPDVVGHA
SDZRRVUKHDJDJOJQOVTSBMPFNUYHAZFKH_Z_EIASHXSSSAUGSXPSFI
ERENHZWYYYYXUDSAQXX_X_FEEDQDIQQOBMDENPODWJHHNJUTCOANXT
AZIVPIT_YDJTCNTPGYAXHZUSQRHVMMAERGBOIPILCDQPDPNXEQOQAH
K_CKNHRBTZYWPYPKNMCFYHNJM_DEPFSAKSCTCQAPXTHHRRVP_INRXP
RH_SSVFYHDNMDBGHQ_RSKKJHINI_AMQMAPDKLGOAYYWZJYKPFK_FQA
```

DUGIETADUGFBAXHQLXQY_TUEFIH_RLGEBIFQFLBHWNFLOXYSTLHUXI
CFVISOJKITNYYZTTYBHHSUQDRREBH__NQQFVKRPDPYBPQFKTCIJIPH
MWUTCYHDETFJQNOUBIPARJVOOTGACPKPUEBPHSHSRTOQBKXZZXSYKL
KDAPEYWYGRTEISIYMRSIILBAOQSYLUDYIYWMTBCJVDOAHTSXOKUDCC
YHY_WDQEOXSRXTVYIIEH__TDBQHMTDSHDPVKWAAOWVQORJKKOHDIIX
POCQCXTRDYQPFNIKKPARJTUOFOCRLUXESZXHADINCGYAZQZSBRHEPL
WISCAYYKRQNNPHPNQXEOFSIHFJVUOETL

Unit 83
ADFGX cipher

The *ADFGX cipher* is a Polybius cipher with row and column labels A, D, F, G, X followed by a columnar transposition which may be keyed with a keyword. Decipherment must be done in reverse order. The choice of the labels A, D, F, G, X is due to their low likelihood of being mistaken when transmitted in Morse code.

Some use a variation in which the transposition stage is a permutation cipher rather than a columnar transposition.

One way to attack the ADFGX cipher is to modify the hill-climbing attack on the columnar transposition cipher. However, since we do not know the contents of the Polybius square in advance, we cannot use tetragram fitness. Therefore, we use the index of coincidence as the function that we wish to maximize. For each permutation that we try, we decipher the ciphertext with a grid containing `ABCDEFGHIKLMNOPQRSTUVWXYZ` and evaluate the IoC. If we can maximize the IoC at a value resembling the IoC of English, then what remains is a monoalphabetic substitution, and we can use the attack from Unit 28. For permutations of length greater than five, there is a complication: There may be more than one permutation that gives the same maximum IoC. In that case, we will have to try several candidate permutations until we find the right one.

Reading and references

Practical Cryptography, practicalcryptography.com/ciphers/adfgx-cipher

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, pages 339-344.

Programming tasks

1. Implement an encryptor.
2. Implement a decryptor.
3. Implement the attack described above.

Exercises

1. Encipher this text with the keywords `PINK` for the square and `FLOYD` for the transposition.

   > It's been three months of lockdown. Please, someone send vegan brownies to Old Pink, in care of the Funny Farm, England.

2. Decipher this text with the keywords `FRANCE` for the square and `PRUSSIA` for the transposition.

   ```
   AFAAGAGGFGADFXFFGFAGFDAAFFFGAGAAXFXAFDXFAAAGFGAFGDXGFF
   FXFAAGAGXXGAAXAAAFDXGXFFFGXXDDFGGFFXFDAAGFGDGXXFDADADA
   ADGAGDGADADADAGGDDFAGGAAGDGDXDDADDDDFDDDDFXDGFGDAXAFFG
   GADFXADDDAGFFAAGAFGDGDAFDGADAAAGXAAAGAGGGFGDDAFAAFDGDF
   DADFFDAFADAGDFFDFDFDDXAGFFAAGGXAADFAADDFFAGDFFAFGGXAGG
   XFGFXDGXGGFGGAADXDDGAFXADGAAGXFFFDGGAAXDXXFFAFGXAGDGGF
   AGDDFFGXAAFFAGXAAAXXDFFGAFXDGXXXAAAAXFGGDDAGAXFGAXDXAG
   FGAAFGFGXFFAGADFADDGAAFDFGXXGFAFDFGGDXGDDFFDAFDADAAAGF
   DFDFDDFAGADDFGFGAADFXAFGGXXDGGDGGFDD
   ```

3. Break this ciphertext. What are the keywords?

   ```
   DXGAGFDAAAXAAAADAFADAAGFDADGAAAGFAGADAGFDGAGFGAGAAADAA
   GDAGADADFFADDDDAXDAFFGDDDXADAAGAGFXDADXFDAADAGDAFAAFAD
   AGFFFDADADAGXAADDFAAAAGXGFDGDGGDAFDFXXDDGDFFDDDAFFDAGA
   AGDXADAAXDADFDXDADGGFDFDAGGXGDGXGDDGXGDDAGDFFXFFDFXGDG
   DFDXGDFFDAFGAFGFFXGDGDFFXGXFXFFFFFGXFDGXFFXGDDFFAXAGGX
   DXDDGGFGGAGGADAXDGDXFDFFFDDGDAXFDXGXGDFXGGDFDGDXFFXGXX
   DGGDDXGADFFDAGFXDGFDAXXDXDAGFFGXADGFGXXDFDGXDGFFDXGDFF
   FXFFGAFDXXDGGGFADFFXFFDGFGXDGXXXFGDGGDDFGAGDFFFDDAXDFF
   AGDAFXADGAGDXADGXFGGXDAXFFFXGAXGGDGGFGXXXGADGGFAAGAGFD
   GGGDAXXXDDGXAGDDGDXXAGDFGGFGFDGXXXFDXAFGFFDDXFFFDGFGGG
   XADFFXFXXGGGDXXFDGDDGFGFGXXFAAADDADFAXXGDADDAAGDDDXAAG
   AFDAAADXGAGDADFDXAAADDFFGGAXDDDAGFDXDXXAGXFFAAGAGDADDA
   GADADDDDDAAGFFADGFAAFAFDDDGFDDDDAAGADAGDDAGFDFADDXADDA
   AAFDAAGAADDAAGAGDFGAAFDAADXGDGDAGAFFDAAADDAFXFGAAAAAGF
   DADDXDXFXXFGDXDXFXDFAGXDXFFDDXXFGFGXGXGFXADGXGXXXDXDAX
   FDAGXFFXFXGDFDDAXAFGADFGDGDFGDXDXDGDFFGDAGDFFGFGGDXFDX
   FXDADGDFXXFFXDAXFFGGGFGXDDGDFFFDDFXDDADGDDGXGDXAFXXGFD
   FGGGDFFXXDGFDDGAFFFDDXGXFFXADAGADAFXDFDDAAADFDAGADDADX
   XGAAFXDDADDADFDDDAGDFGFAAADGAADDFAADADDDADGFDAAAADADAA
   GXDGDAADAAFAXDXAADDDGAAAGDDDDGFGDDFAADXAAAADAADDXDAGAG
   ADDAGDFAFGAAFFGXAAAAGXAAXGGXXGAAGGXDAAFFGADDDDDAAXADXA
   AA
   ```

4. Break this ciphertext. What are the keywords?

AAAFXAFFGAAXDDGGAAAXDGGFGDAAGADAGGDFDDFGAFGDGADDDGAFXG
DAFXDAXDFADADAFFGGDFGAGFGADFAFFAXAFAXFAXFAGAXDAFFXXAGX
GFDFGDDDXAXXAXAXFAFXFXXGDXXAFFADFFFFAAFAXADXAXGGGAFXDF
FDFDDGGGDADDGGADAAADFFGGXAAAFGADFDXGDAGDADGFFFGAAGDGDF
DDFDXFGAGDADDGDGFDDAAAAGFFAGAFGDFGAXFGDDAGGFDAFDGDDAFA
DDGGAXFGDGGDXAADDGFFGDAGAGGAAGDAFFDGFGADDAGGAFGDDDFGAA
GGAGDFXGDFFDAXFDXAGFAXAXAXDAFXXADXDAXFADGXADDADGAGFXDX
XXXAXFXAXFFXFAGDXADGAAGFGAXXXGDGADGFAAGFADXGAXAGFDFAAF
AFXAADFGXAXGFXFDADGAAXDXFGXAADGGAGGDXFXAXFAXFADXFXXXDA
DGDFXDAGGGDDDXGAGAFGGDDGAXAXAAFGFAGDXADGGDXDFDXGXDFAGA
XFDGFXDADXXFDDAFAXXXDXAXFAGGGGFAFDDXDFGFAGDAFADDGXXDFA
AAADAGDAFGAFXDXGGFGGGFFDDADAAGFGGGAGDGAGFGFDAGFDADDADA

Unit 84
ADFGVX cipher

The *ADFGVX cipher* is the extension of the ADFGX cipher by using a 6×6 Polybius square. Because the square has 36 places, it holds the full English alphabet and all ten digits. The choice of the labels A, D, F, G, V, X is due to their low likelihood of being mistaken when transmitted in Morse code.

Some use a variation in which the transposition stage is a permutation cipher.

An approach to breaking the ADFGVX is to look for a columnar permutation that results in the fewest distinct digrams. We are looking for a decryption with mostly letters and few or none of the digits. After the transposition, the Polybius cipher is broken as usual, if possible.

Another approach to breaking the cipher is to extend the attack on the ADFGX to use 36-character alphabets and a 6×6 Polybius square.

Reading and references

Practical Cryptography, practicalcryptography.com/ciphers/adfgvx-cipher

General Solution for the ADFGVX Cipher System, Washington D.C.: U.S. Government Printing Office, 1934, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_269/41784769082379.pdf, archive.org/details/41784769082379

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, pages 339-346.

Programming tasks

1. Implement an encryptor.
2. Implement a decryptor.
3. Implement the first attack described above. The length of the permutation is an input.

4. Implement the second attack described above. The length of the permutation is an input. As a subproject, implement the attack from Unit 28 for an alphabet of 36 characters. In calculating the fitness, it is acceptable to delete digits from the text.

Exercises

1. Encipher this text with the keywords `WEATHER` for the square and `PICNIC` for the transposition (remove repeated letters in the keywords).

   > To give a picnic party a fair chance of success, it must be almost impromptu: projected at twelve o'clock at night at the earliest, executed at twelve o'clock on the following day at the latest; and even then the odds are fearfully against it. The climate of England is not remarkable for knowing its own mind; nor is the weather "so fixed in its resolve" but that a bright August moon, suspended in a clear sky, may be lady-usher to a morn of fog, sleet, and drizzle.
   >
   > from "The Picnic Party" by Horace Smith

2. Decipher this text with the keywords `MUNCHKINS` for the square and `CYCLONE` for the transposition (remove repeated letters in the keywords).

   ```
   DGDADVAADDDDDGGDFVDGDVFGDGDDFADDADGDDGDDDAGDADAGDDDDDD
   GADFFGADGDDDGADAFFGDAAFAGGDAGAADAGDDFGDFDDADDGDAGFDGFG
   GADGFFDDADGFAAFDAFDAFGFGFFGAFADAAFDDGGGDGDDFDDFDAFDADG
   ADXDFFGDGVVFVGXFADVFVXGFFXAXVAFGXVFAFVFFVGGXDFFVXVVVXX
   FVXVGVFXDFVAXVAVDGVVAFFFAVFVVXDFGDDDVXDXAFFAGXFVAVGVDX
   FXVVXFDVGFVVFFDXDFVFFVDXFXDFFAFDXFGXFDXXADVDDDVDDFVVAD
   VDDADGDDDFDADADGADFGAADADFAFDDAADDAGDGGFADGGADDDGDGGDF
   ADGFGDFDFFDFGAAADDDVGADFDGDAGADDFFAFDGGFAGAAADAAGGDFFA
   ADFFDDDFAGDDGFDDDDADDDDFADFDFDGFDAGDFDFAADDFADDADDGDAG
   FFDDGDDDADDAFDADGDDFGADFDFAADFDADGGDAGDDADDAAADGGAFDAA
   AFDAFFAADGDDAAFDDDDDFDFVGDADDDAFDDGGFGDDAGDDGADADDADFF
   DFDGDFAFAGADDGAGGGDGDFAGDGDGDGDDVDVDDFADADDVFGFFGDFGGG
   DFDADDVFVXVFVDDXFXDVAVFVFGFAVVVGDAVFGFDDVFFAXDFVGFFVVV
   FVXFFFVFDGAGVAVDGFVXAFADVFXVFXVFVDFVVFVFFDVVDVDVXAFFVV
   AVFVAGVDDFAADVVFVFXXDFVXVXVVAGADXDAFAFVVVVVVXDVFAXFAXF
   XFDGDDXVDVFXXAVXDVFDXFFVVAVFXADFDFVXDVXXDFFDXDVXFVDXVV
   FDFFFXVVFDAVGFFXFXFFVFVAGVFDDFVGFFXDVFAAFVAFAFGDDDFFAF
   XFVVAFGFDAXDDVXXFAFVVVGFFXXVVFGFDGGGVAXFFVXGFDDXDAGDFG
   DFVVXDAFVF
   ```

3. Break this ciphertext. The transposition has length nine. What are the keywords?

   ```
   GFAADFVAGDXFVAAFADGDDFAADAXAVDAADAGAAADAXDAVGAVFDAGFVA
   XDDDGDXGDAGAFAVDXAFAAGXDFDADFAVFFADAAGVDADXAXFAAVADAVD
   XDDAFDDFXFFADFVADAAGAAAGAFGVFGVDAAAAGDAAXDFAAADAAGVGAG
   AAADVFXDDFADGDAAAAGGDDFAAAAFVDXDAGXGDAAAVGAAVADDXDXAAF
   ```

VDGADDFGAGVFVDXAGDVDAAGGXAAAAFVDGFDFGFADGADDAFFDGGXAAG
FGGFDAAADFDAADGAAFDGGGXAFDGAAAFFFDGADAGGDFDGXAFAFADAAA
GAADXAVFXDGFVAGDDAVAXFAAXDXGDDVGGGVFXDADDAFDVFDDVDGDDA
GAXDVAGAAGVFAAVDVDDAVDAFGDFDXAAAAAAADAAAFADAGAFGADADDD
XGDDXAAGXADAXAAFAAXGDAVDGGAAFAFFDAAADAXFGFADXFDDAAGFXG
DFDGFFAGGAAGXAAGXAVADDGDXFGGAADDGAGDAGDAXAVDAGAADXDAAV
GVAADDFVAGDADXGXDAAXDAFADAAAAAAXGFFDDXAVAVFADADDAAADAA
AGAFDVGXFAFXGXFAGXAXADVADXFXAXAVDVGVFGAXGGGFFGAADXAVAA
AFDGGXDGVFDGDXDAAFAAFXFGAAAFAFDAAAAAFAAXAADGGXAXAAGVDA
AADADADVADAXDFGXAGGFDVFGGDAXAADXAXAAAGAVAGDGFXAXAADFFA
AVDADAGADAAVAXFFDADAAAAXFAFVAFDXFADVDGDGAADXAA