

Afterword

What now? You have learned everything there is to know about classical cryptography. Just kidding. Keep learning. There are still more ciphers we have not covered; many can be found on the American Cryptogram Association's website at www.cryptogram.org/resource-area/cipher-types. When you feel the urge, find one that is new to you. Study it, understand it, and implement it. Find a weakness, then a way to break it. Sometimes, the best you can do is a brute-force attack, but for classical ciphers that is still an achievement when you have modern computers to help you. Furthermore, new classical ciphers are invented still, usually as challenges to other enthusiasts. Several of the ciphers in the section on miscellaneous ciphers were invented for that reason.

After the classical era comes the mechanical era, characterized by rotor machines that use a collection of rotating disks to encipher messages. The disks each contain a wire maze that redirects an electric current as it passes from one disk to the next. Some have reflectors that redirect the current back through the set of disks. Enigma was one such machine. It had three or four disks and a reflector. The disks could be removed and replaced in different order, and the reflector could be swapped out for a different one. By using a reflector, Enigma could never encipher a letter to itself. This weakness helped to break its cipher. The Bombe was a device that, together with a crib, was used to recover the key for messages encrypted with Enigma. Other rotor machines include Lorenz, Purple, and Fialka (which is another shade of purple).

We have not mentioned *Kerckhoffs's principles* yet. He summarized some basic properties of a good cryptographic system, such as its ease of use and portability. His second principle is that the security of the system should not depend on the secrecy of the algorithm (or mechanical device), but rather on the secrecy of the keys. One's enemy can often find and steal the details of the system or device, so we should not rely on keeping them hidden. Instead, the system should be strong enough that an enemy cannot break it without knowing the keys. As you know by now, none of the classical ciphers are secure in this light. Furthermore, when a new classical cipher comes along, we can often figure out the scheme and break it without prior knowledge of it. In the modern era, however, Kerckhoffs's second principle is taken very seriously.

The modern era is characterized by the use of computers. With them comes a level of complexity that makes it impossible to break modern cryptographic systems with pen and paper. But on the other hand, new structures and uses for them arise. The ideas that you should carry forward from the classical into the modern era are substitution, transposition, and fractionation; these ideas are used, albeit in more complicated ways. Here are some of the major differences you will see as you study the cryptography of the modern era:

- Algorithms are far more complex, and therefore...
- We must use computers
- Algorithms are publicly known. In fact, there are competitions for new algorithms. The current standard, *AES* (“*Advanced Encryption Standard*”) employs the algorithm that won a competition held by the U.S. National Institute of Standards and Technology (NIST). Such competitions take years to complete, as the community evaluates each algorithm and tries to find its weaknesses. Since everyone knows the algorithms, security rests in the secrecy of the keys (Kerckhoffs’s second principle).
- *Asymmetric (public-key)* ciphers now allow someone to encrypt a message for a recipient s/he has never met before. Such a cipher has two keys; one locks it, and the other unlocks it. The recipient publishes his/her locking key (the public key) for anyone to use. Messages meant for the recipient are encrypted with the public key, and only the recipient can decrypt with the other, private, key.
- Public-key cryptography also allows us to digitally sign messages. If a message is encrypted with a private key, then anyone can use the public key to decrypt it, thereby proving that it was written by the individual holding the private key. To make this process easier, we only need to encrypt a shorter text, which is a secure digest of the message; this brings us to...
- *Hash functions*: these are functions that take a message and produce a large number, called the *digest* of the message. These functions are special in that it is easy to find the digest of a message, but nearly impossible to recover the message from the digest. For this reason, they are called *one-way functions*.
- The security of a cryptographic system is demonstrated by reducing it to a hard mathematical problem. For example, the *RSA* public-key system uses the difficulty of factoring large integers as the basis of its security.

The quantum era is now beginning. Quantum computers will allow us to solve some classically difficult mathematical problems easily. For example, once a quantum computer can be built that is large enough (really no larger in terms of memory and processing than computers that we now have), it will be able to factor large integers almost instantly. This will mean the death of RSA. Therefore, we need new algorithms, algorithms that are resistant to quantum computing. There is currently a competition at NIST for such things. Stay tuned.

Just keep learning.

Reading and references

American Cryptogram Association, “The ACA and You,” <http://www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf>, 2005 edition: http://web.archive.org/web/*/http://www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf, 2016 edition: web.archive.org/web/*/http://cryptogram.org/docs/acayou16.pdf

Auguste Kerckhoffs, “La cryptographie militaire,” *Journal des sciences militaires* IX (1883) 5-39 and 161-191, www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf, www.petitcolas.net/kerckhoffs/crypto_militaire_2.pdf

Turing Bombe Tutorial, www.lysator.liu.se/~koma/turingbombe/TuringBombeTutorial.pdf

Whitfield Diffie and Martin E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory* 22 (1976) 644-654, ee.stanford.edu/~hellman/publications/24.pdf

Exercises

1. Find a cipher you have never used before and learn how it works. A good place to start is www.cryptogram.org/resource-area/cipher-types. Can you find a weakness in the cipher? Can you modify an attack that you have to break this cipher? Give it a try.
2. Repeat Exercise 1 as often as you like.
3. Read about the rotor machines from the mechanical cryptographic era, about modern ciphers and hash functions, and about quantum key distribution.

Index

Numbers refer to units, not to pages. Numbers in italics refer to the location of a term's definition.
Items in `monospaced typewriter font` are programming items.

addition	14, 15
additive cipher	<i>15</i>
additive identity element	<i>14</i> , 85
additive inverse	<i>14</i>
ADFGX cipher	83, 84
ADFGVX cipher	<i>84</i>
adjugate matrix	85, 86
Advanced Encryption Standard (<i>see</i> AES)	
AES	<i>afterword</i>
affine cipher	22, 23-25, 43-44, 89
affine Hill cipher	89
albam cipher	<i>13</i> , 15
AMSCO cipher	65
<code>append()</code>	2
<code>argv[]</code>	12
asymmetric cipher	<i>introduction</i> , <i>afterword</i>
asynchronous	90, 92
atbash cipher	<i>13</i> , 40, 41
athbash cipher (<i>see</i> atbash cipher)	
autoclave cipher (<i>see</i> autokey cipher)	
autokey cipher	92, 93, 94
Baconian cipher	<i>100</i> , 117
Bacon's cipher (<i>see</i> Baconian cipher)	
base (of number)	55
Bazeries cylinder	<i>124</i>
Beaufort cipher	40, 90, 107, 108
Bellaso 1552 cipher	42
bifid cipher	81, 82, 117
biliteral cipher (<i>see</i> Baconian cipher)	
biliterarie cipher (<i>see</i> Baconian cipher)	
binary	100, 117

binomial coefficient	10
bit	<i>introduction</i>
block cipher	87, 90
block transposition cipher	53
Bombe	<i>afterword</i>
boolean	20
break	<i>introduction</i>
British National Cipher Challenge	117, 118
Brown corpus	1
brute-force attack	16, 23, 34, 39, 42, 56, 59, 60, 63-65, 87, 89, 112, 115, <i>afterword</i>
Cadenus cipher	67, 68
Caesar (shift) cipher	15, 16-19, 33, 38, 41, 96, 108, 120
Chase cipher	119
chi-squared statistic	5
choice()	112
choose	10
cipher	<i>introduction</i>
cipher clock	120, 121-123
ciphertext	<i>introduction</i>
classical	<i>introduction</i>
classical era	<i>introduction, afterword</i>
cleartext	<i>introduction</i>
ciphertext-autokey (<i>see</i> self-synchronizing)	<i>introduction, 99, 100-104</i>
code	69, 99, 103, 117
code word	85
cofactor	85
cofactor matrix	85
coincidence, index of (<i>see</i> index of coincidence)	85, 87
column vector	58, 60, 62, 65, 67, 68, 83, 84, 119
columnar transposition cipher	118
combination-lock cipher	85
commutative	7, 85, 86
complete-unit transposition cipher (<i>see</i> permutation cipher)	51
component (of vector)	20
composition (of permutations)	1, 2-4, 109, 115
coprime	7, 112
corpus (textual) [<i>pl.</i> corpora]	<i>introduction</i>
cosine of angle between vectors	17, 24, 35, 88, 89, 121
crack	<i>introduction</i>
crib	<i>introduction</i>
cryptanalysis	97
cryptography	
<i>Cryptonomicon</i>	
CSP-845 (<i>see</i> M-138-A)	
CSP-488 (<i>see</i> M-94)	

cylinder cipher	124
data, linguistic (<i>see</i> linguistic data)	
decipher	<i>introduction</i>
decode	<i>introduction</i> , 99
decrypt	<i>introduction</i>
decipher	<i>introduction</i>
determinant (of matrix)	85, 86
deterministic	112, 113, 114, 124
dictionary (Python)	112
dictionary attack	27, 36, 40-42, 62, 65, 67, 70-73, 76, 78-82, 87, 89, 92, 107, 109-112, 119, 120
digest	<i>afterword</i>
digram substitution cipher	70, 71-75, 107
dimension (of matrix)	85
dimension (of vector)	7, 85
dinome	103, 104
directed graph	122
division	21
dot product (<i>see</i> inner product)	
double columnar transposition cipher	61
double Playfair cipher	79
doubled-over substitution cipher	116
duplicitous cipher	117
edge	122
element (of matrix)	85, 86
elementary row operations	85
encode	<i>introduction</i> , 99
encrypt	<i>introduction</i>
Enigma	<i>afterword</i>
entropy	11
entry (of matrix)	85, 86
Euclid's algorithm	20
Euclid's extended algorithm	21, 86
extended Euclidean algorithm (<i>see</i> Euclid's extended algorithm)	
factoradic number	55
factorial	55
factorial number	55
factorization	20
False	20
Fialka	<i>afterword</i>
Fibonacci sequence	90
fitness	6, 8, 115
fixed-width code	99, 100, 101, 117
four-square cipher	75
fractionated Morse cipher	109
fractionation	81, 82, 109, 117-119
function	3
gcd (<i>see</i> greatest common divisor)	

German Beaufort cipher (<i>see</i> variant Beaufort cipher)	
Grandpré cipher	112
graph	122
greatest common divisor (gcd)	20
grid-based cipher	69-84
Gronsfeld cipher	39
group	52
Gutenberg (<i>see</i> Project Gutenberg)	
hash function	<i>afterword</i>
Heap's algorithm	54
Hill cipher	87, 88, 89
hill-climbing attack	28, 37, 39-42, 50, 57, 60-62, 68, 71, 74, 77, 78, 81-83, 93, 98, 107, 108, 109, 112, 113, 115-117, 123, 125
homophone	112, 115
homophonic substitution cipher	112, 114, 115
horizontal two-square cipher	73, 74
Hutton cipher 1	110, 111
Hutton cipher 2	110
identity permutation	52
import	3
in	2
index()	12
index of coincidence	10, 12, 31, 70, 81, 83, 87, 118
inner product	7, 85
integers (as a set of numbers)	14, 21, 86
internal state	90, 91, 92, 97, 120
inverse matrix	85, 86, 87
itertools module	34, 52
Jefferson cypher wheel	124
Kasiski examination	30
Kasiski method (<i>see</i> Kasiski examination)	
Kerckhoffs's principles	<i>afterword</i>
key	12
key space	12
key stream	90
keyed substitution cipher (<i>see</i> keyword substitution cipher)	
keyphrase cipher	112
keyword	26, 33, 87, 107, 108, 112, 109, 117-120
keyword cipher (<i>see</i> keyword substitution cipher)	
keyword substitution cipher	26
lcm (<i>see</i> least common multiple)	
least common multiple (lcm)	20, 37
Lehmer code	55
len()	7
length (of vector)	7
lexicographical order	55

linguistic data	1-4
<code>list()</code>	52
<code>log()</code>	4
logarithm	4
Lorenz	<i>afterword</i>
<code>lower()</code>	1
M-138	126
M-138-A	126
M-94	124, 125, 126
MadHatter cipher	116
math module	4, 7
matplotlib module	6, 8, 9
matrix	85, 86-89
matrix transposition cipher	58, 59
mechanical era	<i>introduction</i> , <i>afterword</i>
minor matrix	85
mixed-radix number	116
modern era	<i>introduction</i> , <i>afterword</i>
modular arithmetic	14, 15, 21, 22, 33, 40, 86
module (Python)	3
modulus	14, 86
monoalphabetic	12
monoalphabetic substitution	12, 13, 15-19, 22-28, 45-49, 52, 69, 83, 103-105, 109, 111, 112, 116, 117, 120-123
monoalphabetic substitution with camouflage	115
monogram	3
monogram fitness	6, 8, 12, 18, 19, 112
monome	103, 104
monome-dinome cipher	103, 104
morbit cipher	109
Morse code	83, 84, 99, 102, 109, 115
multiplication	21, 85
multiplicative cipher	22
multiplicative identity element	21, 85
multiplicative inverse	21, 85, 86
Myszkowsky cipher	66
Nicodemus cipher	108
Nihilist substitution cipher	80
Nihilist transposition cipher	62
non-prefix code (<i>see</i> non-prefix-free code)	
non-prefix-free code	99
null	53
one-time pad	106
one-way function (<i>see</i> hash function)	
<code>open()</code>	1, 27
optional argument	3
origin (of vector space)	7, 85
parallel assignment	21

period	29, 30-32, 78, 81, 82
periodic	29
periodic affine cipher	43, 44
periodic polyalphabetic substitution	29, 30-50, 81, 90, 108
permutation	52, 53-57, 62, 65, 68, 117
permutation cipher	53, 56, 57, 62, 83, 84, 90
permutations()	52
Phillips cipher	76, 77, 78
Phillips-RC cipher	78
plaintext	<i>introduction</i>
Playfair cipher	70, 71, 72, 79, 81
Pletts Cipher Machine	120
Pollux cipher	115
polyalphabetic	29
Polybius cipher	69, 83, 84, 99, 117
Polybius square	69, 70-81, 83, 84, 117
Polybius-square cipher	69
polyhomophonic substitution cipher	114
polyphonic substitution cipher	113, 114
pop()	55, 112
Porta cipher	42
prefix code (<i>see</i> prefix-free code)	
prefix-free code	99, 103, 104
prime	20
print()	<i>introduction</i>
probabilistic	112, 114, 116, 124
product()	34
progression index	96
progressive-key cipher (<i>see</i> progressive Vigenère cipher)	
progressive Vigenère cipher	96
Project Gutenberg	1
proto-mechanical ciphers	120-126
public-key cipher (<i>see</i> asymmetric cipher)	
Purple	<i>afterword</i>
pylab module	6, 8, 9
Python	<i>introduction</i>
quagmire 1 cipher	45, 46, 80
quagmire 2 cipher	47
quagmire 3 cipher	48, 110
quagmire 4 cipher	49
quantum era	<i>introduction, afterword</i>
qubit	<i>introduction</i>
radix	55
railfence cipher	63, 64
random module	57, 112
randrange()	119
range()	52
read()	1, 27
reciprocal key	13, 42

reciprocal cipher	13, 15, 40, 42
recursion	20, 85
redefence cipher	64
remove()	55
replace()	1
residues	14, 86
ROT13	15
RSA	<i>afterword</i>
rotor machines	<i>afterword</i>
route transposition cipher	51
running-key cipher	95
scalar	7, 85
scalar product (<i>see</i> inner product)	
Scrabble cipher	111
scytale	58, 59
scytale cipher (<i>see</i> scytale)	
self-synchronizing	90
seriation	79, 117
shuffle()	57
signature	32
simple columnar transposition cipher	58, 59
simulated annealing	71
slidefair cipher	107
solitaire cipher	97, 98
sort()	32
split()	2, 27
square matrix	85, 86
sqrt()	7
stochastic	28
straddling checkerboard cipher	104
stream cipher	90, 91-98, 106, 120, 123
strip cipher	126
substitution cipher	12, 13, 15-19, 22-50, 70-80, 105, 112-114, 116
subtraction	14, 15
symbolic substitution cipher	105
symmetric cipher	<i>introduction</i>
synchronous	90, 91, 96, 97
sys module	12
tableau [<i>pl.</i> tableaux]	33, 40-42
tabula recta (<i>see</i> tableau)	
ternary	101, 117
tetragram	4
tetragram fitness	9, 16, 34, 36, 37, 112
textual corpus [<i>pl.</i> corpora] (<i>see</i> corpus)	
transliterate	105
transpose (of matrix)	85
transposition cipher	51, 53, 56-68
trifid cipher	82, 117

triliteral cipher	101
triliterarie cipher (<i>see</i> triliteral cipher)	
trit	118
Trithemius cipher	91, 96
True	20
twist	32
twist method (for finding period)	32
twisted-scytale cipher	59
two-square cipher	72-74
type 1 (<i>see</i> quagmire 1)	
type 2 (<i>see</i> quagmire 2)	
type 3 (<i>see</i> quagmire 3)	
type 4 (<i>see</i> quagmire 4)	
Unicode	1
update()	112
upper()	1
Urkryptografen	120
variable-length code	99, 102-104
variant Beaufort cipher	41, 90, 107, 108
variant cipher (<i>see</i> variant Beaufort cipher)	
vector	7, 85, 86-89
vector space	85
Vernam's cipher (<i>see</i> one-time pad)	
vertex [<i>pl.</i> vertices]	121
vertical two-square cipher	72, 73, 74
Vigenère cipher	33, 34-38, 40, 41, 45-49, 80, 89-91, 95, 96, 106, 107, 108
Wadsworth cipher disk	120
Wheatstone Cryptograph	120
write()	1
\mathbb{Z} (<i>see</i> integers)	
zero vector	85
+ (<i>see</i> addition)	
− (<i>see</i> subtraction)	
* (<i>see</i> multiplication)	
/ (in Python)	introduction, 3
// (in Python)	introduction, 3, 14
% (in Python)	14
χ^2 statistic	5
◊ (<i>see</i> twist)	

Bibliography

American Cryptogram Association, “The ACA and You,” www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf, 2005 edition: web.archive.org/web/*/http://www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf, 2016 edition: web.archive.org/web/*/http://cryptogram.org/docs/acayou16.pdf; the pages about ciphers are linked from this page: www.cryptogram.org/resource-area/cipher-types

Francis Bacon, *Of the proficience and advancement of Learning, divine and humane*, London: Henrie Tomes, 1605.

Thomas H. Barr and Andrew J. Simoson, “Twisting the Keyword Length from a Vigenère Cipher,” *Cryptologia* 39:4 (2015) 335-341, DOI: [10.1080/01611194.2014.988365](https://doi.org/10.1080/01611194.2014.988365)

Friedrich L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology*, 4th edition, Berlin: Springer-Verlag, 2007.

Étienne Bazeries, *Les Ciffres Secrets Dévoilés*, Paris: Charpentier et Fasquelle, 1901, books.googleusercontent.com/books/content?req=AKW5Q...

Giovan Battista Bellaso, *La Cifra del Sig. Giouan Battista Belaso* [sic], 1553.

Paolo Bonavoglia, “Bellaso’s 1552 cipher recovered in Venice,” *Cryptologia* 43:6 (2019) 459-465, DOI: [10.1080/01611194.2019.1596181](https://doi.org/10.1080/01611194.2019.1596181)

Paolo Bonavoglia, La crittografia da Atbash a RSA, www.crittologia.eu, 2020.

Paolo Bonavoglia, “Trithemius, Bellaso, Vigenère: Origins of the Polyalphabetic Ciphers,” Proceedings of the 3rd International Conference on Historical Cryptology, 2020, ep.liu.se/ecp/171/007/ecp2020_171_007.pdf, DOI: [10.3384/ecp2020171007](https://doi.org/10.3384/ecp2020171007)

Augusto Buonafalce, “Bellaso’s Reciprocal Ciphers,” *Cryptologia* 30:1 (2006) 39-51, DOI: [10.1080/01611190500383581](https://doi.org/10.1080/01611190500383581)

Pliny Earle Chase, “Mathematical Holocryptic Cyphers,” *The Mathematical Monthly* 1:6 (1859) 194-196, books.google.com/books?id=SVNLAAAAMAAJ&pg=PA194

Chris Christensen, "Lester Hill Revisited," *Cryptologia* 38:4 (2014) 293-332, DOI: [10.1080/01611194.2014.915260](https://doi.org/10.1080/01611194.2014.915260)

Benjamin Church, Jr., George Washington Papers, Series 4, General Correspondence: Benjamin Church Jr. to Maurice Cane, July 1775, www.loc.gov/item/mgw443691

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

Noel Curren-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](https://doi.org/10.1080/02684528708431890)

Donald W. Davies, "Charles Wheatstone's Cryptograph and Pletts' Cipher Machine," *Cryptologia* 9:2 (1985) 155-160, DOI: [10.1080/0161-118591859870](https://doi.org/10.1080/0161-118591859870)

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

Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22 (1976) 644-654, ee.stanford.edu/~hellman/publications/24.pdf

Arthur Conan Doyle, "The Adventure of the Dancing Men," first published in 1905, now in *The Complete Works of Sherlock Holmes*, London: Simon & Schuster, 2012.

Niels Faurholt, "Urkryptografen (The Clock Cryptograph)," *Cryptologia* 27:3 (2003) 206-208, DOI: [10.1080/0161-110391891874](https://doi.org/10.1080/0161-110391891874); this article is available also at www.jproc.ca/crypto/crypto_watch.html

William F. Friedman, "Codes and Ciphers (Cryptology)," *Encyclopaedia Britannica*, 1956, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_535/41772109081119.pdf

William F. Friedman, *Elements of Cryptanalysis*, Washington D.C.: Government Printing Office, 1923, www.marshallfoundation.org/library/digital-archive/elements-cryptanalysis

William F. Friedman, *The Index of Coincidence and Its Applications in Cryptography*, Riverbank Laboratories Department of Ciphers Publication 22, Geneva, Illinois, 1920, www.marshallfoundation.org/library/methods-solution-ciphers

William F. Friedman, *Methods for the Solution of Running-Key Ciphers*, Riverbank Laboratories Department of Ciphers Publication 16, Geneva, Illinois, 1918, www.marshallfoundation.org/library/methods-solution-ciphers

William F. Friedman, *Military Cryptanalysis, Part I: Monoalphabetic Substitution Systems*, Washington D.C.: U.S. Government Printing Office, various years for various editions.

William F. Friedman, *Military Cryptanalysis, Part II: Simpler Varieties of Polyalphabetic Substitution Systems*, Washington D.C.: U.S. Government Printing Office, various years for various editions.

William F. Friedman, *Military Cryptanalysis, Part III: Simpler Varieties of Aperiodic Substitution Systems*, Washington D.C.: U.S. Government Printing Office, various years for various editions.

William F. Friedman, *Military Cryptanalysis, Part IV: Transposition and Fractionating Systems*, Washington D.C.: U.S. Government Printing Office, various years for various editions.

William F. Friedman, *Several Machine Ciphers and Methods for their Solution*, Riverbank Laboratories Department of Ciphers Publication No. 20, 1918, www.campx.ca/Several_Machine_Ciphers.pdf and www.marshallfoundation.org/library/methods-solution-ciphers

William F. Friedman, *Six Lectures on Cryptology*, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/publications/ACC15281/41785109082412.pdf

William F. Friedman and Lambros D. Callimahos, *Military cryptanalytics, Parts I through IV*, Aegean Park Press, 1956, reprinted 1985.

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

Greg Goebel, *Codes, Ciphers, & Codebreaking*, vc.airvectors.net/ttcode.html

Lester S. Hill, "Cryptography in the Algebraic Alphabet," *The American Mathematical Monthly* 36:6 (1929) 306-312, DOI: [10.2307/2298294](https://doi.org/10.2307/2298294), www.jstor.org/stable/2298294, web.archive.org/web/20110719235517/http://w08.middlebury.edu/INTD1065A/Lectures/Hill_Cipher_Folder/Hill1.pdf

Lester S. Hill, "Concerning Certain Linear Transformation Apparatus of Cryptography," *The American Mathematical Monthly* 38:3 (1931) 135-154, DOI: [10.1080/00029890.1931.11987161](https://doi.org/10.1080/00029890.1931.11987161), www.jstor.org/stable/2300969, www.cs.jhu.edu/~cgarman/files/Hill2.pdf

Parker Hitt, *Manual for the Solution of Military Ciphers*, Fort Leavenworth (Kansas): Press of the Army Service Schools, 1916, www.marshallfoundation.org/library/digital-archive/manual-solution-military-ciphers, www.gutenberg.org/ebooks/48871

Thomas Jakobsen, "A fast method for cryptanalysis of substitution ciphers," *Cryptologia* 19:3 (1995) 265-274, DOI: [10.1080/0161-119591883944](https://doi.org/10.1080/0161-119591883944)

Thomas Jefferson, "The wheel cypher" or "Project of a cypher," Thomas Jefferson's Papers, volume 128 item 22138, volume 232 items 41575 and 41576, U.S. Library of Congress, www.loc.gov/item/mtjbib025756, founders.archives.gov/documents/Jefferson/01-37-02-0082

Thomas Kaeding, "Automated ciphertext-only attack on the Wheatstone Cryptograph and related devices," Cryptology ePrint Archive, report [2020/1492](https://eprint.iacr.org/2020/1492).

Thomas Kaeding, "MadHatter: A toy cipher that conceals two plaintexts in the same ciphertext," Cryptology ePrint Archive, report [2020/301](https://eprint.iacr.org/2020/301).

Thomas Kaeding, “Slippery hill-climbing technique for ciphertext-only cryptanalysis of periodic polyalphabetic substitution ciphers,” *Cryptologia* 44:3 (2020) 205-222, DOI: [10.1080/01611194.2019.1655504](https://doi.org/10.1080/01611194.2019.1655504)

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

Bruce Kallick, “A Modified Simple Substitution Cipher With Unbounded Unicity Distance,” Cryptology ePrint Archive, report [2019/621](#).

Friedrich Kasiski, *Die Geheimschriften und die Dechiffrier-Kunst*, 1863, digital.onb.ac.at/OnbViewer/viewer.faces?doc=ABO_+Z224431001

Auguste Kerckhoffs, “La cryptographie militaire,” *Journal des sciences militaires* IX (1883) 5-39 and 161-191, www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf, www.petitcolas.net/kerckhoffs/crypto_militaire_2.pdf

Solomon Kullback, General Solution for the Double Transposition Cipher, Washington D.C.: U.S. Government Printing Office, 1934, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_439/41751169079035.pdf

Lanaki, lessons and tutorials, www.cryptogram.org/resource-area/crypto-lessons-tutorials-lanaki

André Langie, *De la Cryptographie: Etude sur les Ecritures secrètes*, Paris: Payot et Companie, 1918, HDL: [2027/coo.31924029486838](https://hdl.handle.net/2027/coo.31924029486838); translated by James C.H. Macbeth as *Cryptography*, London: Constable & Company, 1922, HDL: [2027/uc1.32106002774104](https://hdl.handle.net/2027/uc1.32106002774104) and [2027/uc2.ark:/13960/t0tq62t29](https://hdl.handle.net/2027/uc2.ark:/13960/t0tq62t29)

James Lyons, Practical Cryptography, practicalcryptography.com, 2012.

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

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

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

Greg Mellen, “Cryptanalyst’s Corner,” *Cryptologia* 8:1 (1984) 55-57, DOI: [10.1080.0161-118491858773](https://doi.org/10.1080.0161-118491858773)

Marjorie Mountjoy, “The bar statistics,” *NSA Technical Journal* VII (2, 4), 1963.

Émile Victor Théodore Myszkowski, *Cryptographie Indéchiffrable basée sur de nouvelles combinaisons rationnelles*, Paris: Société Française d’Imprimerie et de Librairie, 1902, gallica.bnf.fr/ark:/12148/bpt6k1265620p

Grant A. Niblo, "The University of Southampton National Cipher Challenge," *Cryptologia* 28:3 (2004) 277-286, DOI: [10.1080/0161-110491892935](https://doi.org/10.1080/0161-110491892935) (see below for links to the challenge)

Merle E. Ohaver, "Solving Cipher Secrets," appeared weekly in *Flynn's*, 1924-1928, toebes.com/Flynns

Seongmin Park, Juneyeun Kim, Kookrae Cho, and Dae Hyun Yum, "Finding the key length of a Vigenère cipher: How to improve the twist algorithm," *Cryptologia* 44:3 (2020) 197-204, DOI: [10.1080/01611194.2019.1657202](https://doi.org/10.1080/01611194.2019.1657202)

Edgar Allan Poe, "The Gold-Bug," 1843, [en.wikisource.org/wiki/Tales_\(Poe\)/The_Gold-Bug](http://en.wikisource.org/wiki/Tales_(Poe)/The_Gold-Bug), www.eapoe.org/works/tales/golddbga2.htm

Giambattista della Porta [Giovanni Battista della Porta] [Ioan. Baptista Porta], *De Furtivis Literarum Notis*, Naples [Neapoli]: Ioa. Maria Scotus, 1563, HDL: [2027/gri.ark:/13960/t37142x6g](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9)

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

Bruce Schneier, "The Solitaire Encryption Algorithm," Schneier on Security, www.schneier.com/academic/solitaire

Claude E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal* 27:3 (1948) 379-423, DOI: [10.1002/j.1538-7305.1948.tb01338.x](https://doi.org/10.1002/j.1538-7305.1948.tb01338.x), HDL: [11858/00-001M-0000-002C-4314-2](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9)

Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, New York: Random House, 1999.

Abraham Sinkov, *Elementary Cryptanalysis: A Mathematical Approach*, 2nd edition, revised by Todd Feil, published by Mathematical Association of America, 2009, www.jstor.org/stable/10.4169/j.ctt19b9krf

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](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9) and [2027/uc2.ark:/13960/t0tq62t29](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9)

James Stanley, "The Wheatstone Cryptograph," incoherency.co.uk/blog/stories/wheatstone-cryptograph.html

S. Tomokiyo, "First Codebreaking in the American Revolution — Benjamin Church's Cipher," cryptiana.web.fc2.com/code/church.htm, 2009-2014.

Johannes Trithemius, *Polygraphiae libri sex*, Reichenau: Joannis Haselberg de Aia, 1518, www.loc.gov/item/32017914

Blaise de Vigenère, *Traicté des chiffres ou secrètes manières d'escrire*, Paris: Abel l'Angelier, 1586, HDL: [2027/ien.35552000251008](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9), [gallica.bnf.fr/ark:/12148/bpt6k1040608n](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9), [gallica.bnf.fr/ark:/12148/bpt6k94009991](https://nbn-resolving.org/urn:nbn:de:hbz:5:1-63888-p0071-9)

Charles Wheatstone, "Instructions for the Employment of Wheatstone's Cryptograph," *The Scientific Papers of Sir Charles Wheatstone*, The Physical Society of London, 1879, pages 342-347.
archive.org/details/scientificpaper00londgoog (the last two pages of the article were completely ruined by Google in that copy), books.google.to/books?id=CtGEAAAIAAJ

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

"Ciphers and Cipher-Writing," *Macmillan's Magazine*, XXIII, Feb 1871, pages 328-338,
babel.hathitrust.org/cgi/pt?id=mdp.39015004979913;view=1up;seq=340

NSA file 41788379082740:
www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_515/41788379082740.pdf

Basic Cryptography, Dept. of the Army Technical Manual 32-220, April 1950, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_238/41748889078809.pdf

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

NOVA Online, "Decoding Nazi Secrets," www.pbs.org/wgbh/nova/decoding

United States Army, Field Manual 34-40-2, Basic Cryptanalysis, U.S. Department of Army,
www.umich.edu/~umich/fm-34-40-2

MysteryTwister C3, www.mysterytwisterc3.org

RingZero Online CTF, ringzer0ctf.com

(British) National Cipher Challenge, www.cipherchallenge.org. Recent years' challenges are also on the site. An archive of past challenges is at github.com/themaddoctor/BritishNationalCipherChallenge