Ciphers

A Little History (Wikipedia)

The first well-documented description of a polyalphabetic cipher was by Leon Battista Alberti around 1467 and used a metal cipher disk to switch between cipher alphabets. Alberti's system only switched alphabets after several words, and switches were indicated by writing the letter of the corresponding alphabet in the ciphertext. Later, Johannes Trithemius, in his work Polygraphiae (which was completed in manuscript form in 1508 but first published in 1518), invented the tabula recta, a critical component of the Vigenère cipher. The Trithemius cipher, however, provided a progressive, rather rigid and predictable system for switching between cipher alphabets.

In 1586 Blaise de Vigenère published a type of polyalphabetic cipher called an autokey cipher – because its key is based on the original plaintext – before the court of Henry III of France. The cipher now known as the Vigenère cipher, however, is that originally described by Giovan Battista Bellaso in his 1553 book La cifra del Sig. Giovan Battista Bellaso. He built upon the tabula recta of Trithemius but added a repeating "countersign" (a key) to switch cipher alphabets every letter. Whereas Alberti and Trithemius used a fixed pattern of substitutions, Bellaso's scheme meant the pattern of substitutions could be easily changed, simply by selecting a new key. Keys were typically single words or short phrases, known to both parties in advance, or transmitted "out of band" along with the message. Bellaso's method thus required strong security for only the key. As it is relatively easy to secure a short key phrase, such as by a previous private conversation, Bellaso's system was considerably more secure.

In the 19th century, the invention of Bellaso's cipher was misattributed to Vigenère. David Kahn, in his book, The Codebreakers lamented this misattribution, saying that history had "ignored this important contribution and instead named a regressive and elementary cipher for him [Vigenère] though he had nothing to do with it".

The Vigenère cipher gained a reputation for being exceptionally strong. Noted author and mathematician Charles Lutwidge Dodgson (Lewis Carroll) called the Vigenère cipher unbreakable in his 1868 piece "The Alphabet Cipher" in a children's magazine. In 1917, Scientific American described the Vigenère cipher as "impossible of translation".,That reputation was not deserved. Charles Babbage is known to have broken a variant of the cipher as early as 1854 but did not publish his work. Kasiski entirely broke the cipher and published the technique in the 19th century, but even in the 16th century, some skilled cryptanalysts could occasionally break the cipher.

The Vigenère cipher is simple enough to be a field cipher if it is used in conjunction with cipher disks. The Confederate States of America, for example, used a brass cipher disk to implement the Vigenère cipher during the American Civil War. The Confederacy's messages were far from secret, and the Union regularly cracked its messages. Throughout the war, the Confederate leadership primarily relied upon three key phrases: "Manchester Bluff", "Complete Victory" and, as the war came to a close, "Come Retribution".

A Vernam cipher whose key is as long as the message becomes a one-time pad, a theoretically unbreakable cipher. Gilbert Vernam tried to repair the broken cipher (creating the Vernam–Vigenère cipher in 1918), but the technology he used was so cumbersome as to be impracticable.

Decryption Using a Polyalphabetic Table

Forward

The Objective:

As with all puzzles the ultimate objective is completion. The reward that one receives is usually the satisfaction derived from a job well done. All the pieces are in place. All the words are in order.

The solution to the jigsaw puzzle is the correct matching and joining of its pieces to form a picture. The solution to the crossword is the correct identification of all the words used to create that particular puzzle.

Most paintings and graphic art pieces are assigned titles by their artists. Like other artists, I title each ***Trithemian Web™***. The solution to a ***Trithemian Web™*** is first, successfully reading and/or deciphering the message body, and second, discovering the title of the piece.

Ciphers

A Trithemian Web™, if encrypted, will use polyalphabetic substitution to encode the piece. You can read more about codes on the Web or in an encyclopedia under cryptology. The best way to learn how to use a Polyalphabetic Table is to actually decipher a sample. On the following page is the Trithemian Tabula Recta, a Polyalphabetic Table. This table will be used to decipher encrypted Trithemian Web™ compositions.

One must have a Keyword to decrypt the ciphertext. The keyword used to decrypt the Sample 1 ciphertext is PLAN. The ciphertext is a group of seemingly random letters. The ciphertext is the **code**. Using a Polyalphabetic Table and a **keyword** we can decipher the ciphertext (code) into a meaningful set of words (plaintext).

Look at the simple ciphertext sheet on page 4. It reads KQSJDDSUZURI. These seemingly random letters are what you would have read in a small Trithemian Web™ composition. Below the ciphertext you will see KEYWORD, CIPHERTEXT, and PLAINTEXT. On a Ciphertext Sheet you would write the letters of the ciphertext (KQSJDDSUZURI) to the right of CIPHERTEXT, from left to right. I have done that for you. You would then write the letters of the keyword (PLAN) to the right of KEYWORD, from left to right, repeating the keyword until you have a keyword letter above each ciphertext letter. I have done that for you also. You will have: P L A N P L A N P L A N.

Note: An encrypted Trithemian Web™ will have **no** spaces between letters. You have to determine the word spacing after deciphering the code. The plaintext in Sample 1 will make that clear. I do not use word spacing so more letters can be included within a composition.

Whether a Trithemian Web™ is encrypted or not can be easily determined. The letters will make sense, and there will be spaces between words and sentences.

Trithemian Tabula Recta

(Polyalphabetic Table)

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

Ciphertext

Sample 1

Simple Ciphertext Sheet

Keyword	**PLAN**											
Ciphertext	**KQSJDDSUZURI**											
Keyword	**P**	**L**	**A**	**N**	**P**	**L**	**A**	**N**	**P**	**L**	**A**	**N**
Ciphertext	**K**	**Q**	**S**	**J**	**D**	**D**	**S**	**U**	**Z**	**U**	**R**	**I**
Plaintext												

Note: Sample 1 does not have a title. The focus is on how to use the polyalphabetic table. Title discovery will be covered in Sample 2.

The keyword used in Sample 1 happens to have four letters. This will **not** always be the case. For example, let's say the keyword here was CAT instead of PLAN. The keyword CAT would be entered and repeated just as the word PLAN, but your filled in keyword blank spaces would look like this: C A T C A T C A T C A T. As you can see, whatever the keyword is**,** it is repeated over and over above each letter of the ciphertext until there is a keyword letter above each ciphertext letter. Now we have to decipher the ciphertext (code) into plaintext.

Look at the table on page 3. You will see the heading Plaintext Alphabet enclosed in a horizontal rectangle. These are the plaintext letters we will be looking for. The letters that will give us the readable text. The word Keys appears in an elongated rectangle to the left. The letters in this vertical row are the corresponding keyword letters. The remaining letters contained in the large square represent the ciphertext (code letters). For example, if you know the keyword letter is P and the ciphertext letter is K you can find the corresponding plaintext letter T. Locate the keyword letter P in the left Key column. Follow the yellow line directly over to the right until you find the ciphertext letter K. Now follow the yellow line straight up to the plaintext alphabet, which gives you the letter T. This is how the Polyalphabetic Table is used.

Now we can go back to our Sample 1 example at the top of the page. Using the table on page 3, locate the first keyword letter P in the left column. Follow a line horizontally until you find the corresponding ciphertext letter K. Now go directly up that row to the top and you will have your first plaintext letter which is T. Write the letter T under the ciphertext letter K on the Sample 1 ciphertext sheet above. Now for the second plaintext letter. Locate the keyword letter L in the left column of the table. Follow a line directly over to the right until you find the corresponding ciphertext letter Q. Follow the row straight up to the top where you get your second plaintext letter H. Write that letter in the plaintext column below the ciphertext letter Q. Continue this procedure until you complete the plaintext. Fill in your completed plaintext on top of the next page. You will find the correct plaintext on the bottom left corner of the next page. I recommend you complete Sample 1 **before** checking.

Important: Punctuation marks and numbers are used throughout a composition. There are no punctuation marks or numbers in the polyalphabetic table. Punctuation marks and numbers are transferred as is onto the Plaintext line of your Ciphertext sheet.

Sample 1 Plaintext

_____

Write completed Sample 1 plaintext here.

Discovering the Title of a Trithemian Web™

I have designed a small Trithemian Web™ cipher for you to use - Sample 2 (next page). Print the page. You should be able to read the code if you reviewed the Sighting instructions. If you have not done so, I recommend you do that before continuing.

Here we will introduce the use of letter numbers. You may have noticed that there are no numbers or punctuation indicated within the polyalphabetic table. Numbers and punctuation are represented in a Trithemian Web™ as you would normally see them. The Trithemian Web™ will divulge the letter numbers that reveal the title of the piece.

When you decipher a Trithemian Web™ you will need a ciphertext sheet, or multiple sheets if a piece has abundant lettering. You can make your own sheet or use the one on the last page.

The keyword used in Sample 2 is CUB.

Letter numbers reveal the title of a Trithemian Web™. Fill in punctuation and numbers on the Ciphertext lines as you see them in the piece, then transfer them to the Plaintext line as is. Familiarize yourself with this methodology by reviewing the ciphertext sheet on page 7.

After the final punctuation mark in a Trithemian Web™, the numbers defining the title of the piece begin. Below is a section of the ciphertext sheet on page 7. Numbers and punctuation are simply transferred from the Ciphertext (C) line to the Plaintext (P) line since there are no listings in the polyalphabetic table for punctuation or numbers.

K	B	C	U	B	C	U	B	C	U	B	C	U	B	C
C	?	2	3	-	1	1	-	1	5					
P	?	2	3	-	1	1	-	1	5					
N	42	43	44	45	46	47	48	49	50					

Dashes separate the numbers. Notice the 2 and 3 are placed on individual spaces just as they are read in the Sample 2 composition. But these numbers are not used individually. The 2 and the 3 actually represent the number 23. The same for the 1 and 1. The two represent the number 11. The same with the 1 and 5. They represent the number 15.

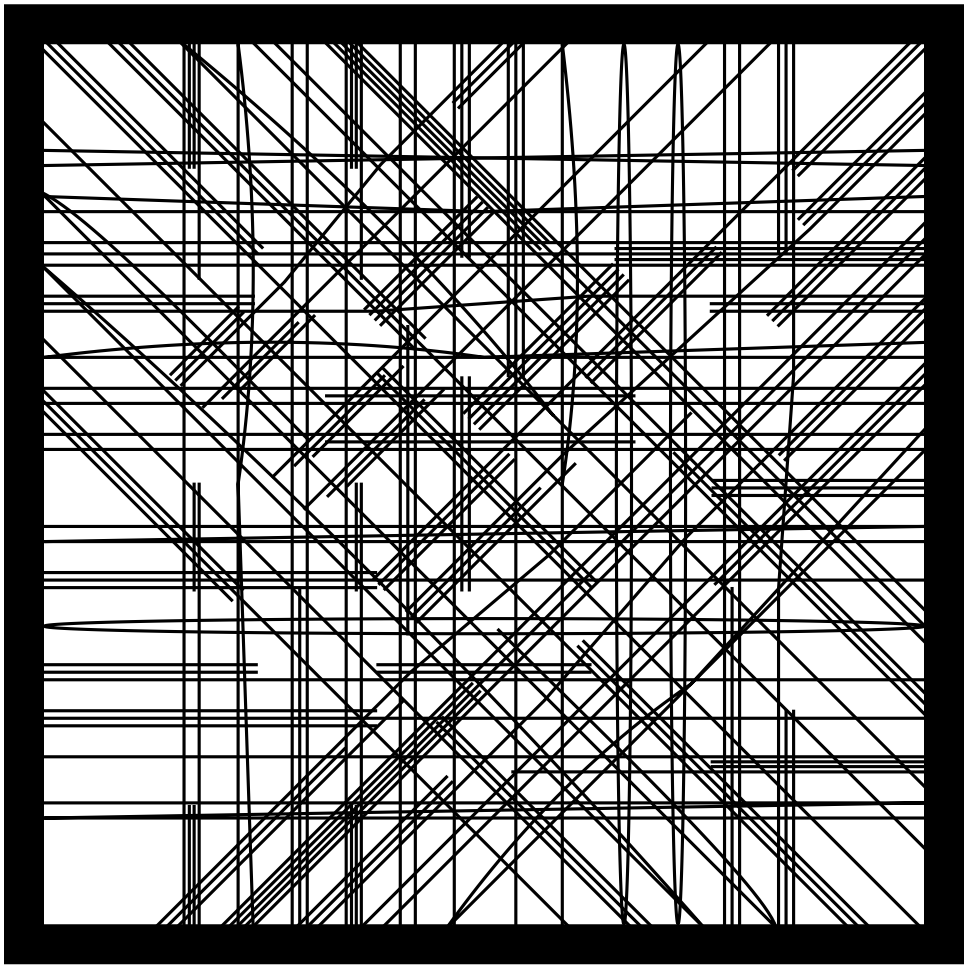
The three numbers - 23 11 15 - designate the plaintext letters that form the title.

The answers to Sample 2 are at the bottom of page 6. **Do not peek!** Decipher Sample 2 **first**.

Answer: The Time Is Now

Sample 2

This is a simple, encrypted Trithemian Web™ without blended graphics or coloration. Since this exercise is about using the polyalphabetic table, I filled in the keyword (CUB), ciphertext, and letter numbers on a Ciphertext Sheet (next page). Print this page and read the ciphertext in this simple Trithemian Web™ composition. Observe how the letters in this piece were transferred to the Ciphertext Sheet.



Start here.

Sample 2 Ciphertext Sheet

Keyword	C	U	B	C	U	B	C	U	B	C	U	B	C
Ciphertext	G	R	U	G	H	F	T	P	O	O	U	Z	T
Plaintext													
Character Number	1	2	3	4	5	6	7	8	9	10	11	12	13

K	U	B	C	U	B	C	U	B	C	U	B	C	U	B
C	L	D	C	L	F	T	P	U	M	N	J	T	F	O
P														
N	14	15	16	17	18	19	20	21	22	23	24	25	26	27
K	C	U	B	C	U	B	C	U	B	C	U	B	C	U
C	T	N	.	H	H	R	S	W	K	X	R	U	S	M
P			.											
N	28	29	30	31	32	33	34	35	36	37	38	39	40	41
K	B	C	U	B	C	U	B	C	U					
C	?	2	3	-	1	1	-	1	5					
P	?	2	3	-	1	1	-	1	5					
N	42	43	44	45	46	47	48	49	50					

Use the polyalphabetic table to decipher each ciphertext letter. Remember, there are no spaces between letters. After you decipher all the letters you can add the word spacing when you write the message body - the plaintext letters you just deciphered.

Write the message body here.

Use the letter numbers at the end of the Ciphertext Sheet to reveal the title of Sample 2. Write the title below. Trithemian Web™ titles may be one or more words. You will be able to see that immediately when you write the title's letters.

Note: Trithemian Web™ compositions may contain numbers that are not meant to be associated with the title. So numbers within the message body are not confused, the word TITLE will appear in the sentence preceding the final set of numbers.

Message Body: The tiger is an endangered species. Will you help?
Title of the piece: SAD

Ciphertext Sheet

100 Characters

Keyword															
Ciphertext															
Plaintext															
Character Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**

K																
C																
P																
N	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**

K																
C																
P																
N	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**

K																
C																
P																
N	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**	**64**	**65**	**66**

K																
C																
P																
N	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**	**76**	**77**	**78**	**79**	**80**	**81**	**82**	**83**

K																
C																
P																
N	**84**	**85**	**86**	**87**	**88**	**89**	**90**	**91**	**92**	**93**	**94**	**95**	**96**	**97**	**98**	**99**	**100**

Reminder: The polyalphabetic table has **no** provision for punctuation or numbers. When you see these symbols in the Ciphertext simply write them as they appear on the Plaintext line. In addition, you will run across a symbol in the Ciphertext that indicates a blank space. Just leave that Plaintext space blank. You will be filling in those letters with the answer to a question. The Character Number refers to that character's position in the container being deciphered. Once deciphered, the containers are read in order from top to bottom, left to right - C1, C2, C3, etc.

Final Container - Ciphertext Sheet

Keyword																
Ciphertext																
Plaintext																
Character Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
K																
C																
P																
N	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
K																
C																
P																
N	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
K																
C																
P																
N	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
K																
C																
P																
N	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83
K																
C																
P																
N	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
K																
C																
P																
N	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117

Note: At present all containers will have 100 characters with the possible exception of the final one. It may contain a few more or a few less characters. This ciphertext sheet takes that into account. Please use this sheet when deciphering the final container.

Containers

The sample Trithemian Web™ composition on page 6 is a single Container. My larger compositions will have multiple containers. Each container will be identified by the letter '**C**', meaning Container, followed by a number and a colon. For example, C1: identifies that container as number 1. There are consistencies in the Trithemian Web™ compositions.

1) Each container is read in four directions. That's explained in the Sighting instructions.

2) A container's identification number will always appear at the beginning of the contents.

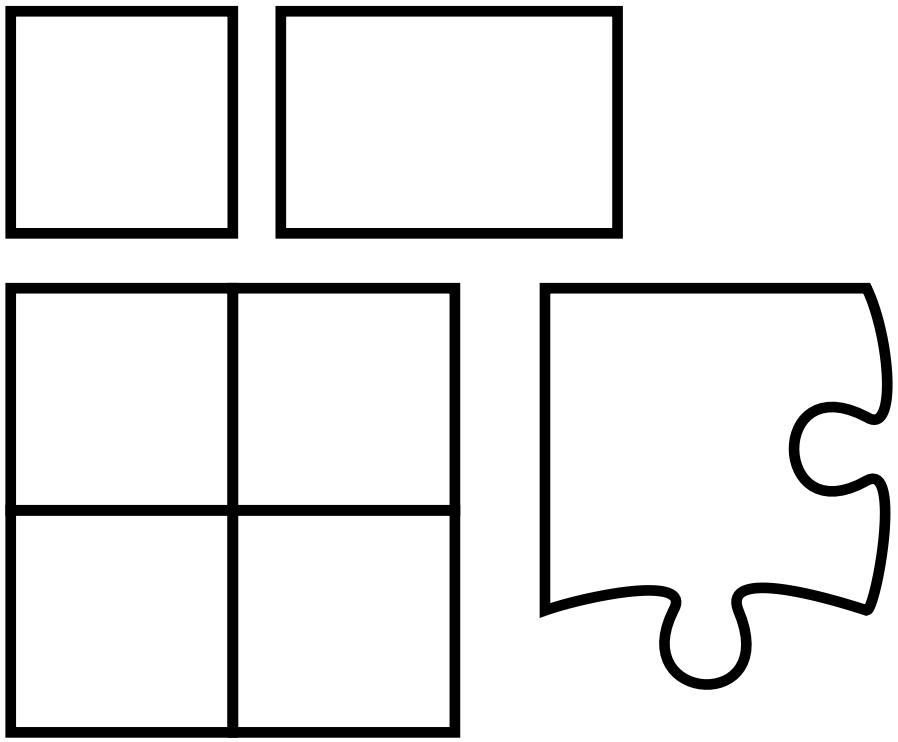
3) The graphics are always read from left to right beginning in Direction One as indicated in the Sighting instructions.

4) Each container is its own entity as far as deciphering its contents is concerned. Remember, the keyword is repeated over and over again on the Ciphertext Sheet enabling you to decipher that container. When you start deciphering the next container the process starts anew. ***Do not*** carry over the Keyword from the previous container.

For simplicities sake, let's say we have two containers that contain only 10 letters each. The Keyword is CAT. Please review the next page. It shows the correct and incorrect way to insert the Keyword into your Ciphertext sheets.

Shapes

The containers I use in a Trithemian Web™ will vary. Below are some examples.



Incorrect placement of the Keyword on the Ciphertext sheets for Container 1 and Container 2. Remember, each container is its own entity. The Keyword does **not** continue from container to container.

Ciphertext Sheet 1

Keyword	C	A	T	C	A	T	C	A	T	C
Ciphertext										
Plaintext										
Character Number	1	2	3	4	5	6	7	8	9	10

Ciphertext Sheet 2

Keyword	A	T	C	A	T	C	A	T	C	A
Ciphertext										
Plaintext										
Character Number	1	2	3	4	5	6	7	8	9	10

This is the correct way to enter the Keyword. It is started anew on the Container 2 Ciphertext sheet.

Ciphertext Sheet 1

Keyword	C	A	T	C	A	T	C	A	T	C
Ciphertext										
Plaintext										
Character Number	1	2	3	4	5	6	7	8	9	10

Ciphertext Sheet 2

Keyword	C	A	T	C	A	T	C	A	T	C
Ciphertext										
Plaintext										
Character Number	1	2	3	4	5	6	7	8	9	10

Important Note Regarding Multiple Containers

As mentioned previously, if there are multiple containers, which probably will always be the case, they are each designated by the letter **C** followed by the container's number - C1, C2, C3, etc. The designation letter **C** will appear in the Plaintext when the Ciphertext has been deciphered.

I want to expand on the use of the numbers to identify the title of a Trithemian Web™. Review page 5 to see how the numbers 23 -11-15 designate the plaintext letters on the completed Ciphertext sheet - page 7. This example represents a single container. What if there are multiple containers and the corresponding character numbers that make up the title come from different containers?

Here's how that will work. First I will designate the container number followed by a colon and then the character number. Here is an example of the sequence.

C1:14-C4:85-C5:27-C2:2-C8:43

This sequence does not relate to anything. It's just an example. The first letter of the title of the piece would come from container 1 character number 14. The second letter of the title would come from container 4 character number 85, etc.

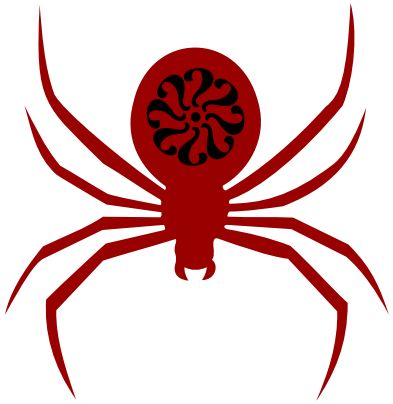
Important: There may or may not be blank spaces on the last container to write the title of the piece. Just write the title on the back of a ciphertext sheet or a blank piece of paper.

Note: At some point new Trithemian Web™designs may have the containers out of order. That's why each container is numbered. I just thought I would let you know in advance.

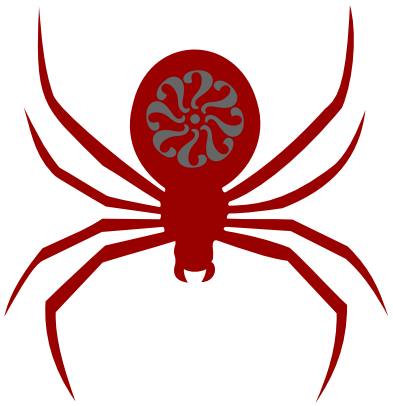
Suggestion: After you have decrypted all the containers, I would take a blank sheet of paper and write the plain text using the proper word spacing. This will make the message flow, making it easier to understand.

Important Note Regarding the Keyword

If you intend to photograph the separate containers of a displayed Trithemian Web™ in order to decipher the piece you first need to know where the keyword is located. Check the spider.



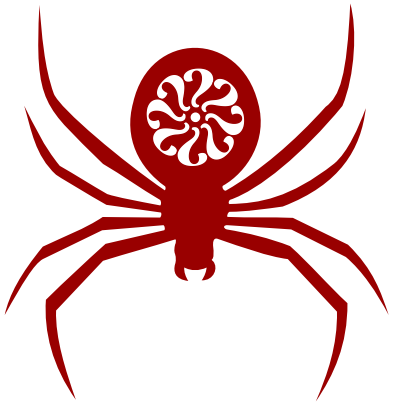
A red spider with black question marks. This indicates that the keyword is hidden within the spider itself. To view the keyword you need access to the original, digital file. You must purchase that piece to get the file and instructions as to how to unveil the keyword and other aspects of that Trithemian Web™. Alternatively, you may be able to borrow the digital file from the owner. Good luck with that.



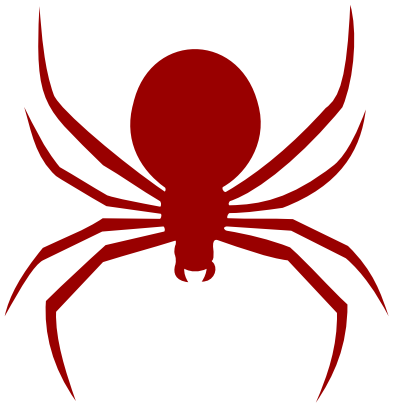
A red spider with gray question marks. This indicates the keyword is within the body text, in readable letters surrounding the piece or subdued letters appearing under the linear graphics. If you don't have the digital file, and if you are looking at a physical piece - a canvas or a LumaChrome HD - you can photograph each container, bring the images into a photo editing program, resize each one to fit on a standard sheet of paper and print them out. Then follow the instructions for deciphering a Trithemian Web™.

Using this methodology you will be able to decipher the body text and unveil the title of the piece. There may be other inclusions for which you will need access to the digital file.

So where is the keyword located if it is within the linear graphics? It will be the first ***plaintext*** letters in container 1 (C1). Those letters will be followed by a colon, the letter C, the number 1 and another colon. The C1 verifies that you are viewing container 1. Everything after that last colon is ciphertext. Write those letters (the keyword) and :C1: in the first plaintext spaces on your ciphertext sheet and then continue deciphering the piece.



A red spider with white question marks. This indicates that the keyword is contained in the piece's stereogram, if it has one. The only exception to this rule is Trithemian Web™ One. Its stereogram contains the trithemian website URL.



A red spider with no question marks. This indicates that the keyword will be broadcast at a specific time on Twitter and other media outlets.