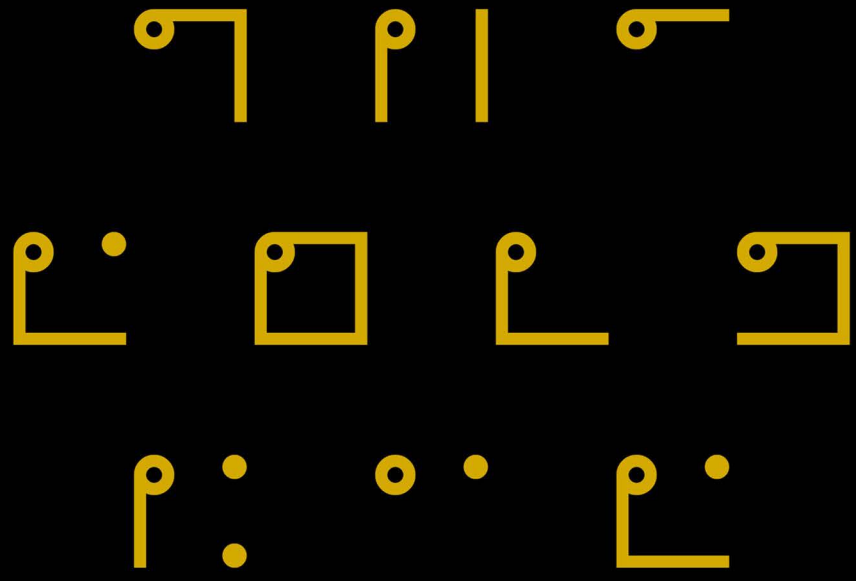
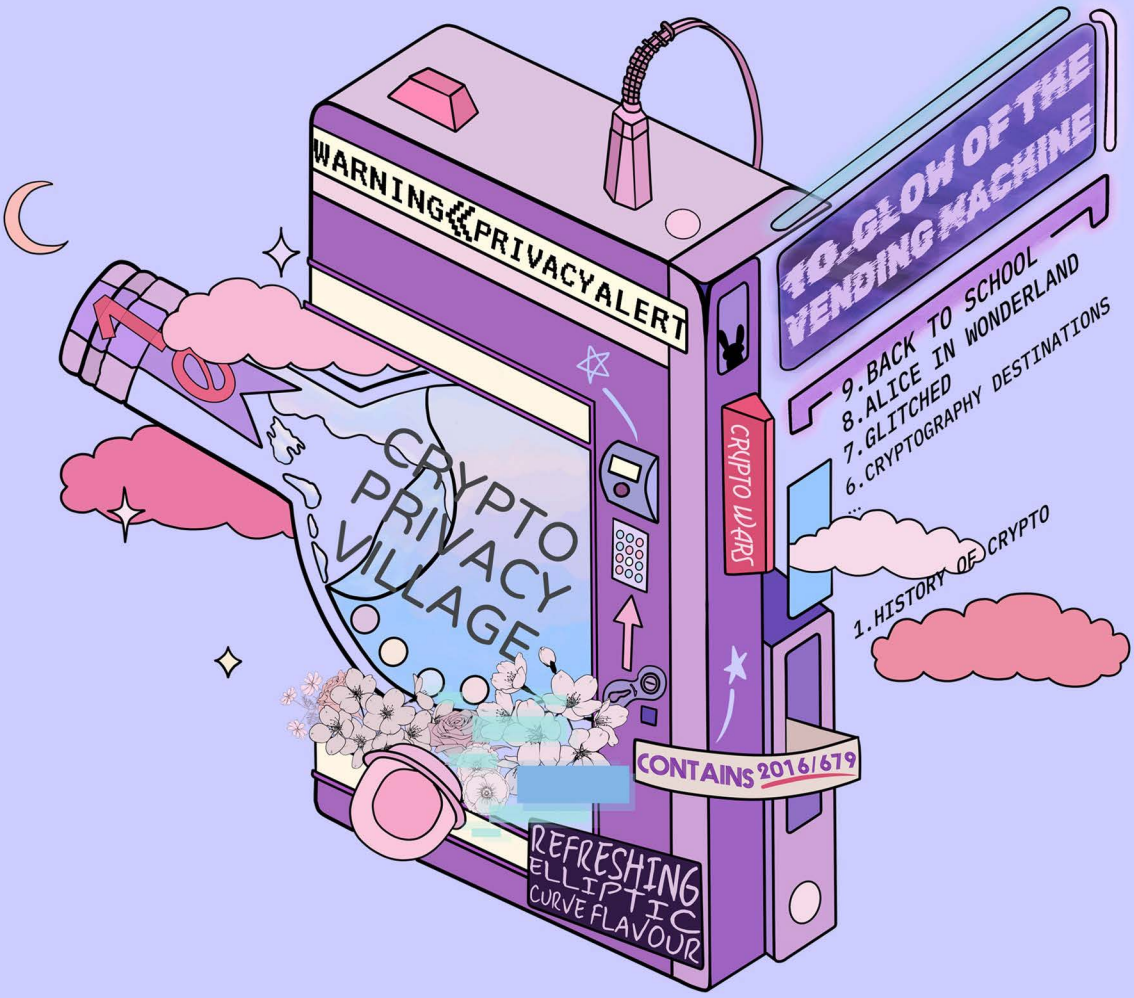
CRYPTO & PRIVACY VILLAGE 2023





CRYPTO + PRIVACY VILLAGE


WELCOME

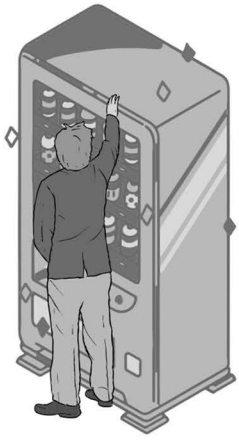
Forward

Welcome to the Gold-Bug Contest presented by the Crypto and Privacy Village at DEF CON 31. This is our first time making a magazine dedicated to this contest and it was both fun and challenging to put together. We hope the puzzles and content contained herein will also be both fun and challenging.

If you are not familiar with the Crypto and Privacy Village, we are a non-profit dedicated to making information about privacy, particularly digital privacy, and cryptography available and accessible. As well as this contest, we host talks and workshops. Please make sure to come visit us at our village space, at cryptovillage.org, or on social media @cryptovillage! Oh, and if you were wondering, "crypto" means cryptography.

This year, the Crypto and Privacy Village theme is "In the Glow of the Vending Machine." The puzzles will share this theme, some more directly than others.

The contest is formatted as a puzzle hunt, which is a series of challenges, each with its own unique puzzling clues, which work together almost like a scavenger hunt getting you toward a final destination. In our case, there is an overarching "meta" puzzle which requires you to complete preliminary puzzles in order to solve. Physical versions of many of the individual puzzles for this contest are contained in this magazine, but some are only available digitally or as a hybrid with some physical and some digital aspects.



IN THE GLOW OF THE VENDING MACHINE

As you encounter each new puzzle, the first challenge is to figure out what needs to be done. While the clues will often hint at a direction, the puzzles do not come with explicit instructions for how to proceed. This year we made a special effort to include puzzles accessible to all skill levels – from the newest novice (even kids!) to seasoned puzzle hunters. While we want to provide some challenges, we still want it to be fun! So, if you find yourself stuck, either find our table in the contest area or reach out for a hint in the #cpv-gold-bug-text channel on the official DEF CON Discord server. Also feel free to stop by (in the contest area or on Discord) just to chat, tell us how very much you enjoy our puzzles, or let us know what frustrates you (and whether it's the good kind of frustration that makes the "A-ha!" moment all the sweeter, or if it's the bad kind that makes you want to stop puzzling and knock over the vending machine). We love meeting fellow puzzle lovers and getting to talk about all things cryptography.

Please enjoy this magazine and happy puzzling!

Sincerely,

The Gold Bug Puzzle Team

@0xCryptok @tseven @llamaprincess @pleoxconfusa @avi

All puzzles can be accessed and answers can be submitted at:

https://bbs.goldbug.cryptovillage.org/

An Introduction to Cryptographic Ciphers

As an introduction to basic cryptographic ciphers, let's start with a definition. A cipher is the result of hiding or encoding a message. The practice of creating such ciphers is called cryptography. From the most basic pen and paper cipher to the most complex computer systems, the goal is essentially the same: keep one or more pieces of information private only to those who should be able to access it.

Some of the earliest examples of cryptography appearing in popular culture come from Edgar Allan Poe's "The Gold-Bug" (for which this contest is named) and Sir Arthur Conan Doyle's "The Adventure of the Dancing Men." In "The Gold-Bug," a cipher is decoded which ultimately leads to buried treasure.

In "The Adventure of the Dancing Men," Sherlock Holmes is on a case with mysterious pictures of men in various strange positions. Holmes identifies this as a substitution cipher where each unique position represents a letter of the alphabet. See Table 1 for illustrations of Gold Bug, Dancing Men, and several other substitution ciphers which map to the English Alphabet.

In the United States, the English alphabet is the most common means of conveying information, and therefore, most substitution ciphers use the twenty-six letters of the English Alphabet as the basis of substitution. There are infinite options for substitution ciphers. Instead of letters, one can use numbers, pictures, symbols, or non-visual cues like textures, noises, even flavors or smells. As long as there are twenty-six distinct options, they can represent the English alphabet. In Table 1, we illustrate some examples of substitution ciphers, including Morse code where the dots and dashes are visual ways of conveying the noises ("dits" and "dahs") that telegraph operators send back and forth. Real world examples of these used everyday include Braille, which conveys information through texture, and American Sign Language, which uses visual hand gestures to represent letters, numbers, words, and phrases.

Substitution Cipher Special Mention: ROT13

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

ROT13 (also called Caesar shift 13 or rotate 13) is the simplest substitution cipher used in English and is often used in puzzles to convey optional hints to solvers. To encrypt a message using ROT13, each letter is replaced with the letter 13 places after it in the English Alphabet. Because 13 is exactly half of 26 (the size of the English alphabet), you can decrypt ROT13 by simply counting 13 places again! The Encryption algorithm is exactly the same as the decryption algorithm, as illustrated above!

The below text was encrypted using ROT13. Decrypt it to uncover Ralphie's decoded Orphan Annie secret decoder ring message from the 1983 film A Christmas Story!

OR FHER GB QEVAX LBHE BINYGVAR

Table 1: Examples of Substitution Ciphers

English Alphabet	Alpha -Index	Gold Bug*	At-bash	Caesar (shift 13)	Morse Code	Braille	Binary Index	Nycto-graph	Pig-pen	Dancing Men**
A	1	5	Z	N	.-	⠁	00001			
B	2	2	Y	O	-...	⠂	00010			
C	3	-	X	P	-.-.	⠃	00011			
D	4	†	W	Q	-..	⠄	00100			
E	5	8	V	R	.	⠅	00101			
F	6	1	U	S	..-.	⠆	00110			
G	7	3	T	T	--.	⠇	00111			
H	8	4	S	U	....	⠈	01000			
I	9	6	R	V	..	⠉	01001			
J	10	,	Q	W	.---	⠊	01010			
K	11	7	P	X	-.-	⠋	01011			
L	12	0	O	Y	.-..	⠌	01100			
M	13	9	N	Z	--	⠍	01101			
N	14	*	M	A	-.	⠎	01110			
O	15	‡	L	B	---	⠏	01111			
P	16	.	K	C	.--.	⠐	10000			
Q	17	$	J	D	--.-	⠑	10001			
R	18	(	I	E	.-.	⠒	10010			
S	19	)	H	F	...	⠓	10011			
T	20	;	G	G	-	⠔	10100			
U	21	?	F	H	..-	⠕	10101			
V	22	¶	E	I	...-	⠖	10110			
W	23	]	D	J	.--	⠗	10111			
X	24	¢	C	K	-..-	⠘	11000			
Y	25	:	B	L	-.--	⠙	11001			
Z	26	[	A	M	--..	⠚	11010			

*Neither "The Gold-Bug," nor "The Adventure of the Dancing Men" stories included the full alphabet. Missing Gold-Bug cipher letters use the rumkin.com extrapolation.

**Dancing Men are using the Gutenberg Labo font. (https://www.fontspace.com/gl-dancingmen-font-f12468)

One common method of converting text to numbers is to use a table or grid. The English alphabet, with 26 letters, is one character too long to perfectly fit into a square grid. To get around this, cryptographers have had to get creative. For instance, American Prisoners of War in Vietnam arranged the alphabet into a five-by-five grid by using the phonetic C instead of K to spell words. The POWs would talk to one another by tapping on the walls, spelling words letter by letter by tapping the number of lines down, then columns across (for example, the letter S would be 4 taps for lines down followed by 3 taps for columns across).

Table 2: Example of a Tap Code 5x5 Grid

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

Another grid formation could arrange the alphabet around a rectangle with six letters on the shorter sides, and seven letters on the longer sides—allowing for other types of geometric representations. For example, this could map to a room with photos on the wall to correspond to the positions. Or perhaps a workbench with tools scattered around. See? Infinite options!

Table 3: Example of the English Alphabet as a Rectangle

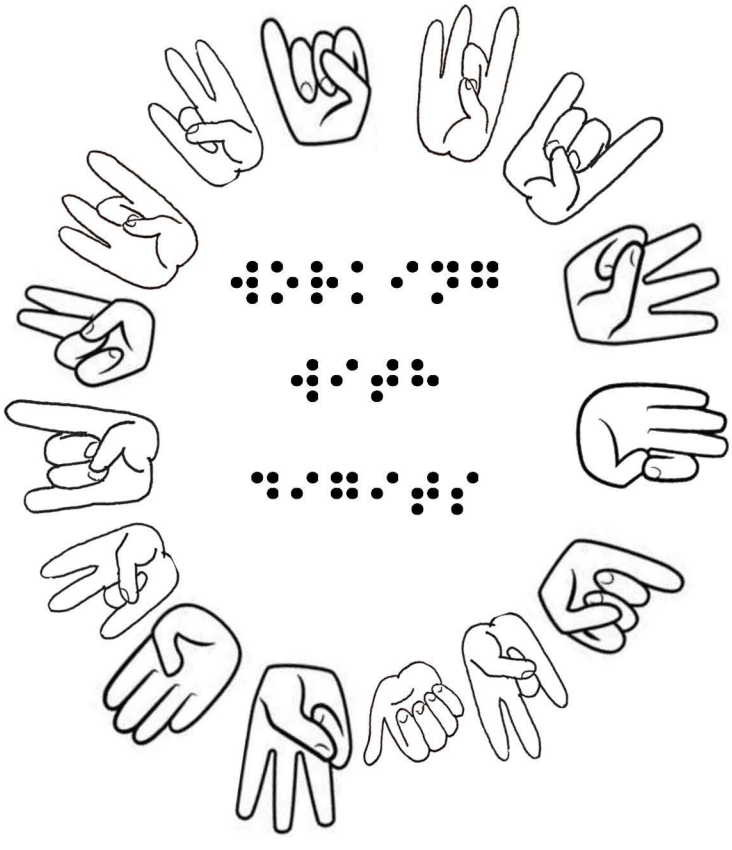
	G	H	I	J	K	L	M	
F								N
E								O
D								P
C								Q
B								R
A								S
	Z	Y	X	W	V	U	T	

Beyond substitution ciphers, another simple encryption technique is called transposition. In transposition ciphers, the letters in a message are rearranged according to an algorithm. While substitution ciphers tend to be most effective with short texts (when frequency analysis is difficult), transposition ciphers are most effective in longer texts (when it is difficult to identify likely anagrams). By combining transposition and substitution techniques, it is possible to generate simple but powerful cipher systems that would pose a challenge to even the most seasoned cryptographers!

The simple encryption methods covered here are only effective if the encryption algorithm itself is kept secret. On the other hand, modern encryption methods (like the ones used to protect the content of your encrypted internet traffic from man-in-the-middle snooping) use publicly known encryption algorithms that are based on mathematical problems proven to be resistant to analysis and cracking by even the most advanced super computers. However, Cryptologists and privacy advocates fear that advances in computer science will someday in the "not-too-distant future" overcome these mathematical protections through new quantum computing capabilities, requiring adoption of new post-quantum cryptography. But that's another story for another time.

The vast array of ciphers, simple and complex, available to encrypt information is an infinitely interesting topic. Hopefully these brief descriptions have whet your appetite for learning more about cryptographic ciphers and trying your hand at solving some of the ciphers in the remaining pages of this magazine, which offer a range of difficulty and utilize many, many techniques.

Good Luck!



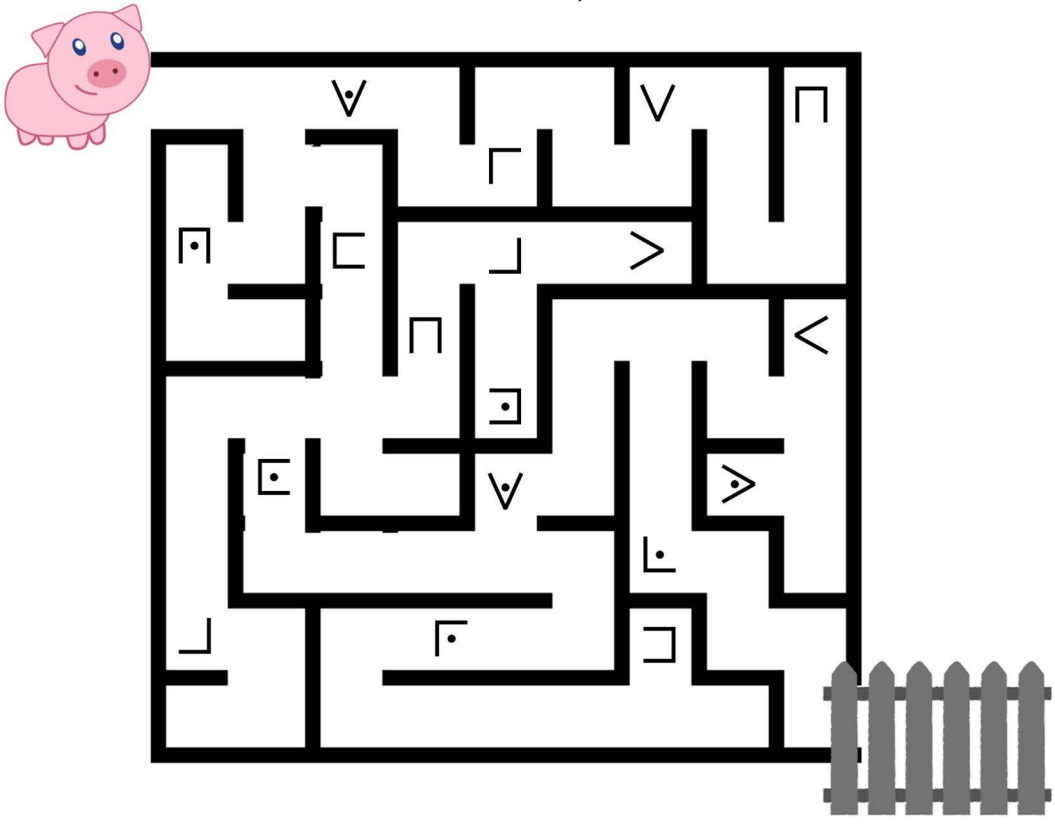
Junior Cryptographer's Corner

Welcome puzzle hunters! The tables and explanations in An Introduction to Cryptographic Ciphers (pages 6-9) will be especially helpful in solving these puzzles. See if you can solve these five challenges to answer the riddles. Once you have solved them all, take a crack at solving the Junior Meta. Make sure to submit your meta-answer online! Good luck!

https://bbs.goldbug.cryptovillage.org/

An a-MAZE-ing Pig

Help Sir Francis the Pig get back to the pig pen! Be sure to pick up any symbols along the way!



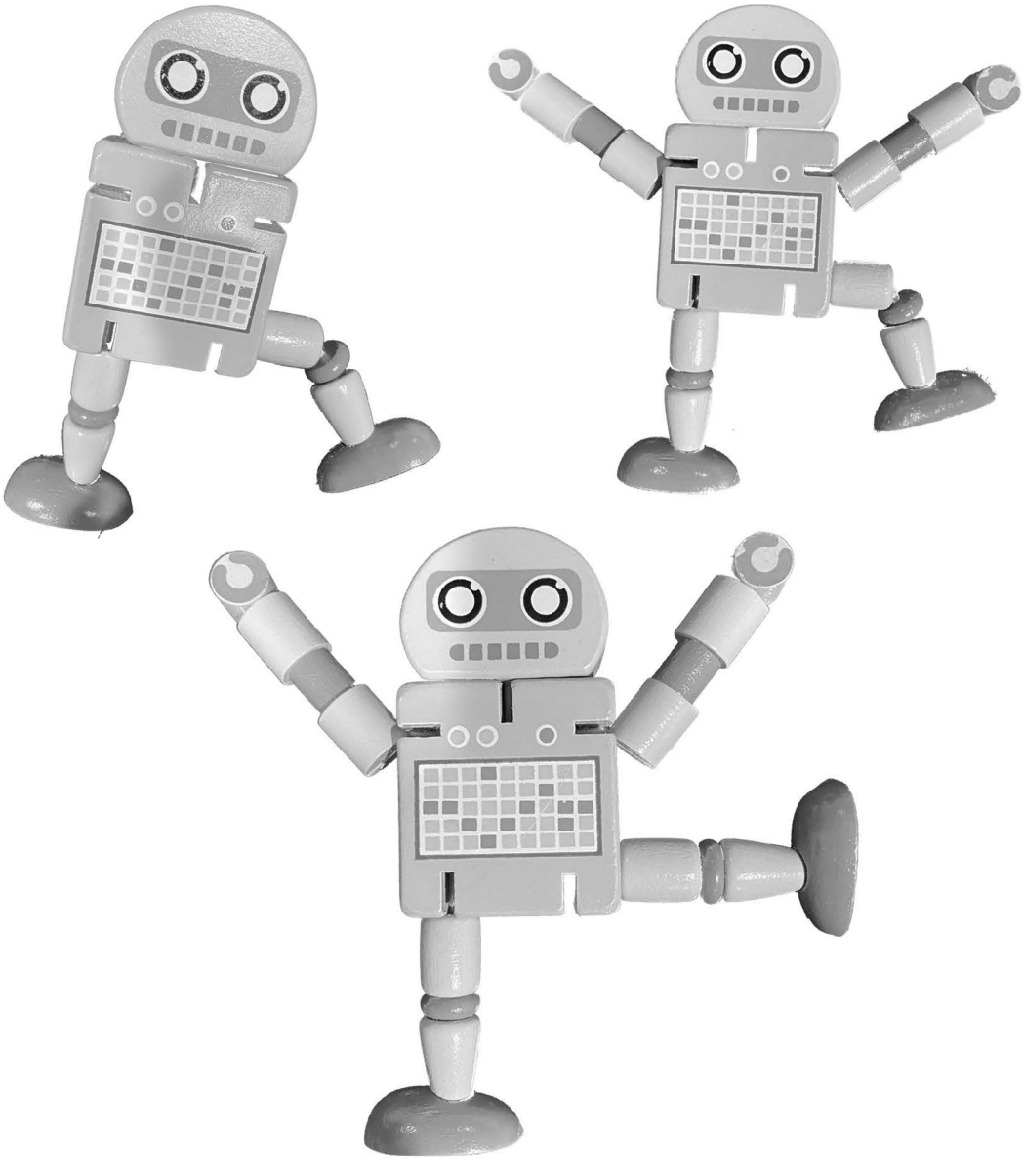
Why did the chicken get cut from the baseball team?

He only hit ____ ____ ____ ____ balls

13 12 8 9

Dancing Robots

Clink, Clank, and Clunk love to boogey! But I can't help but think they're trying to tell us something with their dance moves!



What do a lawyer and a dancer in a limbo contest have in common?

They both passed the ____ ____ ____

3 2 11

Mind your Manners

Miss **Dottie** is sending out invitations for her fancy tea party in a **dash**. Can you help her solve the riddle? Make sure to **dot** the i's and **cross** the t's!

Please join us for tea, ice cream, and friends!

Monday, April 25, 2022

4 PM, Awesome Castle

RSVP by March 31, 2022

What kind of toy should you never lick?

A toy ____ ____ ____

4 5 15

Backstage

The famous actress Elvira Enigma will only answer her dressing room door if the proper code is **tapped**. Elizabeth and William each remember one part to **tap** for each of the three knocks. Help them put the parts together to solve the puzzle.

Knock one:

Elizabeth: 3 Knocks William: 4 Knocks

Knock two:

Elizabeth: 2 Knocks William: 1 Knock

Knock three:

Elizabeth: 2 Knocks William: 1 Knock

What would you call it if William and Elizabeth went head to head in a knocking contest?

A Knock ____ ____ ____

7 1 6

Same or Different?

Some animals have multiple common names. But some other animals have close cousins who are similar, but different!

Figure out which animal names refer to the same species and which names refer to different species!

If they are the same, place a 1 in the blank. If they are different, place a 0 in the blank. Use the table on page 7 and see if you can solve the riddle below!

Animal 1	Animal 2	Same = 1, Different = 0
Cougar	Puma	
Wolf	Coyote	
Turtle	Tortoise	
Newt	Salamander	
Alligator	Crocodile	
Horse	Zebra	
Orca	Killer Whale	
Llama	Alpaca	
Frog	Toad	
Crayfish	Crawdad	

What is a circle's favorite dish? ____ ____
10 14

Junior Meta Puzzle Answer:

____	____	____	____	____	____	____	____	____	____	____	____	____	____	____
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Think you solved it? Submit your answer online!

https://bbs.goldbug.cryptovillage.org

Everything Dispense-O

Vending Menu

0. WATER
1. CANDYBAR
2. JUICE
3. LOTTERYTICKET
4. CHIPS
5. CRACKERS
6. PASTRY
7. NOODLES
8. CHEWINGGUM
9. SOFTDRINK
10. POSTAGESTAMP
11. FRUIT
12. TOOTHBRUSH
13. GIFTCARD
14. SANDWICH
15. POPCORN
16. POSTCARD
17. NUTS
18. COOKIE
19. HEADPHONES
20. PRETZELS
21. COFFEE
22. NEWSPAPER
23. TRAINTICKET
24. BITCOIN

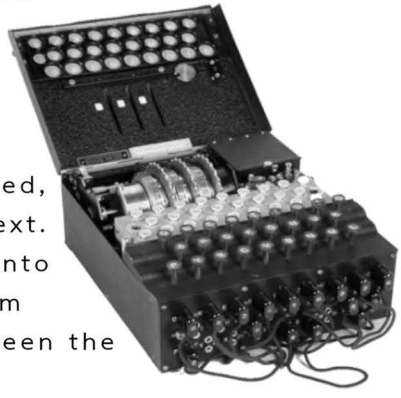
It seems our new vending machine got dropped off the truck when it was delivered. Now all of the contents have been shifted around and I'm not sure how to order my favorite snacks!

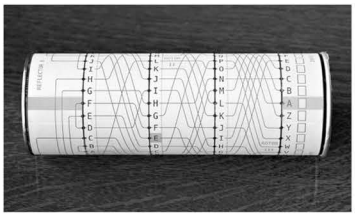

W A T E R S Q L X X S E F N K U
B X O C M A R W T J N D A N J V
J T Z S S G D K N A M E A D A V
R W V G Y Z X E Z A M R F C S K
Y I D Q Q N R G S Z N D T E O S
H A F O M C X N T Z Q G N Z L L
M H E X Z Y C D K Q O C D K W Z
D G I F J H G R P V D Q G Q L H
B X J K L W O E M S G Z E C A S
O L S Q Y F B R E L K J T F N S
E N Q F N H R N Q G U Z Q T C A
Z D H Z T P K T V S G P N E Q G
C M T H Y J W C O Z G R A M G L
B X N B F W Q T O Q C L H M C M
S Z M Q M X V C C S A Q X L N T
N Q D O R W W H U B W L F N H W
Everything Dispense-O
Vending Menu
0. WATER
1. CANDYBAR
2. JUICE
3. LOTTERYTICKET
4. CHIPS
5. CRACKERS
6. PASTRY
7. NOODLES
8. CHEWINGGUM
9. SOFTDRINK
10. POSTAGESTAMP
11. FRUIT
12. TOOTHBRUSH
13. GIFTCARD
14. SANDWICH
15. POPCORN
16. POSTCARD
17. NUTS
18. COOKIE
19. HEADPHONES
20. PRETZELS
21. COFFEE
22. NEWSPAPER
23. TRAINTICKET
24. BITCOIN

A Strange Machine

The Enigma machine is a cipher device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication... The Enigma machine was considered so secure that it was used to encipher the most top-secret messages.

The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plain text is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connectionsbetween the keys and the lights with each keypress.





You can build your own working enigma machine out of paper using the next pages in this magazine!

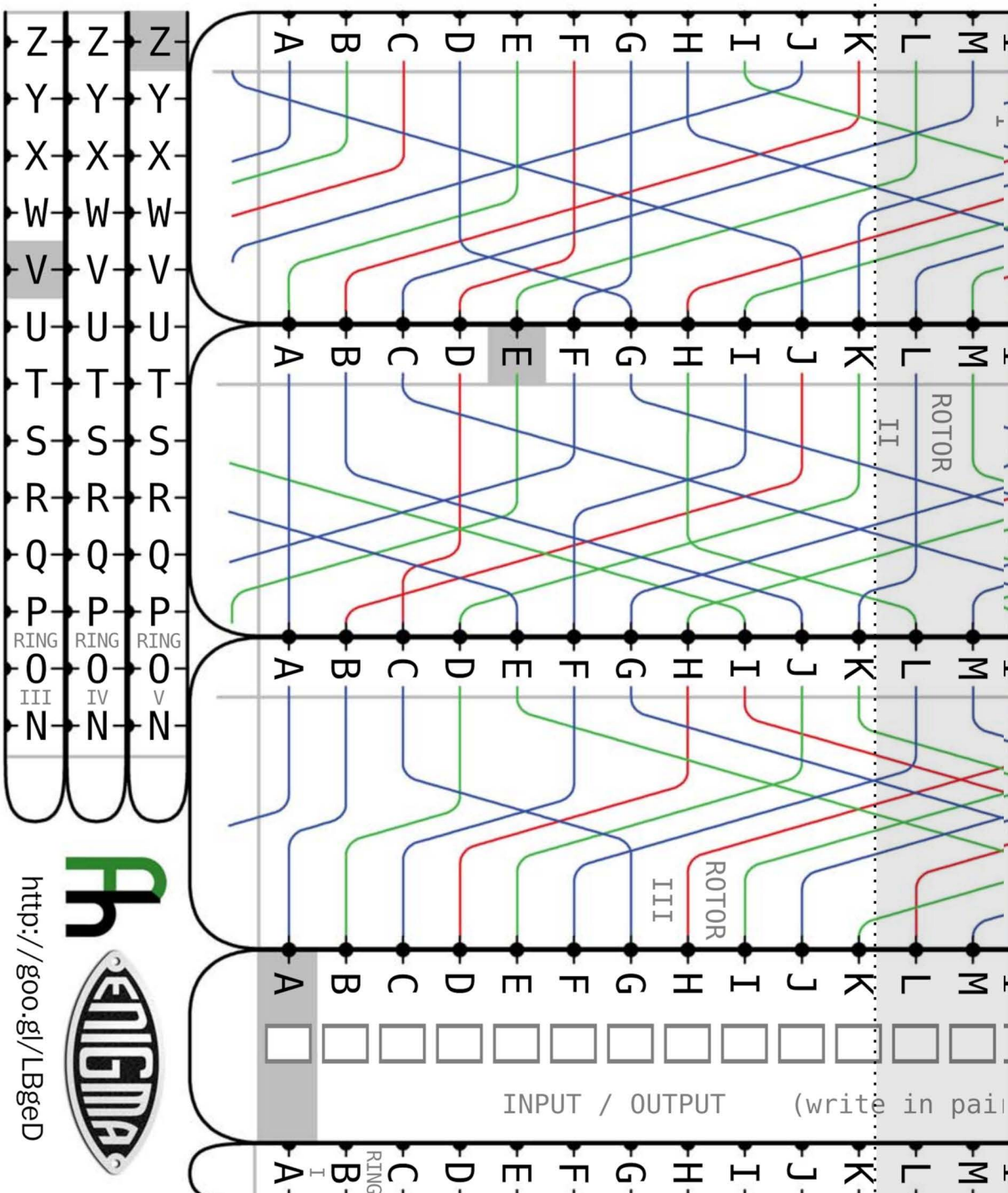
Give it a try and see if you can decode this message.

I F K I C N Y J K M A A F E Y

Reflector: B
Rotors: IV, I, III
Starting Positions: J B Q
Plugboard: SE, WG, FI, HQ, UA, PZ

Cut these pages out to make your own Enigma machine out of paper!
It will fit on a 75mm diameter tube that is 225mm long.

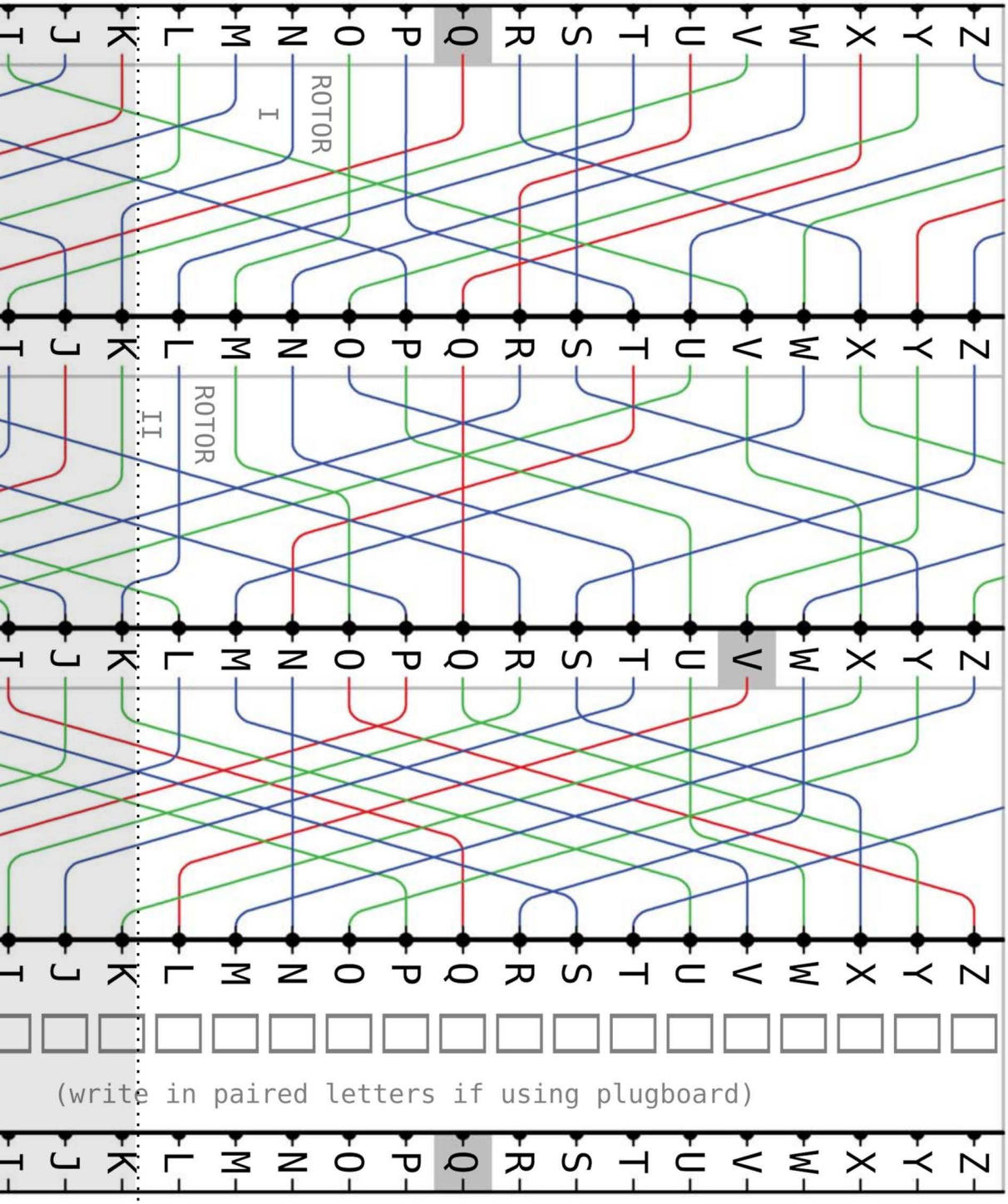
Paper Enigma machine for crisp tube v1.1 © 2012 Franklin Heath Ltd Reproduction pe



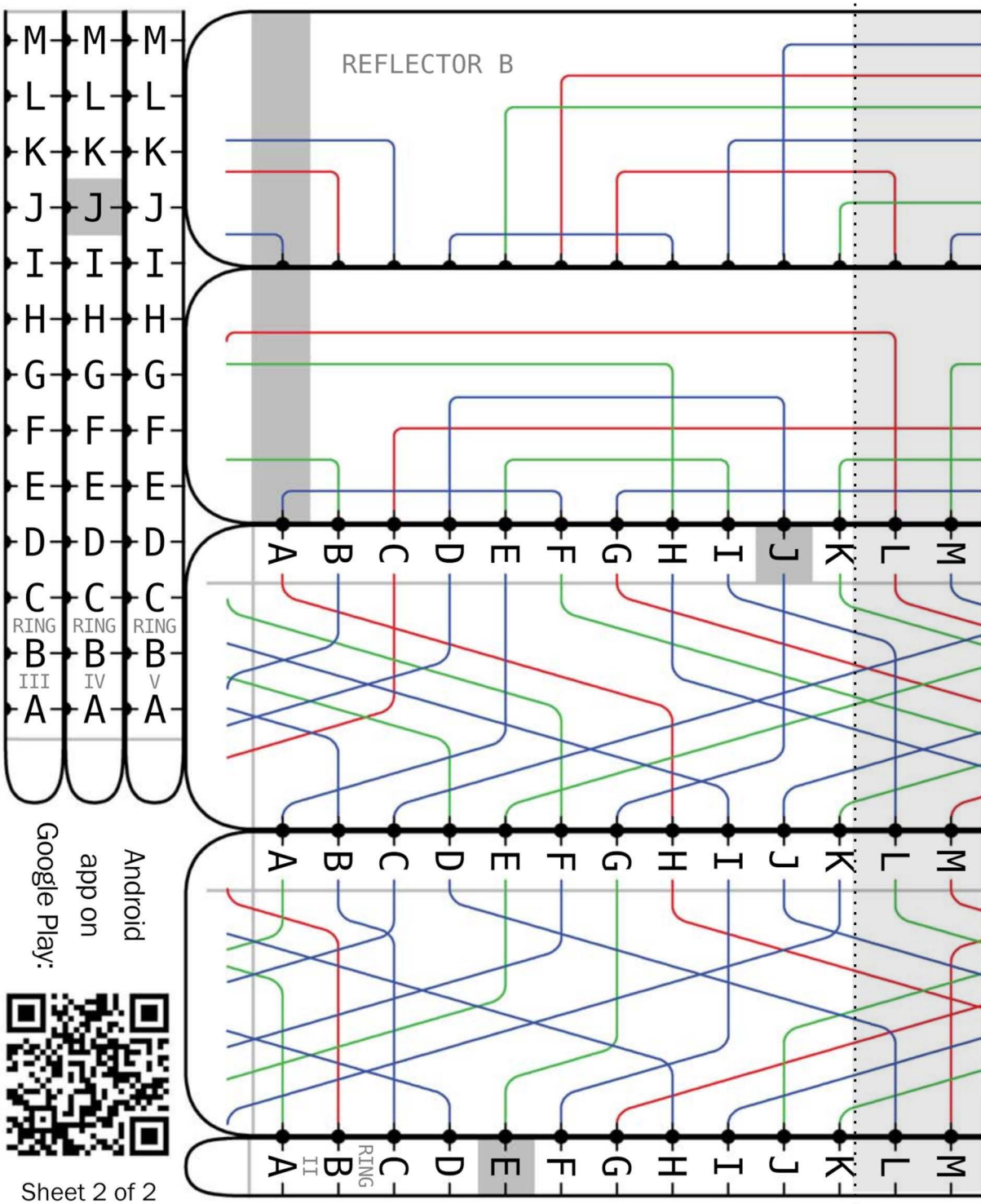
http://goo.gl/LBgeD

Sheet 1 of 2

If you can find some chips that come in a tube, it is probably the perfect size!



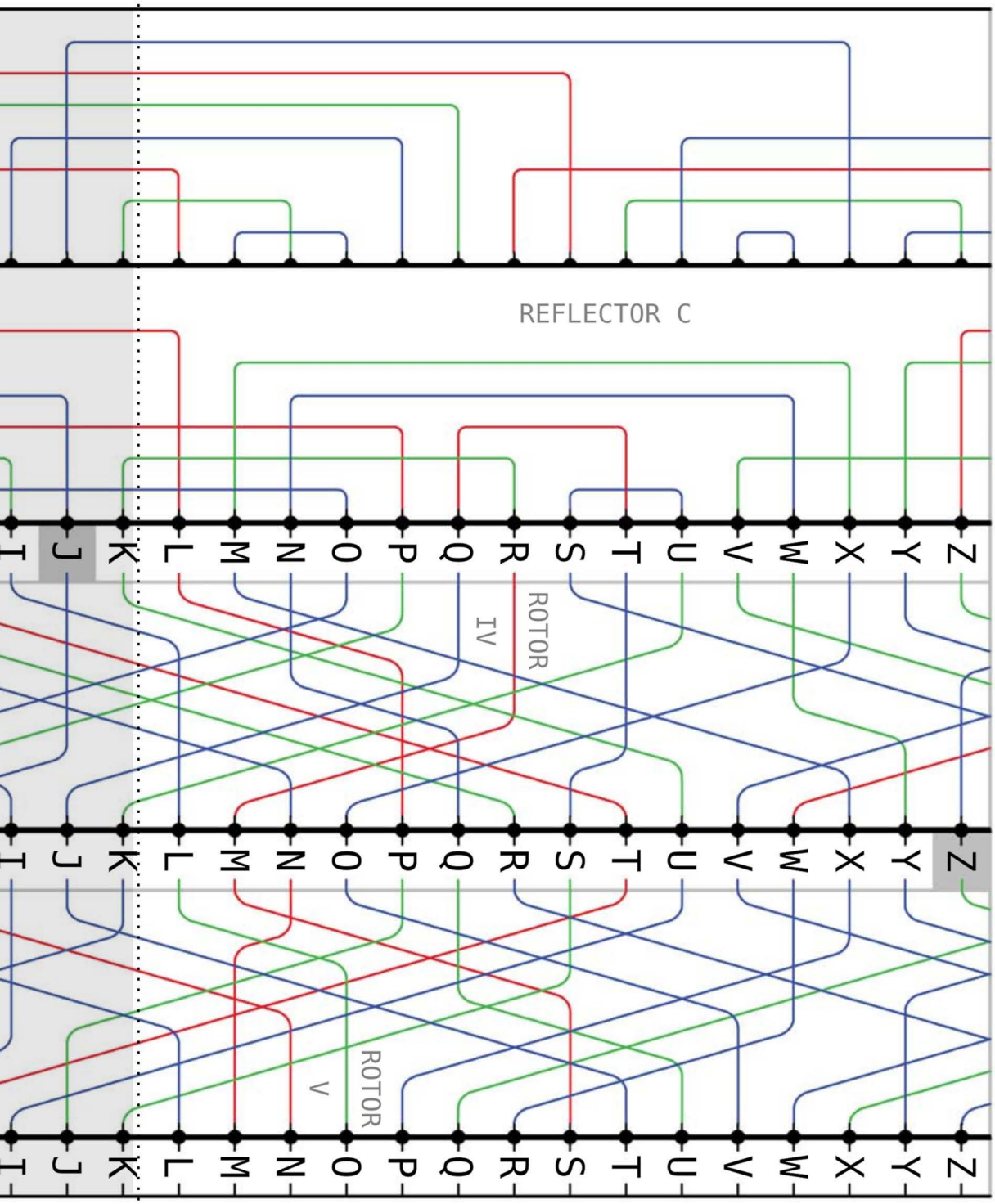
You can find the assembly instructions at
http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma



Google Play: Android app on

Sheet 2 of 2

You can also print these pages from the website if you'd rather not cut out your magazine!



Sudoku Break

Sometimes it's helpful to take a break and relax. We've compiled some of our favorite randomly generated Sudoku puzzles as mental yoga!

Also, In the spirit of generative algorithms, we've asked ChatGPT to tell us about some of our favorite cryptographers. We hope it confidently told us accurate things. Probably not relevant though. But seriously, they're totally not a puzzle. ;)

Ab, ernyyl, gur ovbtencuvrf ner abg n chmmyr. Whfg fbzr PungTCG sha!

1 WIRELESS

Sir Francis Bacon (1561-1626): Renowned philosopher, statesman, and cryptographer. He developed the Baconian cipher and introduced the concept of polyalphabetic substitution, laying the groundwork for future encryption techniques.

			2		7	6		
6		9			1		2	8
				3			4	
	8	3	1		4			6
				7				
			9		5	3	8	
	6			4				
3	4		5			8		7
		7	3		2			

2 KERNEL

	5		8			3		
	8	9	7		1			
	7		3			9		4
		6		3				
	3		4	1	2		7	
				5		2		
8		2			3		9	
			1		9	6	2	
		3			4		5	

Joan Clarke (1917-1996): British codebreaker and mathematician who worked at Bletchley Park during WWII, making significant contributions to cracking the Enigma code.

3 BINARY

Taher Elgamal (1955-present): Egyptian cryptographer known for his contributions to the development of the Elgamal encryption algorithm, a widely used public-key encryption system.

2	3	5	6					
								6
7	4		8	9	1			
	5						6	2
3			1		5			4
9	7						1	
			4	1	3		2	5
8								
					6	1	3	9

4 PARTITION

Elizabeth Friedman (1892-1980): Pioneering cryptographer whose work in codebreaking during World War II and groundbreaking research on frequency analysis established her as a trailblazing figure in the field.

	5				8	2		9
	1		2		9	6	3	
3						8	7	
				7			5	
			5		4			
	3			6				
	6	8						1
	7	3	9		1		4	
1		4	3				2	

5 FUNCTION

7			3	6	2			9
8	6						7	
						6	1	
		9		1	4			8
	1						5	
5			6	2		1		
	4	2						
	8						9	6
6			9	8	1			7

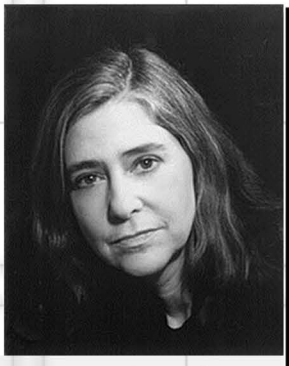
William Friedman (1891-1969): Distinguished cryptographer whose work in codebreaking and cryptanalysis during World War II laid the foundation for modern intelligence operations .

6 YIELD

5			8				6	
1	2	4		6	5			7
		9				1	4	
		8					1	
3				1				4
	5					7		
	1	2				8		
9			2	8		4	7	1
	7				4			2

Shafi Goldwasser (1958-present): Israeli-American computer scientist and mathematician, known for groundbreaking contributions to cryptography and complexity theory.

7 ALGORITHM



Margaret Hamilton (1936-present): American computer scientist and systems engineer. She led the team that developed the onboard flight software for NASA's Apollo missions, making significant contributions to the success of the moon landing.

1								6
2	9			5	4	3	8	
			6	8				1
	7					1		
		8	5		3	6		
		2					9	
5				6	8			
	6	4	7	2			3	9
7								8

8 OUTPUT BUFFER

Roberto Ierusalimschy (1959-present): Brazilian computer scientist and creator of the Lua programming language, widely used in various domains including game development, embedded systems, and scripting.

4		2	9				6	
		1	2		7			
			3				8	
		7	1					8
1	4	3				9	7	2
2					3	5		
	1				5			
			7		9	6		
	9				1	8		3

9 CODING

		9			7	6		3
	7	5	3			8	1	
			6					4
			9	6			3	5
				3				
4	8			7	5			
7					1			
	9	8			6	3	4	
5		4	8			1		

David Naccache (1967-present): French cryptographer and computer scientist. Naccache has made significant contributions to the field of cryptography, particularly in the areas of public-key encryption and smart card security. His research has advanced the understanding and development of secure communication systems.

10 MICROCHIP

		6		7	4	8		
8		9		3	5			7
								4
2				4				6
	5	1				4	9	
4				5				1
3								
9			7	6		3		2
		5	4	2		1		

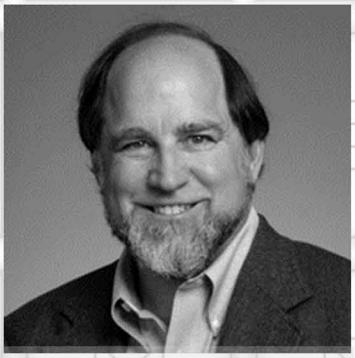
Rafail Ostrovsky (1961-present): Israeli-American computer scientist and cryptographer. Notable contributions in secure multiparty computation, privacy-enhancing technologies, and algorithmic game theory, advancing secure and privacy-preserving protocols.

11 COMPONENT

Pascal Paillier (1971-present): French cryptographer known for his development of the Paillier cryptosystem, a widely used public-key encryption scheme that enables secure computations on encrypted data. His work has had a significant impact on the field of cryptography.

	7		3					9
					7			
	3	1	8	4	5		2	
		9			2		6	
		8	6		4	9		
	5		7			8		
	9		2	1	8	7	5	
			4					
2					3		4	

12 NETWORKING



Ron Rivest (1947-present): American cryptographer and computer scientist. Co-inventor of the RSA encryption algorithm, Rivest has made substantial contributions to cryptography, security protocols, and computer algorithms. His work has had a profound impact on the field of computer science.

	3						8	4
		8	5	3				
	6		9		7	3		
					8	6		9
8		4				7		5
6		7	1					
		2	4		3		9	
				1	9	4		
9	4						5	

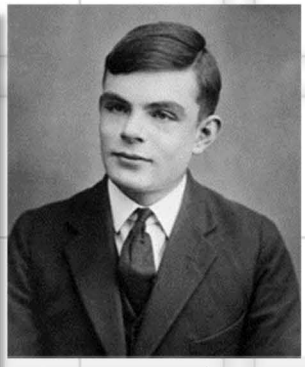
13 CONTROL

	2			9	4		1	6
	4							5
				1	7		8	
				3			6	9
		9	4		1	5		
4	3			5				
	8		1	2				
7							3	
5	9		8	7			4	

Adi Shamir (1952-present): Israeli cryptographer and computer scientist. Co-inventor of the RSA encryption algorithm and one of the pioneers of modern cryptography. His groundbreaking work has had a profound impact on secure communication and data protection.

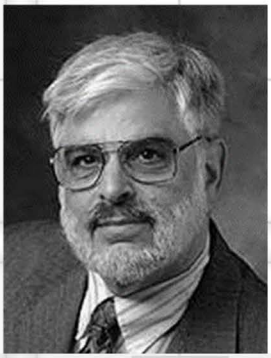
14 HOTSPOT

		9		6	4			
	5				8	2		
3		8	5		9		1	
					3			7
5	3						2	9
9			4					
	6		2		5	9		1
		5	9				7	
			1	4		6		



Alan Turing (1912-1954): British mathematician, computer scientist, and logician. Known as the father of modern computer science and artificial intelligence. Turing played a pivotal role in breaking the Enigma code during World War II.

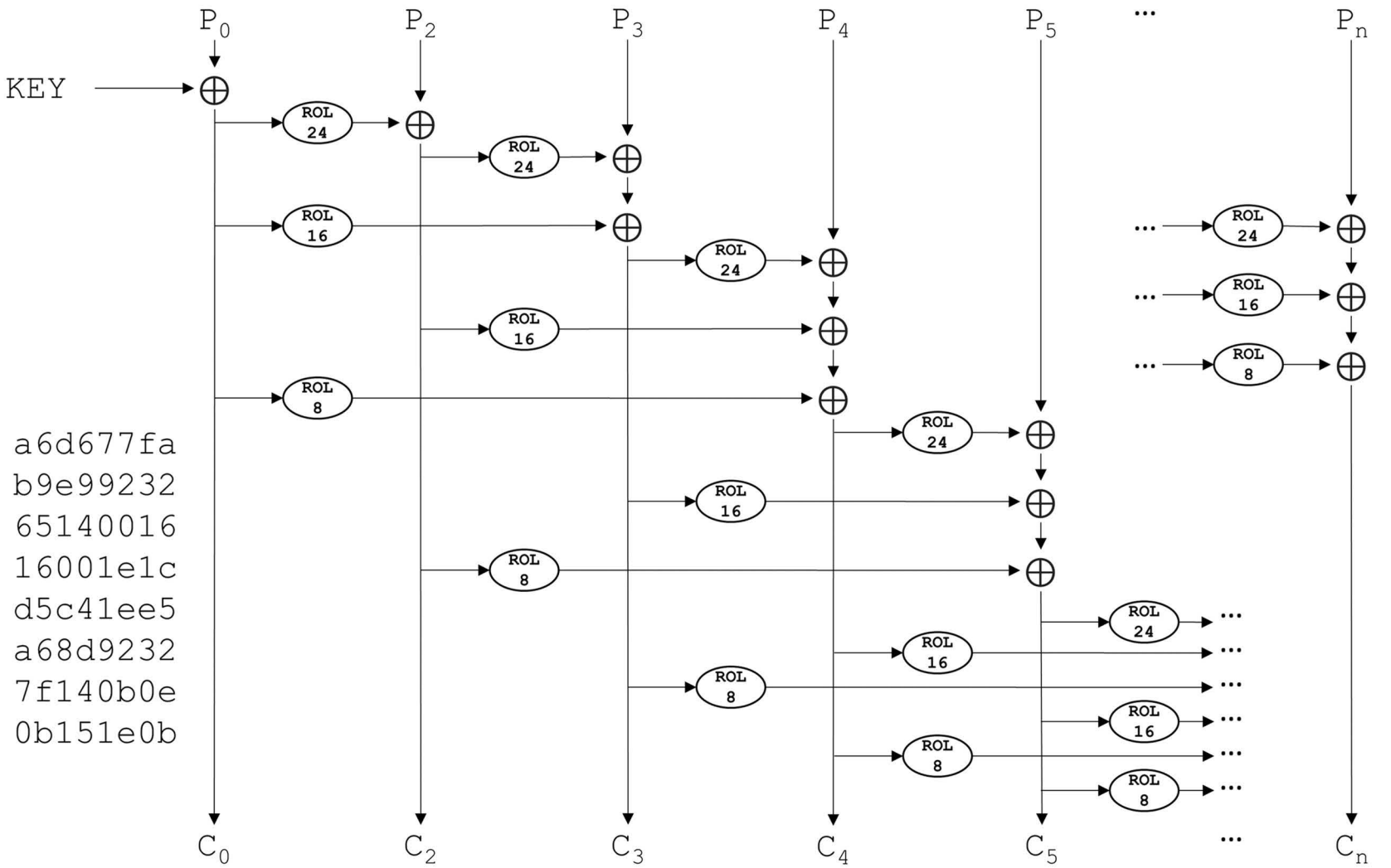
15 CONTROLLER



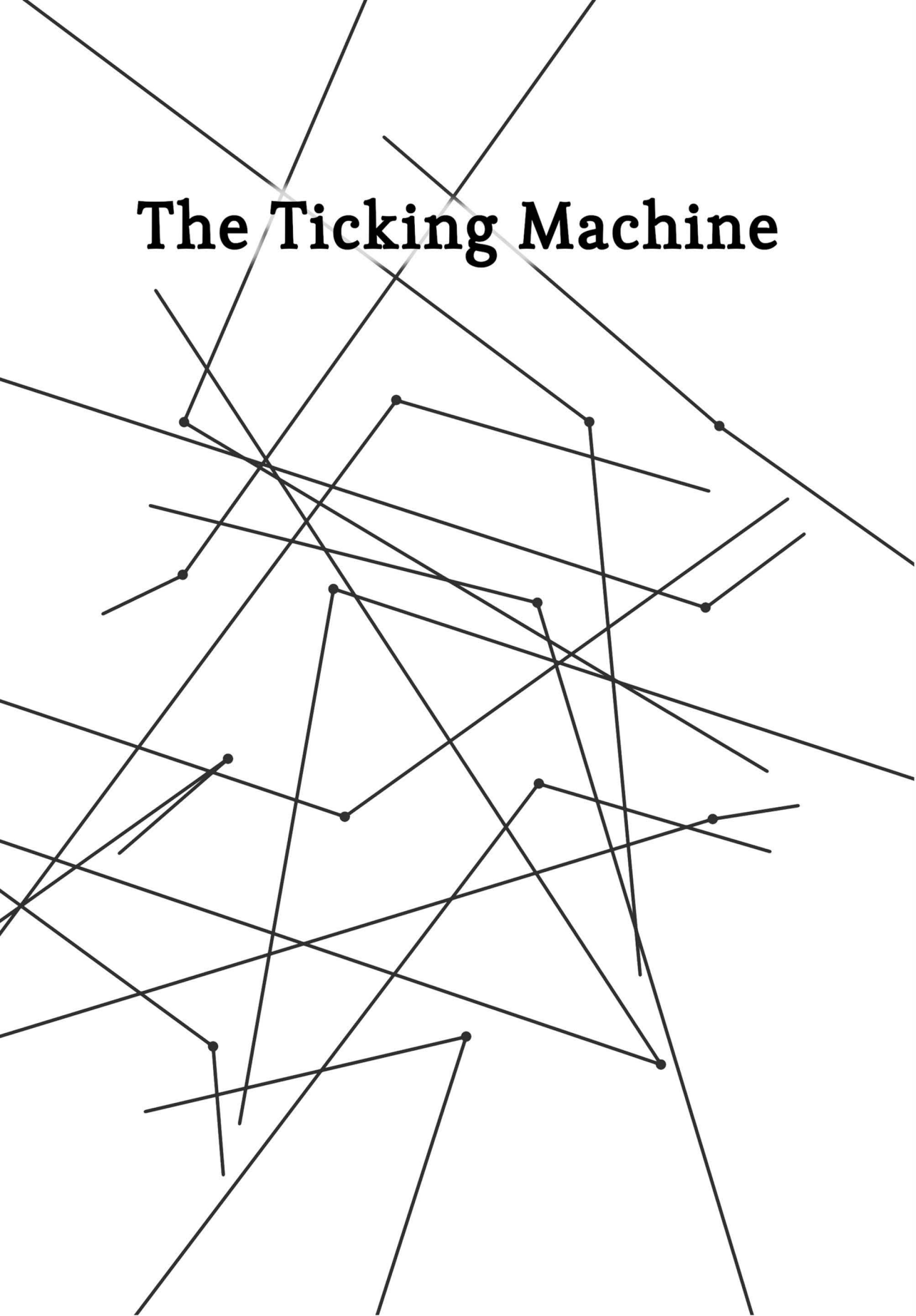
Jeffrey Ullman (1942-present): American computer scientist and professor. Renowned for his contributions in database theory, data mining, and algorithms. Ullman has authored influential textbooks and played a significant role in advancing the theoretical foundations of computing.

		3			9	1		2
				5			3	
9			3		6		8	
	1				4	5	7	
		4				3		
	7	9	6				2	
	3		2		7			5
	4			8				
7		8	5			2		

The 32-bit MORXOR Encryption System



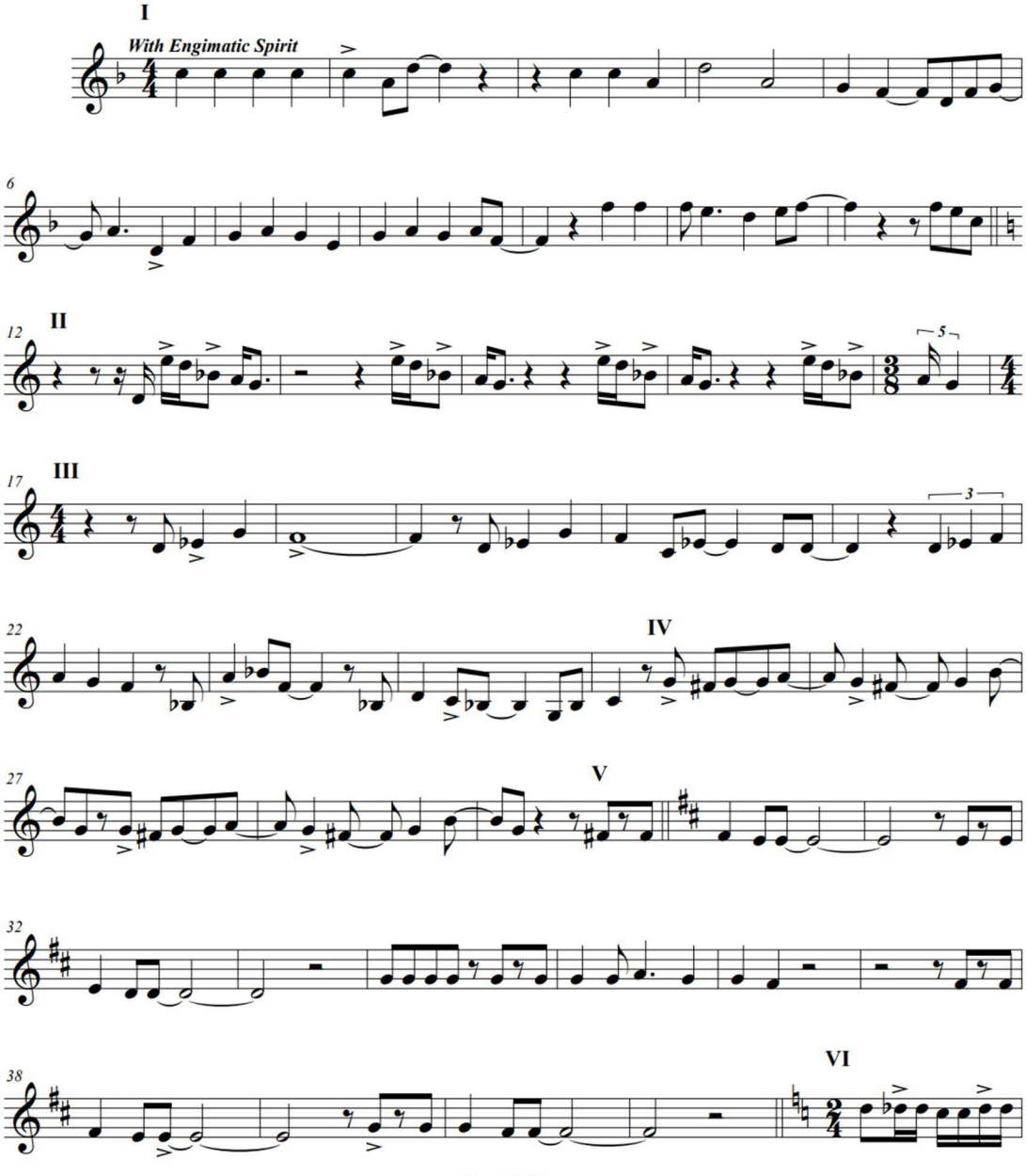
The Ticking Machine



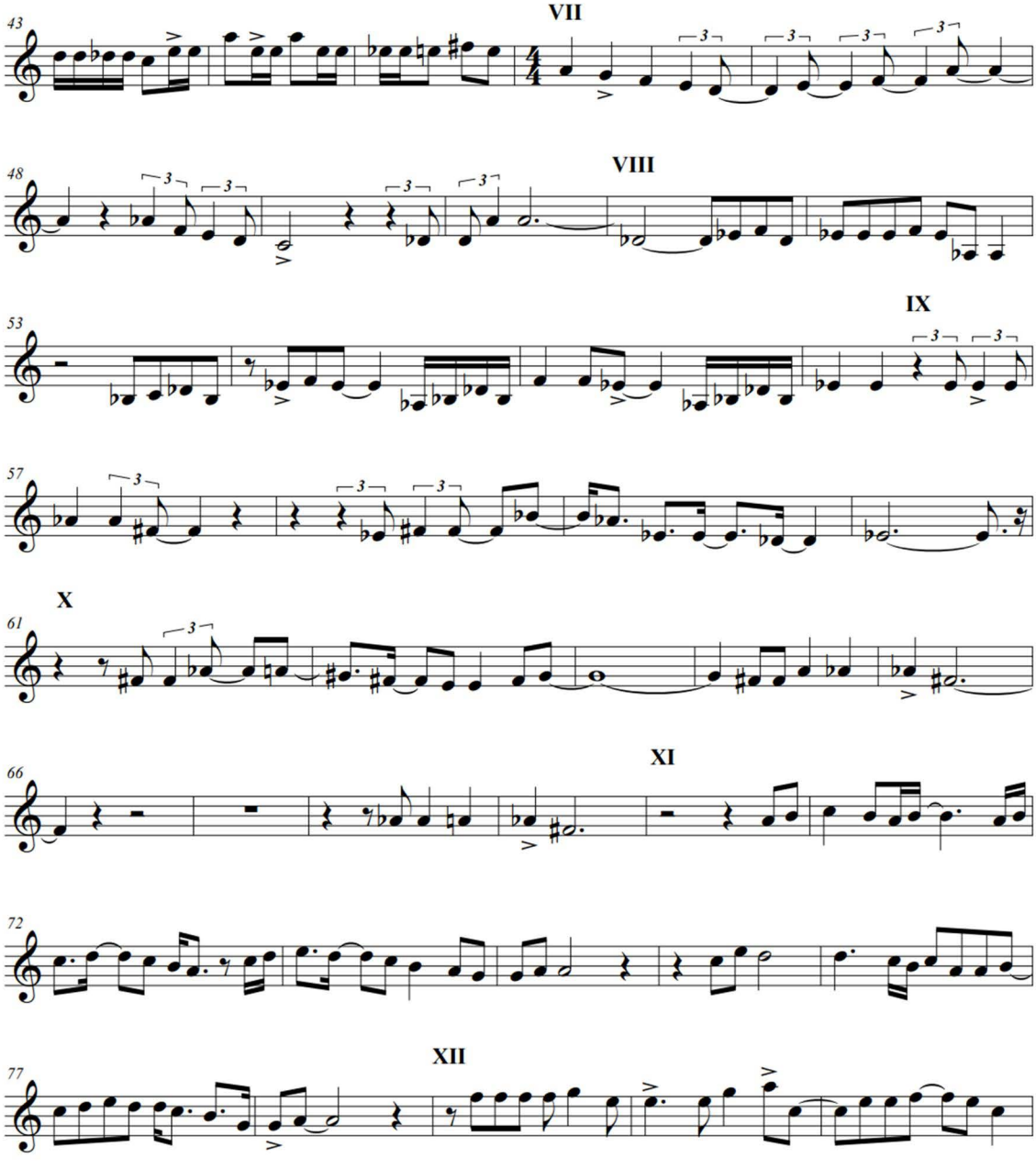
Mind your accents

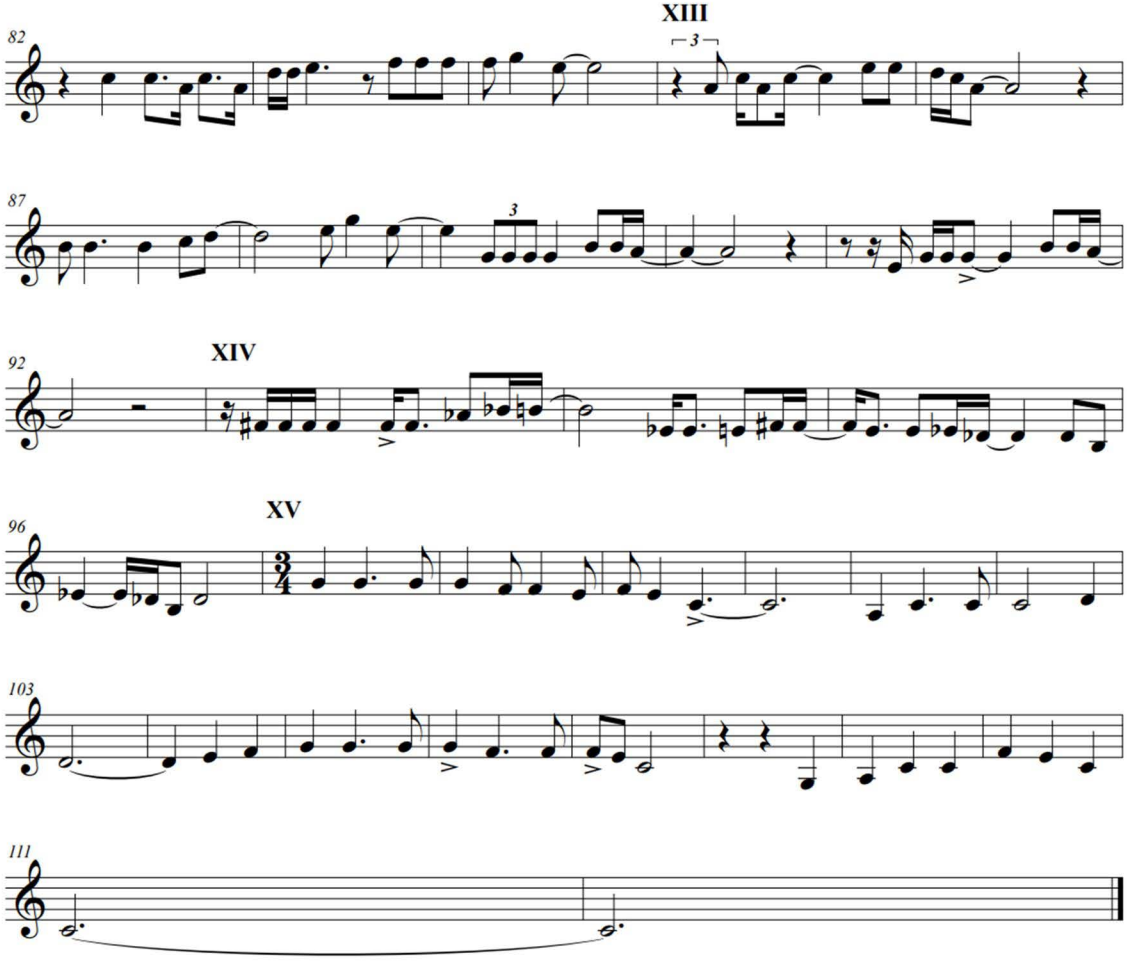
Name That Tune

Various Artists



The Gold Bug

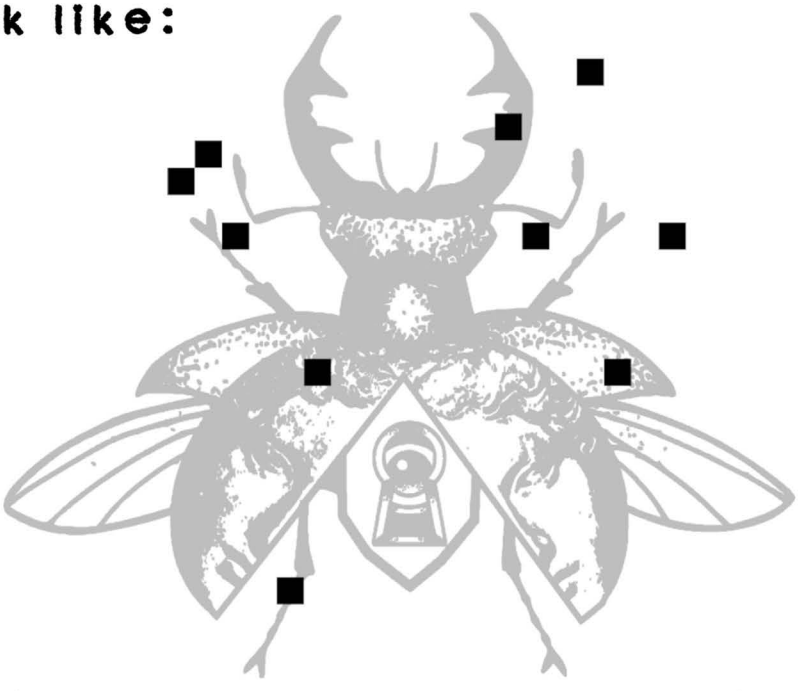

VII
VIII
IX
X
XI
XII


XIII
XIV
XV

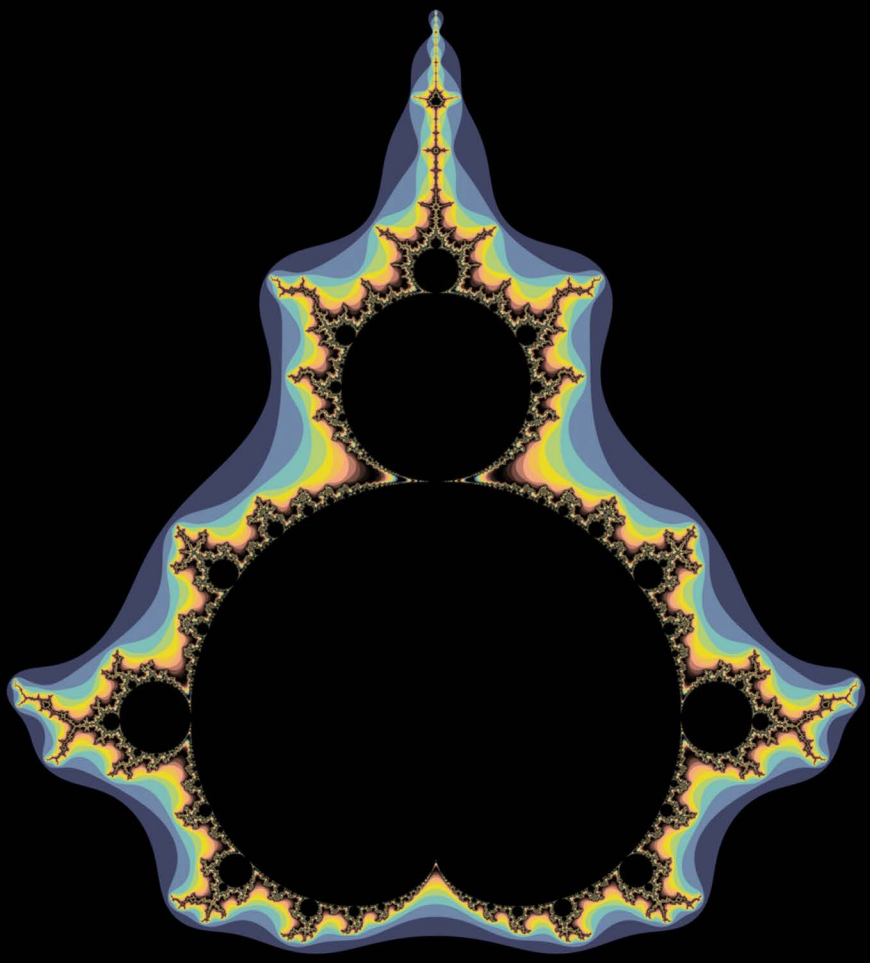
Lost Bugs

I came to DEF CON with my jar of bugs to show all my new friends. I walked around all over the conference before I noticed the lid was loose, so now they could be anywhere.

Here is a picture of what they look like:



Find as many as you can and take note of their unique markings. You can hold one or two for a while, but make sure to release it when you are done so all can enjoy. Be sure to leave them in plain sight!



Crypto
means
Cryptography