

Cryptography and murder – The Zodiac killer

Håvard Raddum
Selmersenteret
University of Bergen

Beginning of the story

- Tor got an email
- Someone wanted help with a cipher
- Could the plaintext be in Norwegian?
- Decided to have a look at it

The Zodiac killer case

- ❑ Serial killer active in the San Francisco area in the years 1967 – 1974 (at least)
- ❑ Linked to 7 murders, but claimed many more
- ❑ Never caught
- ❑ Police investigation closed in 2004
- ❑ Lots of theories and speculations around the case

This is the Zodiac speaking...

- ❑ Wrote many letters (at least 18) to the police and to newspapers in the SF area

This is the Zodiac speaking
Like I have always said
I am crack proof. If the
Blue Meannies are eveve
going to catch me, they had
best get off their fat asses
& do something. Because the

Ciphers

- ❑ Four letters contained ciphers
- ❑ Appear to be substitution ciphers, but with more ciphertext symbols than ordinary letters
- ❑ Two of them contain too little ciphertext to be solved

www.zodiackiller.com

*This is the Zodiac speaking
By the way have you cracked
the last cipher I sent you?
My name is —*

A E N ⊕ ⊗ K ⊗ M ⊗ J N A M

A I M o e F e n e r m a n ?



408 cipher

- ❑ First cipher the Zodiac sent
- ❑ Was divided in three parts and sent to three different newspapers
- ❑ All three parts published on the front pages
- ❑ Solved in a week by a high school teacher and his wife

How did they do it?

- ❑ Knew the killer had a big ego, assumed he would start with 'I'
- ❑ Assumed the word 'kill' would appear several times
- ❑ This was 1969 – only pencil and paper!

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

Observations

- ❑ One symbol = one letter
- ❑ More symbols than letters => one letter may be represented by several symbols
- ❑ Simple frequency analysis will not work
- ❑ 53 symbols used, each one appearing $408/53 = 7.7$ times on the average

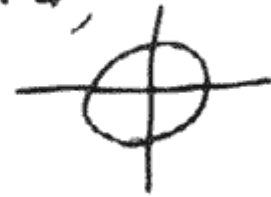
Cycle structure

- ❑ Symbols representing the same letter used in order
- ❑ Makes sure symbols are used equally often
- ❑ However, system messed up a bit

340 cipher

- Sent to the San Francisco Chronicle in Nov. 1969

PS could you print
this new cipher-
in your front page?
I get awfully lonely
when I am ignored,
so lonely I could
do my Thing!!!!
Dec



H E R > 9 J A V P X I O L T G O O
N 9 + B φ ■ O ■ D W Y · < ▣ K F φ
B X ± E ∩ M + u z G W φ φ L ■ φ H J
S 9 9 Δ Λ J ▲ ▣ V O 9 O + + R K O
□ Δ M + φ J τ O I ● F P + P ● X /
9 ▲ R Λ F J O - ■ O C ■ φ > ● D φ
■ ● + K φ φ τ ■ O + u ∩ X G V · φ L I
φ G ● J F B + Z R ● + □ N Y φ + □ L Δ
O < M + B + N R ● F B ∩ X < A O ● K
- φ J u v + Λ J + O 9 Δ < F B X I
u + R / ● L E I D Y B 9 B · T M K O
● < ∩ J R J I ■ ● T ● M · + P B F
φ ● O Δ S Y ■ + N I ● F B ∩ v φ ● L ▲ R
J G F N Λ F ● ● ● B · ∩ v u z ● + +
Y B X ● ■ E ● Δ C E > v u z ● + +
I ∩ · ● φ B K φ O 9 Λ · F J W B I φ ● L
R ∩ T + L ● ● C < + F J W B I φ ● L
+ + φ W C φ W ∩ P O S H T / φ φ 9
I F K Q W < Δ J B □ Y O B - C ∩
> M D H N 9 K S ◆ Z O ▲ A I K E +

UNSOLVED

Initial observations

- ❑ Appears to be same kind of cipher as the 408
- ❑ Each line contains 17 symbols, as in the 408
- ❑ Contains 63 symbols, each appearing
 $340/63 = 5.4$ times each on the average

Frequency analysis

1: **** - 4
2: *** - 3
3: **** - 8
4: **** - 4
5: **** - 11
6: **** - 7
7: **** - 6
8: **** - 6
9: *** - 3
10: **** - 5
11: **** - 10
12: ** - 2
13: **** - 6
14: **** - 5 7.7% - T,A,O,I,N,S?
15: **** - 6
16: **** - 10
17: **** - 5
18: **** - 5
19: **** - 24
20: **** - 12
21: **** - 7

22: **** - 5
23: **** - 10
24: ** - 2
25: **** - 4
26: **** - 6
27: **** - 4
28: **** - 6
29: **** - 6
30: **** - 6
31: **** - 7
32: **** - 4
33: **** - 5
34: **** - 5
35: ** - 2
36: **** - 9
37: **** - 7
38: **** - 5
39: **** - 4
40: **** - 9
41: **** - 4
42: **** - 4

43: *** - 3
44: **** - 4
45: ** - 2
46: *** - 3
47: **** - 4
48: ** - 2
49: **** - 4
50: ** - 2
51: **** - 11
52: **** - 10
53: *** - 3
54: *** - 3
55: **** - 5
56: **** - 6
57: ** - 2
58: ** - 2
59: *** - 3
60: ** - 2
61: * - 1
62: *** - 3
63: ** - 2

Same method as the 408?

- Maybe symbols representing the same letter appear in cyclic order?
- Knowing which symbols represent the same letter makes cipher vulnerable to frequency analysis
- Assume cycle system used, identify different symbols representing the same letter

2-cycles

- ❑ Try all pairs of symbols and see which ones appear in alternating pattern (2-cycle)
- ❑ Number of 2-cycles in the 340 cipher is 90
- ❑ Most of them consist of symbols only appearing a few times
- ❑ Exceptions:
 - (\wedge , \blacksquare) – 6 times each
 - (\lrcorner , \mathfrak{M}) – 7 times each

^ and ▣ same letter?

□ 9 symbols appear 6 times each, what is the probability that two of them form a 2-cycle?

□ Given two of the symbols, probability they appear in alternating pattern:

$$\frac{\# \text{ of alt. patterns}}{\# \text{ of pos. patterns}} = \frac{2}{\frac{12!}{(6!)(6!)}} = \frac{1}{66}$$

□ $\Pr(\text{at least one 2-cycle}) = 1 - (65/66)^{\binom{9}{2}} \approx 0.423$

□ Can not conclude anything

┘ and **m** same letter?

- 4 symbols appear 7 times each
- Given two of the symbols, probability they appear in alternating pattern:

$$\frac{2}{\frac{14!}{(7!)(7!)}} = \frac{1}{1716}$$

- $\Pr(\text{at least one 2-cycle}) = 1 - (1715/1716)^{\binom{4}{2}} \approx 0.0035$

- Good basis for guessing $\text{┘} = \mathbf{m}$ in the 340 cipher

n-cycles

□ May find all n-cycles ($n > 2$) by trying all $\binom{63}{n}$ possibilities

□ Better way, use following result :

(s_2, s_3, \dots, s_n)	all form (n-1)-cycles	\Leftrightarrow	(s_1, s_2, \dots, s_n)
(s_1, s_3, \dots, s_n)			forms an n-cycle
:			
$(s_1, s_2, \dots, s_{n-1})$			

□ Example: $(1,5)$, $(1,13)$ and $(5,13)$ are 2-cycles

\Updownarrow

$(1,5,13)$ is a 3-cycle

Overview of n-cycles

- Knowing all 2-cycles, may use result to recursively produce all n-cycles, $n > 2$

- | n | # of n-cycles |
|---|---------------|
| 2 | 90 |
| 3 | 62 |
| 4 | 14 |
| 5 | 2 |

- Using this to identify symbols representing same letter => too many letters (45)

Are we on the right track?

- ❑ Questions: {
 - Maybe cipher should be read columnwise?
 - Has the cycle system been used at all?
- ❑ If cycle system used, we should see more cycles than what to expect in a random symbol sequence
- ❑ Generated 10.000 random sequences from the set of symbols found in 340 cipher, counted the number of n -cycles in them

Result

Actual 340 cipher

n	# of n-cycles
2	90
3	62
4	14
5	2

10.000 random seq.

n	min	avg	max	# of times above actual 340
2	8	34.9	79	0
3	0	16.0	102	46
4	0	4.2	113	713
5	0	0.6	79	626

Transposed cipher:
(reading columnwise)

n	# of n-cycles
2	35
3	10
4	1
5	0

Findings (?)

- ❑ Strong bias in number of n -cycles, $n = 2,3$

Evidence that cycle system has been used

- ❑ No bias when reading columnwise

Cipher to be read linewise

- ❑ Analysis that allows for small deviations in cycle system needed