

# Cracking the Copiale Cipher

Simon MacDonald

February 6, 2012

# What Is the Copiale Cipher?

- 105-page enciphered book dated 1866
- found in the East Berlin Academy
- mix of Roman letters, abstract symbols, and punctuation

= m z f z l i n z q c z r i e n e c p f f i z v r b g j m k e i d g j n l v b r n v t a s  
 h i c i x i g n u + r l n r i g a p o r z e d o y a g a r f + i m z z c u i r i r i r i d e y a  
 e . k z a n u i r d e z y a g o i n o h i + b z i b s e r r m z r d m z p f l i n u d : r p i o  
 c e p f m h e d g x p u e l r a k e a s e l m u o d z l v k s d n t e z f i d l s f h i e l g r i  
 m p o r d o b h n : s e r r u i + u i j d n h e i u g r z g m a s u i a y o r i n t g z  
 j l m e m a x c i t e i r i x i i z o z e p f l i n h i + v z y l e b o n r m z i j g z a h a l  
 k = i w z e l m . x b c h n y d o f h i e n p b i h z v i + r m e r i + h i r u e i l a z i n f i j j  
 g n + u y z h e i z m v r i e r a i e c r i c i u r i n q s i m p a o l p u + v z o i v j e  
 m e . l h i z l f o i r a i u r e m u b i h i u r c e i r a l e z i n : f i c y e p l m w  
 z i j e . l b z y a i u m h i j r a i a s o z z g i h z u x i i n l i r i b o n i j a o x o n : p s  
 a + t g r i n o r f i z m p h e f i n v a l i b c i n u n a l i q u o p i h u i n d e y i u  
 d e s o f f . l a z i u i n p o d e a h z u m v i x i a f l e . l y h g r z i b a r i n e s t a z  
 m o r u o f o r i a m z n a h l d u i m u r i n . l d a t l f z h c u p i t g z n e  
 h f i r h i a b d o r i : m o s u i n e e d o d a i i n h e z o z i r : l t o f g g r z m w  
 r i z a i a y a : g p n i z e r r h i c : u i r h p m d i u z u w p z p u i r i z o z  
 g p o j m n u p i n z y i h m z o u n r r + i m l o d + i m e c t i n g i d u  
 d i u m : e l o s = l i j y r i u e i n e r r : d h i a z o g r i m i c : f i j u s a l o a c : e n  
 z d a l

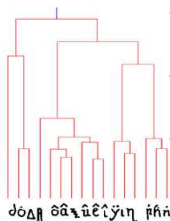
d a l o m i r i m f a i t e r r a e z r z d o c : i x m z r o n . l d o d e f c a : u d  
 d y e c : a i r m l e z r o d y m p l o p h e c a r n a z i h i e i u b .  
 Η ρ α ο o d x i i c : u b .  
 Α η ν i x p a c a n n o m π γ e r o d e n p u h e i n r i y r m z m o b z e d e  
 u p a t : i z x z i h f b d e y i r e g a t h i c i u x d i z o z x i p o u e l i u p a z m m p g p  
 i n t e d i u c p h e m e i d : r r e p r a f i z g z p i r l i n h i y z s n i p u d o a u r e  
 r n y y g d i n p a d a x p o c i a p r o d m d e r y z : n x u m p u r i = z a s b k r  
 r n y e b i n o i : u o h m z z f a h i m h e d j r e p z z a z o p m + i k a s : i r u l r i  
 x i e u i n z e i h i t a l o t e r b z v n p u l i d e z j r m s i m p r o + h i h e g n y  
 z v i b z e i u d o l a s i m t h e x a e z y i l k e i n h e d i s f i h i e i a c i  
 f l o b m u o r e o a d c i h z e y r i c a g z w z i n f l i u a z h i d i o n i a n  
 t e s x d e i r m b o n m g n y q n a s h e c e l u o m z i u p p a x i c o d a f z e  
 c a r d o i u m . l t r i l m n y a b d a z i t m o v i n i d o l m i n r o z  
 e l o c r a i m i c : + h i c e y r x u i n i n d o s a n i a o m d o g i u z e +  
 u i r z i + g n e : a c y r u d a h z o r i o r y m m .  
 Η ρ e o o b d n .  
 C a p u d e i r n o r a r . l d a n a y i u e n i p o y z g h a t r

# Preliminary Steps

## 1 machine-readable transcription

πδipηΔpεζcâ=γλûb◊u r⊕z

pi oh j v hd tri arr eh three c. ah  
ni arr lam uh b lip uu r o.. zs



ο η	99
ε :	66
η λ	49
: ε	48
z η	44

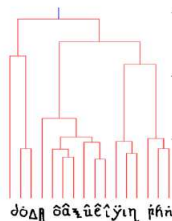
ο η λ	47
ε : ε	23
η ο η	22
γ ο η	18
η ε	17

# Preliminary Steps

- 1 machine-readable transcription
- 2 digraph and trigraph frequencies

πδipηΔpεζcâ-zλûb ◊ u r ⊕ z

pi oh j v hd tri arr eh three c. ah  
ni arr lam uh b lip uu r o.. zs

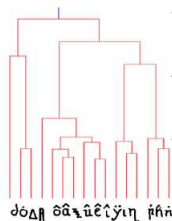


# Preliminary Steps

- 1 machine-readable transcription
- 2 digraph and trigraph frequencies
- 3 behavioral similarity

πδipηΔrεζcâ=γλûb ◊ ыр⊕z

pi oh j v hd tri arr eh three c. ah  
ni arr lam uh b lip uu r o.. zs



ρ η	99
ε :	66
η λ	49
: ε	48
z η	44

ρ η λ	47
ε : ε	23
η ρ η	22
ζ ρ η	18
η ε	17

# Path to Decipherment

## 1 NULLs

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution



# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression
- 6 unaccented Roman letters for spaces

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression
- 6 unaccented Roman letters for spaces
- 7 punctuation shortcuts

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression
- 6 unaccented Roman letters for spaces
- 7 punctuation shortcuts
- 8 cipher letters for trigraphs

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression
- 6 unaccented Roman letters for spaces
- 7 punctuation shortcuts
- 8 cipher letters for trigraphs
- 9 German native guidance

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression
- 6 unaccented Roman letters for spaces
- 7 punctuation shortcuts
- 8 cipher letters for trigraphs
- 9 German native guidance
- 10 ambiguous symbols

# Path to Decipherment

- 1 NULLs
- 2 monoalphabetic substitution
- 3 homophonic substitution
- 4 German digraph frequency table
- 5 avalanching substitution progression
- 6 unaccented Roman letters for spaces
- 7 punctuation shortcuts
- 8 cipher letters for trigraphs
- 9 German native guidance
- 10 ambiguous symbols
- 11 indication of logograms



# Worth It?

- valuable resource to historians
- political commentary about the natural rights of man
- modern challenges persist (e.g., Zodiac cipher)
- potential hoaxes (e.g., Voynich manuscript)

# Sources

<http://www.nytimes.com/2011/10/25/science/25code.html>

<http://www.isi.edu/natural-language/people/copiale-11.pdf>