

# K4 Class Grid (0-96)

<b>Class 0</b>	0 <b>O</b>	6 <b>X</b>	12 <b>B</b>	18 <b>B</b>	24 <b>V</b>	30 <b>G</b>	36 <b>W</b>	42 <b>S</b>	48 <b>W</b>	54 <b>U</b>	60 <b>N</b>	66 <b>V</b>	72 <b>P</b>	78 <b>Z</b>	84 <b>I</b>	90 <b>A</b>	96 <b>R</b>
<b>Class 1</b>	4 <b>U</b>	10 <b>U</b>	16 <b>I</b>	22 <b>L</b>	28 <b>R</b>	34 <b>O</b>	40 <b>J</b>	46 <b>Z</b>	52 <b>K</b>	58 <b>W</b>	64 <b>Y</b>	70 <b>Z</b>	76 <b>D</b>	82 <b>C</b>	88 <b>H</b>	94 <b>C</b>	
<b>Class 2</b>	2 <b>K</b>	8 <b>G</b>	14 <b>O</b>	20 <b>W</b>	26 <b>Q</b>	32 <b>S</b>	38 <b>Q</b>	44 <b>E</b>	50 <b>T</b>	56 <b>I</b>	62 <b>B</b>	68 <b>T</b>	74 <b>W</b>	80 <b>T</b>	86 <b>K</b>	92 <b>E</b>	
<b>Class 3</b>	3 <b>R</b>	9 <b>H</b>	15 <b>L</b>	21 <b>F</b>	27 <b>P</b>	33 <b>S</b>	39 <b>S</b>	45 <b>K</b>	51 <b>J</b>	57 <b>A</b>	63 <b>N</b>	69 <b>M</b>	75 <b>G</b>	81 <b>J</b>	87 <b>U</b>	93 <b>K</b>	
<b>Class 4</b>	1 <b>B</b>	7 <b>O</b>	13 <b>S</b>	19 <b>B</b>	25 <b>Q</b>	31 <b>K</b>	37 <b>T</b>	43 <b>S</b>	49 <b>A</b>	55 <b>D</b>	61 <b>F</b>	67 <b>T</b>	73 <b>K</b>	79 <b>X</b>	85 <b>G</b>	91 <b>U</b>	
<b>Class 5</b>	5 <b>O</b>	11 <b>L</b>	17 <b>F</b>	23 <b>R</b>	29 <b>N</b>	35 <b>T</b>	41 <b>Q</b>	47 <b>Z</b>	53 <b>L</b>	59 <b>I</b>	65 <b>P</b>	71 <b>F</b>	77 <b>K</b>	83 <b>D</b>	89 <b>U</b>	95 <b>A</b>	

## Cribs:

 EAST (21-24)	 NORTHEAST (25-33)	 BERLIN (63-68)	 CLOCK (69-73)	 Tail (75-96)
--	---	--	---	--

## Decrypt Formulas:

- Vigenère:  $P = C - K \pmod{26}$
- Beaufort:  $P = K - C \pmod{26}$
- Variant-Beaufort:  $P = C + K \pmod{26}$

Letter-Number: A=0, B=1, ..., Z=25

**Class Function:  $\text{class}(i) = ((i \bmod 2) \times 3) + (i \bmod 3)$**

# Forcing K at Anchor Positions

## Crib: EAST

Index: 22

Ciphertext: L = 11

Plaintext: A = 0

Class: 1

Family: vigenere

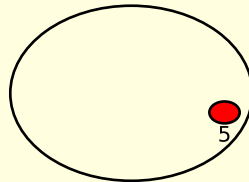
Period L: 17, Phase: 0

Slot: 5

$$K = C - P = 11 - 0 = 11$$

**K = 11 (L)**

✓  $K \neq 0$  (Option-A satisfied)



Class 1 Wheel

## Crib: NORTHEAST

Index: 27

Ciphertext: P = 15

Plaintext: R = 17

Class: 3

Family: vigenere

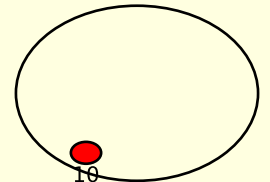
Period L: 17, Phase: 0

Slot: 10

$$K = C - P = 15 - 17 = 24$$

**K = 24 (Y)**

✓  $K \neq 0$  (Option-A satisfied)



Class 3 Wheel

## Crib: BERLIN

Index: 65

Ciphertext: P = 15

Plaintext: R = 17

Class: 5

Family: vigenere

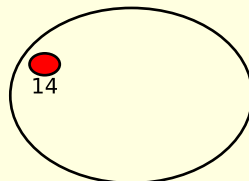
Period L: 17, Phase: 0

Slot: 14

$$K = C - P = 15 - 17 = 24$$

**K = 24 (Y)**

✓  $K \neq 0$  (Option-A satisfied)



Class 5 Wheel

## Crib: CLOCK

Index: 71

Ciphertext: F = 5

Plaintext: O = 14

Class: 5

Family: vigenere

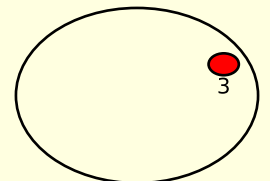
Period L: 17, Phase: 0

Slot: 3

$$K = C - P = 5 - 14 = 17$$

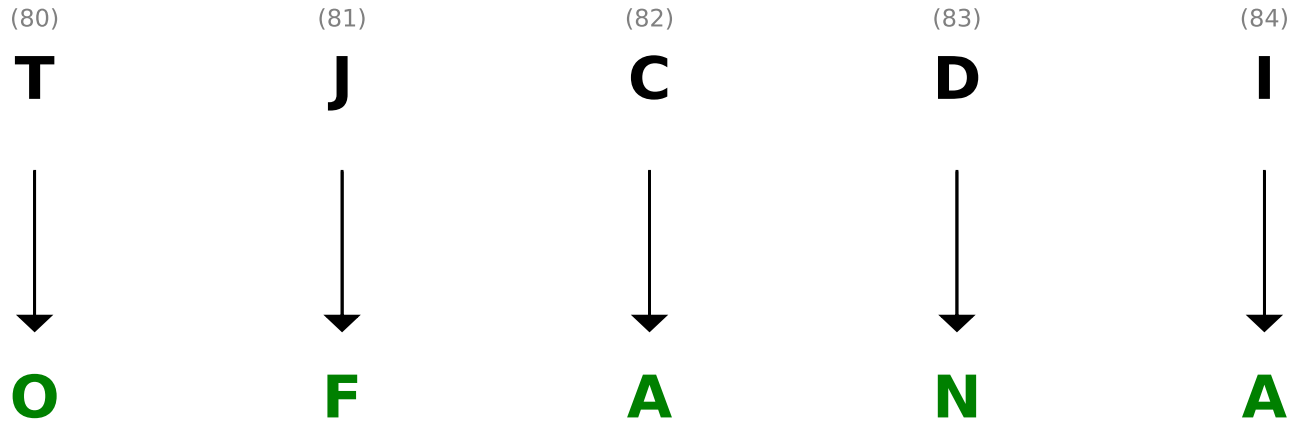
**K = 17 (R)**

✓  $K \neq 0$  (Option-A satisfied)



Class 5 Wheel

# Tail Propagation: Indices 80-84



*"...JOY OF AN ANGLE..."*

Index	CT	Class	Family	Slot	K	Formula	PT
80	T	2	beau	12	7(H)	$P = K - C = 7 - 19 = 14$	O(14)
81	J	3	vige	13	4(E)	$P = C - K = 9 - 4 = 5$	F(5)
82	C	1	vige	14	2(C)	$P = C - K = 2 - 2 = 0$	A(0)
83	D	5	vige	15	16(Q)	$P = C - K = 3 - 16 = 13$	N(13)
84	I	0	vige	16	8(I)	$P = C - K = 8 - 8 = 0$	A(0)

# Verification: Round-trip & Drop-crib

## Round-trip Verification

Example: Re-encrypting position 22 (EAST anchor)

Index 22:  $P=A \rightarrow C = P + K = 0 + 11 = 11 \rightarrow C=L$  ✓ (matches)

Example: Re-encrypting position 80 (tail)

Index 80:  $P=O \rightarrow C = K - P = 7 - 14 = -7 \equiv 19 \rightarrow C=T$  ✓ (matches)

Example: Re-encrypting position 40 (non-anchor)

Index 40:  $P=S \rightarrow C = P + K = 18 + 2 = 20 \rightarrow C=U$  ✓ (matches)

## Drop-crib Illustration

With BERLIN crib:

<b>Y</b>	<b>P</b>	<b>V</b>	<b>T</b>	<b>T</b>	<b>M</b>
↓	↓	↓	↓	↓	↓
<b>B</b>	<b>E</b>	<b>R</b>	<b>L</b>	<b>I</b>	<b>N</b>

Without BERLIN crib:

<b>Y</b>	<b>P</b>	<b>V</b>	<b>T</b>	<b>T</b>	<b>M</b>
↓	↓	↓	↓	↓	↓
<b>?</b>	<b>?</b>	<b>?</b>	<b>?</b>	<b>?</b>	<b>?</b>

*Note: Removing a crib does not reconstruct it.  
Those positions remain undetermined.*