

# Three Encodings

- CBWRP TWIFE IGQBR TQEJN TWZCC JEHVG KFLDY XUGFN JLHRK GMENP NVZMC  
TVVPX YGHWN URGSM LRTVY GXQNP PJTOI YUFDX GZBNM CBXRG VYMJL EAFJM  
UHTHU UCXFI ZDVPH TVROR PGBIQ JRTTY EZKCG TLEAF UMVHH FYFPZ BRGJV  
GGHAA EFKBN RVVZC HHXUG IQRAS BUVJX OIFQW YHVGK KTGHF AVVYG CHYEE  
CMXLX RTVBG XWVFX LRXLN NCQIA IFGTF DBGRU RPTII EUFLP EFHVV TTKCB  
PVGCH THUUC XLLNT VQIAI TQRJD YFRVK CGBRT VYCLH VYFSW SHMAI KFTPS  
EMFDV HHFWI CARXU KJGHT RNFDG GTFYG HSTLX
- LOFNT BRTCI ECPIE EUSNH ESERH DTNIO PEEDL SDEHL WPUIT DOAEH NOYVL  
FREIB YSHRT RAERU NTRAN EGHUT EODWO TDNLS OEANL XIEEE NVFAE MIOLO  
WEDER NNWHR NNEEN BIETE DSOCE ADHEY RISEH FNWEA ITUAI EANH N TYTMW  
DTIPN HNREI DRMSD GANEW ABODT IIIDT CCSES HEATS LLSRB EASEE TAEAG  
ALNNF NNNNS CEOIT AEHSH FLGII CCTIA BAEIN VDOSO FLENS EESOT MIIEN  
COYOA AVUYL TBDBT SCDSI YGOAD CCAED TRRSO OPIEO TDNOT YSTLN OEGIT  
RAFOY RETSV TNIAN BOPHH MGSTA TAWHU JEHUE
- QAYYW ECQGY ITQAB PGEIT RJIMY CEGGY RCJMM YCQGX VEOEM JSIRP BPQYY  
IASIR MYRPY YQQAY GYITQ AJPQA MYYVE OABIT QJIHJ ISHYI QOGEB RYIRQ  
JYIRY LSEGG XNMYE QAQEF BITVE OQAYC JMMBR JMOV B RQAVA BCAYE OBGXC  
JSGRA EUYEC CJHHJ REQYR OBRYN XOBRY KEOOY ITYMQ MEBIO QAYCY IQYMJ  
PQAYA EGGVE XVEOR JQQYR NXQAY JCCEO BJIEG OQEQS YJMCJ GJOOE GKJMC  
YGEBI SMIVA BCAA OY MUYRE OEQEO QYPSG RBUBR YMEIR FYKQQ AYPGJ VJPQM  
EPPBC HJUBI TRJVI JIYVE GGEIR SKQAY JQAYM

# Rearrangement

- Encoding (b):

50: E	46: E
33: N	34: T
31: T	29: A
27: AI	28: O
25: O	27: I
24: S	26: N
20: D	24: S
18: H	22: R
17: R	20: H
14: L	15: L
12: C	14: D
9: BY	11: C
8: FUW	10: U
7: G	9: M
6: P	8: F
5: MV	7: PGW
1: JX	6: BY
	4: V
	2: K
	1: JX

- Thus, a rearrangement cipher.

# Rearrangement

- LOFNT BRTCI ECPIE EUSNH ESERH DTNIO PEEDL SDEHL WPUIT DOAEH NOYVL  
 FREIB YSHRT RAERU NTRAN EGHUT EODWO TDNLS OEANL XIEEE NVFAE MIOLO  
 WEDER NNWHR NNEEN BIETE DSOCE ADHEY RISEH FNWEA ITUAI EANHN TYTMW  
 DTIPN HNREI DRMSD GANEW ABODT IIIDT CCSES HEATS LLSRB EASEE TAEAG  
 ALNNF NNNNS CEOIT AEHSH FLGII CCTIA BAEIN VDOSO FLENS EESOT MIIEN  
 COYOA AVUYL TBDBT SCDSI YGOAD CCAED TRRSO OPIEO TDNOT YSTLN OEGIT  
 RAFOY RETSV TNIAN BOPHH MGSTA TAWHU JEHUE

LOFNTBRTCI ECPIEEUSNHESERHDTNIOPEEDLSDEHLWPUITDOAEHNOYVLFREIBYSHRTRAERUNTR  
 ANEGHUTEODWOTDNLSOEANLXIEEENVFAEMIOLOWEDERNNNWHRNNEENBIETEDSOCEADHEYRISEHF  
 NWEAITUAIEANHNTYTMWDTIPNHNREIDRMSDGANEWABODTIIIDTCCSESHEATSLLSRBEASEETAEA  
 GALNNFNNNNSCEOITAEHSHFLGII CCTIABAEINVDOSOFLENSEESOTMIIENCOYOA AVUYLTBDBTSC  
 DSIYGOADCCAEDTRRSO OPIEOTDNOTYSTLNOEGITRAFOYRETSVTNIANBOPHHMGSTATAWHUJEHUE

L	O	F	N	T	B	R	T	C	I	E	C	P	I	E	..
A	N	E	G	H	U	T	E	O	D	W	O	T	D	N	..
N	W	E	A	I	T	U	A	I	E	A	N	H	N	T	..
G	A	L	N	N	F	N	N	N	S	C	E	O	I	..	
D	S	I	Y	G	O	A	D	C	C	A	E	D	T	R	..

LANGD	ONWAS	FEELI	NGANY	THING	BUTFO	RTUNA	TEAND	COINC	IDENC	EWASA	CONCE	..
-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	----

- Langdon was feeling anything but fortunate, and coincidence was a concept he did not entirely trust. As someone who had spent his life exploring the hidden interconnectivity of disparate emblems and ideologies, Langdon viewed the world as a web of profoundly intertwined histories and events. The connections may be invisible, he often preached to his symbology classes at Harvard, but they are always there, buried just beneath the surface.

# Monoalphabetic Substitution

- Encoding (c):

45: Y	46: E
33: Q	34: T
32: E	29: A
26: J	28: O
25: I	27: I
23: R	26: N
22: A	24: S
21: G	22: R
20: M	20: H
19: BO	15: L
16: C	14: D
11: PV	11: C
9: S	10: U
7: T	9: M
6: X	8: F
5: H	7: PGW
4: KU	6: BY
3: N	4: V
2: F	2: K
1: LW	1: JX

- Thus, a monoalphabetic cipher. (Y=E? Q=T?)

# Monoalphabetic Substitution

- QAYYW ECQGY ITQAB PGEIT RJIMY CEGGY RCJMM YCQGX VEOEM JSIRP BPQYY  
 IASIR MYRPY YQQAY GYITQ AJPQA MYYVE OABIT QJIHJ ISHYI QOGEB RYIRQ  
 JYIRY LSEGG XNMYE QAQEF BITVE OQAYC JMMBR JMOV B RQAVA BCAYE OBGXC  
 JSGRA EUYEC CJHHJ REQYR OBRYN XOBRY KEOOY ITYMQ MEBIO QAYCY IQYMJ  
 PQAYA EGGVE XVEOR JQQYR NXQAY JCCEO BJIEG OQEQS YJMCJ GJOOE GKJMC  
 YGEBI SMIVA BCAOY MUYRE OEQEO QYPSG RBUBR YMEIR FYKQQ AYPGJ VJPQM  
 EPPBC HJUBI TRJVI JIYVE GGEIR SKQAY JQAYM

- Replacing the four most common letters (YQEJ) with the four most common letters in English (ETAO) gives...

- T\_EE\_ A\_T\_E \_\_T\_\_ \_\_A\_\_ \_O\_\_E \_A\_\_E . . . \_\_T\_E OT\_E\_

- ...and then using A=H (because the frequent QAY = THE?) gives something ending with THEOTHE\_; using M=R to make that “the other” gives...

- THEE\_A\_T\_E\_\_TH\_\_A\_\_O\_RE\_A\_\_E\_\_ORRE\_T...O\_THREE...THEOTHER

- Then “\_ORRE\_T” = CORRECT, and etc., etc., until:
- The exact length, if Langdon recalled correctly, was around fifteen hundred feet, the length of three Washington Monuments laid end to end. Equally breathtaking was the corridor’s width, which easily could have accommodated side by side passenger trains. The center of the hallway was dotted by the occasional statue or colossal porcelain urn, which served as a tasteful divider and kept the flow of traffic moving down one wall and up the other.

- Plaintext:    ABCDEFGHIJKLMN**OP**QRSTUVWXYZ  
 Ciphertext:  ENCRYPTABDFGHIJKLMOQSUVWXYZ

# Polyalphabetic Substitution

- Encoding (a):

27: GV	46: E
25: T	34: T
24: F	29: A
23: H	28: O
21: R	27: I
17: C	26: N
16: I	24: S
15: X	22: R
14: UY	20: H
13: EL	15: L
12: BNP	14: D
11: J	11: C
10: AM	10: U
9: KQ	9: M
8: W	8: F
7: DZ	7: PGW
6: S	6: BY
3: O	4: V
	2: K
	1: JX

- Thus, a polyalphabetic cipher.

# Polyalphabetic Substitution

- CBWRP TWIFE IGQBR TQEJN TWZCC JEHVG KFLDY XUGFN JLHRK GMENP  
 NVZMC TVVPX YGHWN URGSM LRTVY GXQNP PJTOI YUFDX GZBNM CBXRG  
 VYMJL EAFJM UHTHU UCXFI ZDVPH TVROR PGBIQ JRTTY EZKCG TLEAF  
 UMVHH FYFPZ BRGJV GGHAA EFKBN RVVZC HHXUG IQRAS BUVJX OIFQW  
 YHVIG KTGHF AVVYG CHYEE CMXLX RTVBG XWVfV LRXLN NCQIA IFGTF  
 DBGRU RPTII EUFLP EFHVV TTKCB PVGCH THUUC XLLNT VQIAI TQRJD  
 YFRVK CGBRT VYCLH VYFSW SHMAI KFTPS EMFDV HHFWI CARXU KJGHT  
 RNFDG GTFYG HSTLX

- There are a few decoding techniques that work here, but to cut to the punchline:

- ENCRYPT = 4 13 2 17 24 25 19
- C B W R P T W I F E I G Q B R T Q E J N ...  
4 13 2 17 24 25 19 4 13 2 17 24 25 19 4 13 2 17 24 25 ...  
 Y O U A R E D E S C R I B I N G O N L Y ...

- “You are describing only a small portion of the Opus Dei population,” Aringarosa said. “There are many levels of involvement. Thousands of Opus Dei members are married, have families, and do God’s Work in their own communities. Others choose lives of asceticism within our cloistered residence halls. These choices are personal, but everyone in Opus Dei shares the goal of bettering the world by doing the Work of God. Surely this is an admirable quest.”

# Enciphering Texts

- **Week 1**: eht iquz is adery in eht ceerst abilmox ew  
deen ot aekm ceiops beefor addeenswy

the quiz is ready in the secret mailbox  
eht iquz is adery in eht ceerst abilmox

we need to make copies before Wednesday  
ew deen ot aekm ceiops beefor addeenswy

- Clearly a rearrangement cipher.
  - “The letters in each word are rearranged.”
  - (But: then why does the = eht both times? Why doesn't in change?)
- $E(\text{text}) =$  “Alphabetize the letters in each word.”

# Enciphering Texts

- **Week 2**: htq eiui zr saeyd ni hts eceerm tiablxo ew  
ende ot amek ocipse ebofer ewndseady

t	h	e		q	u	i	z		i	s		r	e	a	d	y		i	n		t	h	e		s	e	c	r	e	t		m	a	i	l	b	x	o
h	t	q		e	i	u	i		z	r		s	a	e	y	d		n	i		h	t	s		e	c	e	r	m		t	i	a	b	l	x	o	

w	e		n	e	e	d		t	o		m	a	k	e		c	o	p	i	e	s		b	e	f	o	r	e		w	e	d	n	e	s	d	a	y
e	w		e	n	d	e		o	t		a	m	e	k		o	c	i	p	s	e		e	b	o	f	e	r		e	w	n	d	s	e	a	d	y

- Again, clearly a rearrangement cipher.
  - But what's up with the letters jumping between words?
- $E(\text{text}) =$  “Switch each pair of letters.”  
 $E^{-1}(\text{text}) =$  “Switch each pair of letters.”

# Enciphering Texts

- **Week 3**: qeb nrfw fp obxav fk qeb pbzobq jxfiylu  
tb kbba ql jxhb zlmfbp ybclob tbakbpaxv

the quiz is ready in the secret mailbox  
qeb nrfw fp obxav fk qeb pbzobq jxfiylu

we need to make copies before wednesday  
tb kbba ql jxhb zlmfbp ybclob tbakbpaxv

- There's a consistent substitution...

- Plaintext: abcdefghijklmnopqrstuvwxyz  
Ciphertext: xyzabc\_ef\_hijklmnopqr\_tuvw

- $E(\text{text}) =$  “Caesar shift forward 23 (or back 3).”  
 $E^{-1}(\text{text}) =$  “Caesar shift back 23 (or forward 3).”

# Enciphering Texts

- **Week 4**: ht4 l13b 3j k45xc 3n ht4 j4yk4h p53qz2d  
f4 n44x h2 p5r4 y2m34j z4w2k4 f4xn4jx5c

the quiz is ready in the secret mailbox  
ht4 l13b 3j k45xc 3n ht4 j4yk4h p53qz2d

we need to make copies before wednesday  
f4 n44x h2 p5r4 y2m34j z4w2k4 f4xn4jx5c

- Again, there's a consistent substitution...

- Plaintext: abcdefghijklmnopqrstuvwxyz  
Ciphertext: 5zyx4w\_t3\_rqpn2mlkjh1\_fdcb

# Enciphering Texts

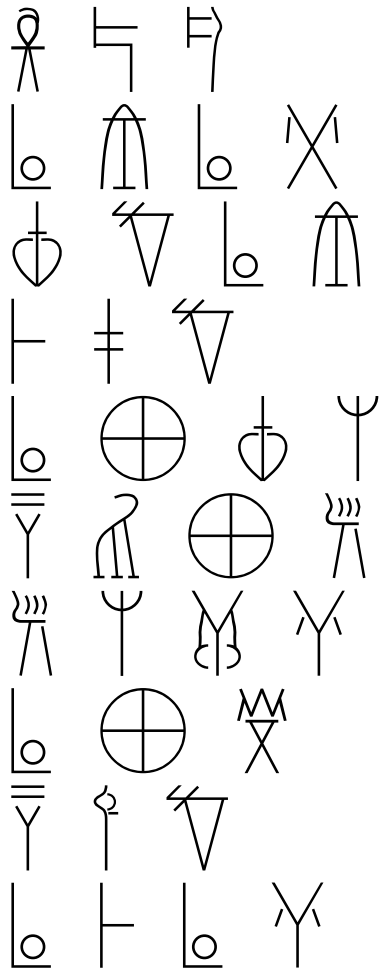
- **Week 5**: ord jsea cs inkob xs ord dobmoc hylvskw  
og noox yd oukw coszym obypol ikncoxnog

the quiz is ready in the secret mailbox  
ord jsea cs inkob xs ord dobmoc hylvskw

we need to make copies before wednesday  
og noox yd oukw coszym obypol ikncoxnog

- This time, there's no consistent substitution...
  - ...but there's some.
  - In fact, there are a lot of O's in the words with E's, S's in the words with I's...
- $E(\text{text}) =$  "Caesar shift forward 10 and reverse."  
 $E^{-1}(\text{text}) =$  "Caesar shift back 10 and reverse."

# Brae Nil



*kimono* ‘robe’

*samurai* ‘warrior’

*tamari* ‘soy sauce’

*orikami* ‘paper-folding’

*karate* ‘martial art’

*karaoke* ‘empty-orchestra’

*satori* ‘enlightenment’

*ikepana* ‘flower arranging’

*katakana* ‘writing system’

*kamikaze* ‘divine-wind’

- How to match them up?

# Brae Nil

- *ka-ta-ka-na* and *ka-mi-ka-ze*: both are going to be A-???-A-???.
  - ...which must be  $\underline{\circ} \vdash \underline{\circ} \Upsilon$  and  $\underline{\circ} \hat{\Lambda} \underline{\circ} \times$ . Which is which?
- Either  $\vdash$  or  $\hat{\Lambda}$  must be *ta*; the other is *mi*. *ta* begins one of the Japanese words (and ends none); *mi* ends one (and starts none).
  - So given  $\circlearrowleft \nabla \underline{\circ} \hat{\Lambda}$  and  $\vdash \ddagger \nabla$ ...
  - $\underline{\circ} \vdash \underline{\circ} \Upsilon = \text{ka-ta-ka-na}$ ,  $\vdash \ddagger \nabla = \text{ta-ma-ri}$ ;
  - $\underline{\circ} \hat{\Lambda} \underline{\circ} \times = \text{ka-mi-ka-ze}$ ,  $\circlearrowleft \nabla \underline{\circ} \hat{\Lambda} = \text{o-ri-ka-mi}$
- $\underline{\circ} = \text{ka}$ ,  $\vdash = \text{ta}$ ,  $\Upsilon = \text{na}$ ,  $\ddagger = \text{ma}$ ,  $\nabla = \text{ri}$ ,  $\hat{\Lambda} = \text{mi}$ ,  $\times = \text{ze}$ ,  $\circlearrowleft = \text{o}$ ,  $\hat{\Lambda} = \text{mi}$ 
  - So  $\underline{\circ} \oplus \circlearrowleft \Upsilon = \text{ka-???-o-???} = \text{ka-ra-o-ke}$
  - ...and so on.
- Thus:
  - *Naomi* =  $\text{na-o-mi} = \Upsilon \circlearrowleft \hat{\Lambda}$
  - *mimosa* =  $\hat{\Lambda} \vdash \Upsilon$
- And  $\ddagger \overset{\text{w}}{\Lambda} \times = \text{ma-i-ze}$ , which would be “maize”...
  - except that the syllables are based on pronunciation, not spelling.