7467 mod 2464 = 75, r.= 75, 21=3 $X_3 = X_1 - 3 \cdot X_2 = 1$ 43=41-3.42=-3

 $\chi_4 = \chi_2 - 32\chi_3 = -32$

2464 mod
$$75 = 64$$
, $72 = 64$, $92 = 32$
 $14 = 12 - 3213 = -32$
 $14 = 12 - 3213 = 1 + 32 \cdot 3 = 1 + 96 = 97$

75 mod
$$64 = 11$$
, $r_3 = 11$, $g_3 = 1$
 $x_5 = x_3 - x_4 = [+3z = 33]$
 $y_5 = y_3 - y_4 = -3 - 97 = -100$

64 mod $11 = 9$, $r_4 = 9$, $q_4 = 5$
 $x_6 = x_4 - 5x_5 = -32 - 5 : 33 = -32 - 165 = -197$
 $y_6 = y_4 - 5y_5 = 97 - 5x - 100 = 597$

11 mod $9 = 2$, $r_5 = 2$, $g_5 = 1$
 $x_7 = x_5 - x_6 = 33 + 197 = 230$
 $y_7 = y_5 - y_4 = -100 - 597 = -697$

9 mod $2 = 1$, $r_6 = 1$, $q_6 = 4$
 $x_6 = x_6 - 4x_7 = -197 - 4 \times 30 = -197 - 920 = -1117$
 $y_6 = y_6 - 4y_7 = 597 + 4x_697 = 3385$

2 mod $1 = 0$, $1 = 0$, $1 = 0$

12 mod $1 = 0$, $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod $1 = 0$

16 mod $1 = 0$

17 mod $1 = 0$

18 mod $1 = 0$

19 mod $1 = 0$

10 mod $1 = 0$

11 mod $1 = 0$

11 mod $1 = 0$

12 mod $1 = 0$

13 mod $1 = 0$

14 mod $1 = 0$

15 mod

we have at = | mod | & take a = 11, (116 = 1) mod 18, then ((116) = 116) mod 18 => | 42 mod 18 = | And 115 mod 18 = 5 : [(1142 mod 18) [115 mod 18)] mod 18 = 5 > 1147 mod 18=5 % X = (| # 5. $\begin{cases} 3 = x \mod 7 \\ 5 = x \mod 11 \Rightarrow M = 924 \end{cases}$ 2 = x mod 12 M1=132 M2=84 M3=77 Mi'mod 7 = 6, Mi'mod 11 = 8, Mi'mod 12=5 x= (3x132x6+5x84x8+2x77x5) mod 924 = (2376 + 3360 + 770) mod 924 = 6506 mod 924 = 38# 6. Using program to calculate the frequency of each alphabet The alphabet "n" has the most frequencies of others. We suppose "n" as "e".

And we find "ozn" which appears for many times. So, substitute "02 n" as "the" At line four, there is a word for only one alphabet "q", it may be "a" or "I", at here, choosing "a"

Then suppose the third word at first line "wqc" as "was". And another word "wzsxz" as "which". After a few supposing substitution, we can decrypt this message "phileas fogg was not known to have either wife or children, which may happen to the most honest people seither relatives or near friends, which is certainly more unusual. he lived alone in his house in saville row, whither non penetrated a single domestic suffered to serve him he breakfasted and dined at the club, at hours mathematically fixed, in the

	Sar	ne	101	0m ,	at	the	ટ ક	Samo	e ti	able	, ne	ever	ta	king	his	me	als	wir	eh	otl	ver			
														ا م									Ł	
	ex0	ctlu	. 1	idn	ia h		nole	A f	ກ 1	reti	re 4	at.	DNC	2 60	k	ed	he	n	eve	~	MER	d		
	the	Co	SU	ch	am k	0ers		which	h. +	the.	We'	fuen	\ 01	ovide	٠.	hor	it		favo	Med		men	nbe	٧<
	he	DOLS	se o	lt	21	Noc	lrs.	but	. n	+ +	he	tw	enta	-fou	r	in.	sav	ille	v	OW)	ا ج	the	y in	٦.
	SIPE	Poin	Δ.	אמ	mal	cino	h	is	toil	et .	, H		4						ľ					
	,,,		4			9					4													
7.	٢	0	N.	0	Т		D	+ 6.	n (2	+	ov 6	> n	LAT	eni	n	مام	c+.	,	200	+ .				
	n	e	M	ヌ	7									tts										
	v	b	C	t	a		٩	< S11	υm	6	s re	Stl	() ce	x	CR	NO	t.	t.we	2				
	6	i/j	k	m	4									nyi										
		S					Į,			ď				9.		10.1								
	-				7.5		, D	t	hor	1 4.	ดทธ	ی و	Me.	nir	16.	િલ	1	1 0	ctic	2 1 0.				
														t t										
														cre										
							re	0116	>c+	o (C	0 e d	in	forw	ati	DN C	, "	,,							
								0	-30		18		30111	l occi		^ 1								
ጵ	\\	100	fm	٥	att		eu	CI	IO	1.1	a	~P.	off		nv	atk		er		han	. 6	o io		
8.	" -	iee	tm	e "	att	; h	eu ''	કા	la	lpl	æ	e	a t(. е	ŊΥ	ath	L	er	t	han	, e	eig		
8.	_ h	ta		n	att	2 E	eu ''	51	la	lpl						ath	L	er					1	
8.	l 12	ta 4	4	n 	att	. h 22	leu ''	કા	<u>J</u> Q	lpl	Γ	49	71	(00)		ath	L	er		22	20	22		
8.	h (ک (۹	ta 4 12	4	n I	att	22 22	eu ''	કા	J O	lpl		49 71	71	(b0)		ath	L	er		[22 (9	20 2	22		
8.	h (2 เจ	ta 4 12 19	4 4	n I	att	2 k	ieu ''	51	la	lpl		48 71 71	71 125 171	(60) (83) (90		ath	L	er		22 (9 (5	20 2 15	22		
8.	19 19 7	ta 4 12 19 4	4 4 19 20	n .	+	22			la	l _p l		4P 71 71 71 55	71 65 (7) (37)	(60) (83) (90)		ath		er		22 (9 (5	20 21 15	22		
8.	19 19 7	to, 4 12 19 4 20	4 4 9 20 0	n	+	22	5					41 71 71 71 55 58	71 025 (71 (37 124	(60) (83) (90) (31) 210						22 (9 (5 15	20 21 15 7 4	22		
8.	h [2 19 0 7 CP 11	12 19 4 20 15	4 4 9 28 0 11	n	1	3 4	5 6	M			()	4P 71 71 55 58	71 625 (71 (37 124 (4.8	(60) (83) (40) (31) 240 (89)		ath				22 (9 (5 25 6 (4	20 2 15 7 4	22 8 9 2		
8.	h 12 19 7 CP 11	to 4 (2 (9 4 20 (5 2	4 4 [9 20 0 [1 4	n	1	22	5 6	M			() () = ()	48 71 71 55 58 .18	71 125 171 137 134 148 28	(60) (83) (40) (39) 240 (89)						22 (9 (5 25 6 (4 6	20 21 15 7 4 18 2	22 8 9 2 7 2		
8.	h	t 0. 4 12 19 4 20 15 2	4 4 19 20 01 4	n	1	3 4	5 6	M			= (49 71 71 355 58 .18 32	71 125 171 137 124 148 28 17]	(60) (83) (90) (39) 240 (89) 28 (90)						22 (9 (5 25 6 (4 6	20 21 15 7 4 18 2	22 8 9 2 7 2 8		
8.	h 12 14 0 7 14 11 0 0 4	to. 4 12 19 4 20 15 2 19 3	4 4 19 28 0 11 4 19	n	1	3 4	5 6	M				49 71 71 71 555 58 18 32	71 125 171 137 124 148 28 17]	(60) (83) (90) (39) 240 (89) 28 (90) (66)						(22 (9 (15 125 6 (4 6 (5)	20 21 15 7 4 18 2 15	22 8 9 2 7 2 8 10		
8.	h	to. 4 12 19 4 20 15 2 19 13	4 4 19 20 0 11 4 19 17 7	n	1	3 4	5 6	M			= 0	49 71 71 555 58 18 32 171 49	71 125 137 134 148 28 17 149 111	(60) (83) (90) (39) 240 (89) 28 (90) (66) (42)						22 19 15 25 6 14 6 15	20 21 15 7 4 18 2 15 19	22 8 9 2 7 2 8 10 12		
8.	N 12 19 10 10 10 10 10 10 10	to 4 12 19 4 20 15 2 19 13 19 17	4 4 19 28 0 11 4 15 17 7 19	n	1	3 4	5 6	M			== 0	49 71 71 71 555 58 18 32 171 49 81	71 05 171 137 148 148 17 149 111	(83) (90) (83) (140) (189) (140) (140) (141) (178)						22 19 15 25 6 14 6 15 17	20 2 15 7 4 18 2 15 19 7	22 8 9 2 7 2 8 10 12 16		
8		to 4 12 19 4 20 15 2 19 13 19 17 0	4 4 19 20 0 11 4 19 17 7 19 13	n	1	3 4	5 6	M				4P 71 71 555 558 11P 322 171 49 87	71. 055 (171) (137) (148) (17) (149) (11) (17) 886	(60) (83) (50) (31) 240 (83) (40) (60) (60) (142) (198) 87						(22 (9 (5) 15 6 (4) 6 (5) (9 15) 20	20 21 15 7 4 18 2 15 19 7	22 8 9 2 7 2 8 10 12 16 9		
88	12 19 0 7 CP 11 0 0 4 0 4 7 4	to 4 12 19 4 20 15 2 19 13 19 17 0 8	4 4 19 20 0 11 4 15 17 7 19 13 6	n	1	3 4	5 6	M				49 71 71 555 58 18 32 171 49 87 71	71 05 171 137 148 28 17 149 111 175 86 74	(60) (83) (40) (34) 240 (40) (64) (142) (198) 87 92						(22 19 15 15 6 14 6 15 17 9 15 20	20 21 15 7 4 18 2 15 19 7 19 8	22 8 9 2 7 2 8 10 12 16 9 14		
8		to 4 12 19 4 20 15 2 19 13 19 17 0 8 19	4 4 19 20 0 11 4 19 17 7 19 13	n	1	3 4	5 6	M				49 71 71 555 58 18 32 171 49 87 71	71 05 171 137 148 28 17 149 111 175 86 74	(60) (83) (50) (31) 240 (83) (40) (60) (60) (142) (198) 87						(22 (9 (5) 15 6 (4) 6 (5) (9 15) 20	20 21 15 7 4 18 2 15 19 7	22 8 9 2 7 2 8 10 12 16 9 14		

Then translate the numbers to alphabets. We can get the answer: WIN TUB PPI ZHJ GEC OSH GCC PPI TTK JHM PTQ DIJ KWO TTT DBY # 9. Key: hello > 7,4,11.11,14 Word: cryptographic > encrypt: JVJAHVKCLDOMN* (0.a) send more money ⇒ 18 4 13 3 12 14 17 4 12 14 13 4 ±4 + 3 11 5 7 17 21 0 11 14 8 7 13 9 = 21 15 18 10 29 35 17 15 26 12 20 17 33 mod 26 21 15 18 10 3 9 17 15 0 22 20 17 7 ⇒ V P S K D J R P A W LIRH => encrypt: VPSKDJRPAWURH * (b) VPSKDJRPAWDRH 3 2 1 15 18 10 3 9 17 15 0 22 20 17 7 - 201871314191344343 = 19 15 0 3 10 -5 -2 2 -4 18 17 13 4 mod 26 (9 (5 0 3 16 21 24 2 22 18 17 13 4 > key: 1915 0 3 16 21 24 2 22 18 17 13 4 [[. [5]: I. 151-1=150=2×75 $\begin{array}{l}
\boxed{1} \text{ let } a = 43 \\
43^{150} \mod |5| = |43^{75} \mod |5| = |43^{75} \mod |5| = |5|
\end{array}$ let a= 98 98150 mod 151 = 9875 mod 15 =1

let a = 25 let a=129 (29¹⁵⁰ mod |5|=|
129⁷⁵ mod |6|=-| 25150 mod 15/ =1 25 75 mod [5] =1 From I and I, we can conclude 151 is probably a prime number. y. 161: I. 161-1=255 II. let a = 15 (5160 mod (6) = (155 mod (6))25 mod (6) = (992 mod (6))24 mod (6) = (1412 mod 161)23 mod 161 = (782 mod 161)22 mod 161 = (1272 mod (6/)2 mod (6/ = 292 mod (61 = 36 36 \$ 1, from Fermat's Little Theorem, we can have the answer that 161 is not a prime number. A