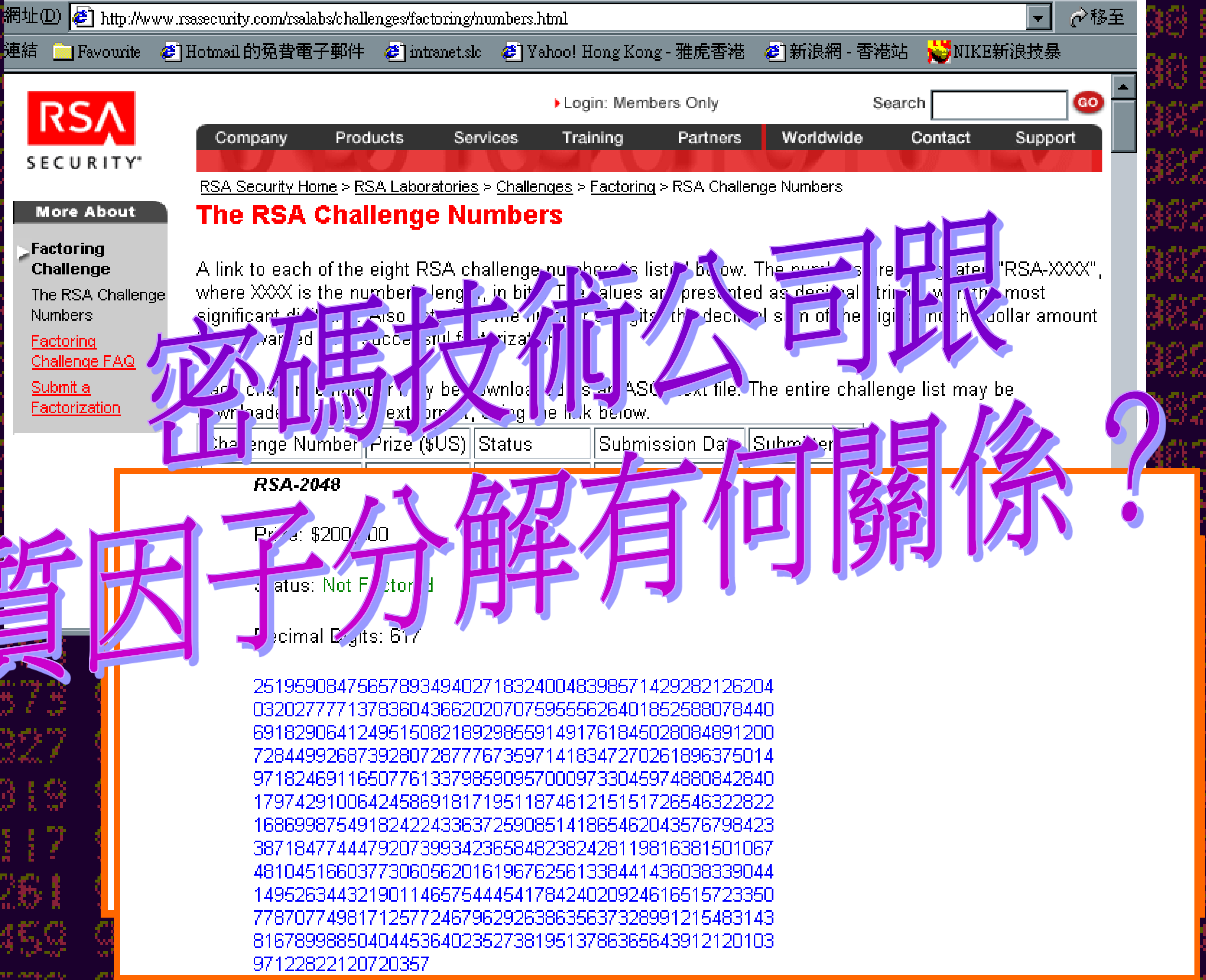
密碼之謎

獎金：$10000 美元

- 只要你可以**質因子分解**以下數字，便可赢取現金一萬美元：
- 188198812920607963838697239461650439
807163563379417382700763356422988859
715234665485319060606504743045317
388011303396716199692321205734031879
550656996221305168759307650257059
- (位數：174)

密碼技術公司跟質因子分解有何關係？



RSA Security Home > RSA Laboratories > Challenges > Factoring > RSA Challenge Numbers

The RSA Challenge Numbers

A link to each of the eight RSA challenge nu…s list… b…ow. The … re… ated "RSA-XXXX", where XXXX is the number… leng…, in bit… T… values ar… pres…ted as decimal … trin… w… th… most significant di… Also … the … digits, th… deci…l s…n of the digi… and th… dollar amount …war…ed … ucce…sful f…torizat…

…ch cha… … y be …wnloa… … s … ASC… …xt file. The entire challenge list may be …wnloade… …ext form… … g …e l…k below.

Cha…enge Number	Prize ($US)	Status	Submission Dat…	Subm…er

RSA-2048

Pri…e: $200,…00

…tatus: Not F…ctor…d

…ecimal D…gits: 617

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035
7

密碼術

Cryptography

一種偽裝訊息，唯有指定的
收信人才能讀出原意的技術

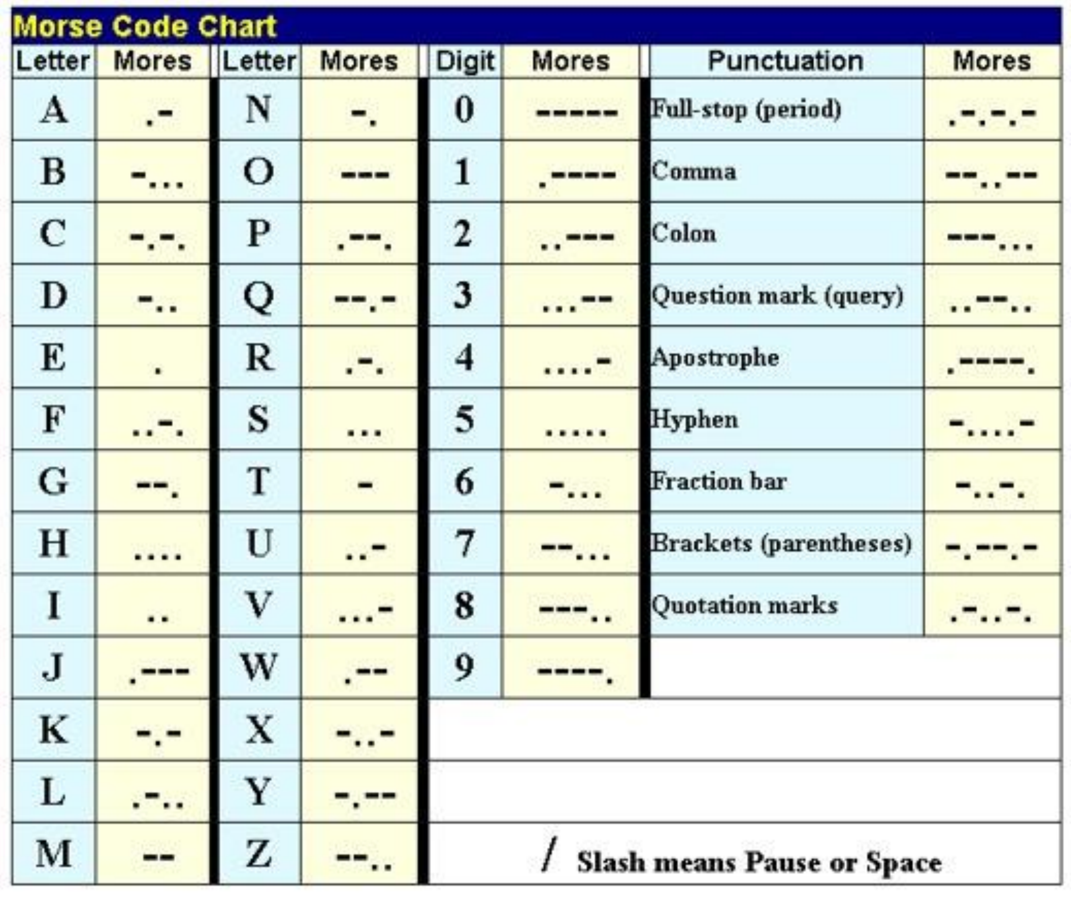
© 2002 MEDIAASIA GROUP ALL RIGHTS RESERVED.

無間道
INFERNAL AFFAIRS
梁朝偉
劉德華
12月全城同道

© 2002 MEDIAASIA GROUP ALL RIGHTS RESERVED.

摩斯密碼

摩斯密碼 Morse Code



Morse Code Chart

Letter	Mores	Letter	Mores	Digit	Mores	Punctuation	Mores
A	.-	N	-.	0	-----	Full-stop (period)	.-.-.-
B	-...	O	---	1	.----	Comma	--..--
C	-.-.	P	.--.	2	..---	Colon	---...
D	-..	Q	--.-	3	...--	Question mark (query)	..--..
E	.	R	.-.	4	....-	Apostrophe	.----.
F	..-.	S	...	5	.....	Hyphen	-....-
G	--.	T	-	6	-...	Fraction bar	-..-.
H	....	U	..-	7	--...	Brackets (parentheses)	-.--.-
I	..	V	...-	8	---..	Quotation marks	.-..-.
J	.---	W	.--	9	----.		
K	-.-	X	-..-				
L	.-..	Y	-.--				
M	--	Z	--..	/ Slash means Pause or Space			

– 解碼方法已經公開，不算『密碼』。

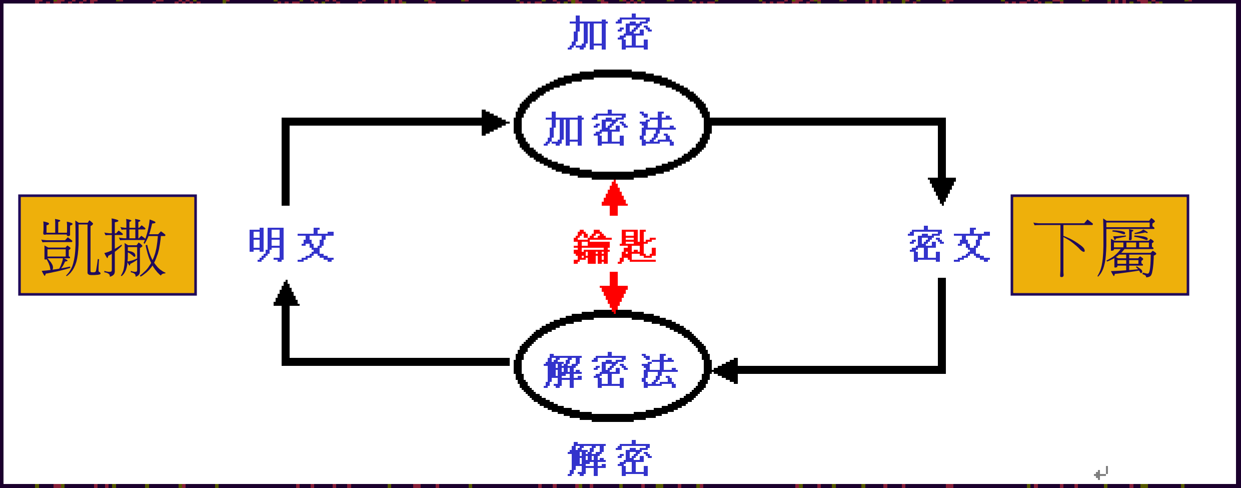
編碼者與解碼者的永恒鬥爭

凱撒密碼
－古老的加密法

- 把每個字母向後移三個位
- 例：I love you →loyhbrx
- 加密公式：

  密碼 =（明碼 + 3）mod 26

例：明碼 y〔25〕，(25+3)÷26 餘數是 2；所以密碼是 b〔2〕



加密

加密法

凱撒

明文

鑰匙

密文

下屬

解密法

解密

- 要破解密碼，必須要找出密匙(Key)
- 『+3』是凱撒密碼的密匙
- 密匙可以是非常複雜，甚至是隨機數目
- 加密和解密雙方都擁有相同密匙，屬於對稱系統

統計學大破凱撒密碼！

頻率分析法

- 阿拉伯人在公元九世紀已開始研究，十九世紀歐洲人廣泛使用。
- 這是統計學和語言學的合作，還要高強的推理能力。

letter	frequency (%)	letter	frequency (%)
a	8.167	n	6.749
b	1.492	o	7.507
c	2.782	p	1.929
d	4.253	q	0.095
e	12.702	r	5.987
f	2.228	s	6.327
g	2.015	t	9.056
h	6.094	u	2.758
i	6.966	v	0.978
j	0.153	w	2.360
k	0.772	x	0.150
l	4.025	y	1.974
m	2.406	z	0.074

- 例如以下密碼：

K DKVO DYVN LI KX SNSYD, PEVV YP CYEXN KXN PEBI, CSQXSPISXQ XYDRSXQ.

- 先統計字母分佈：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	4	3	0	0	0	3	0	4	1	0	4	1	4	3	1	6	0	0	4	0	7	4	0

- 對比字母分佈，分析出密匙：

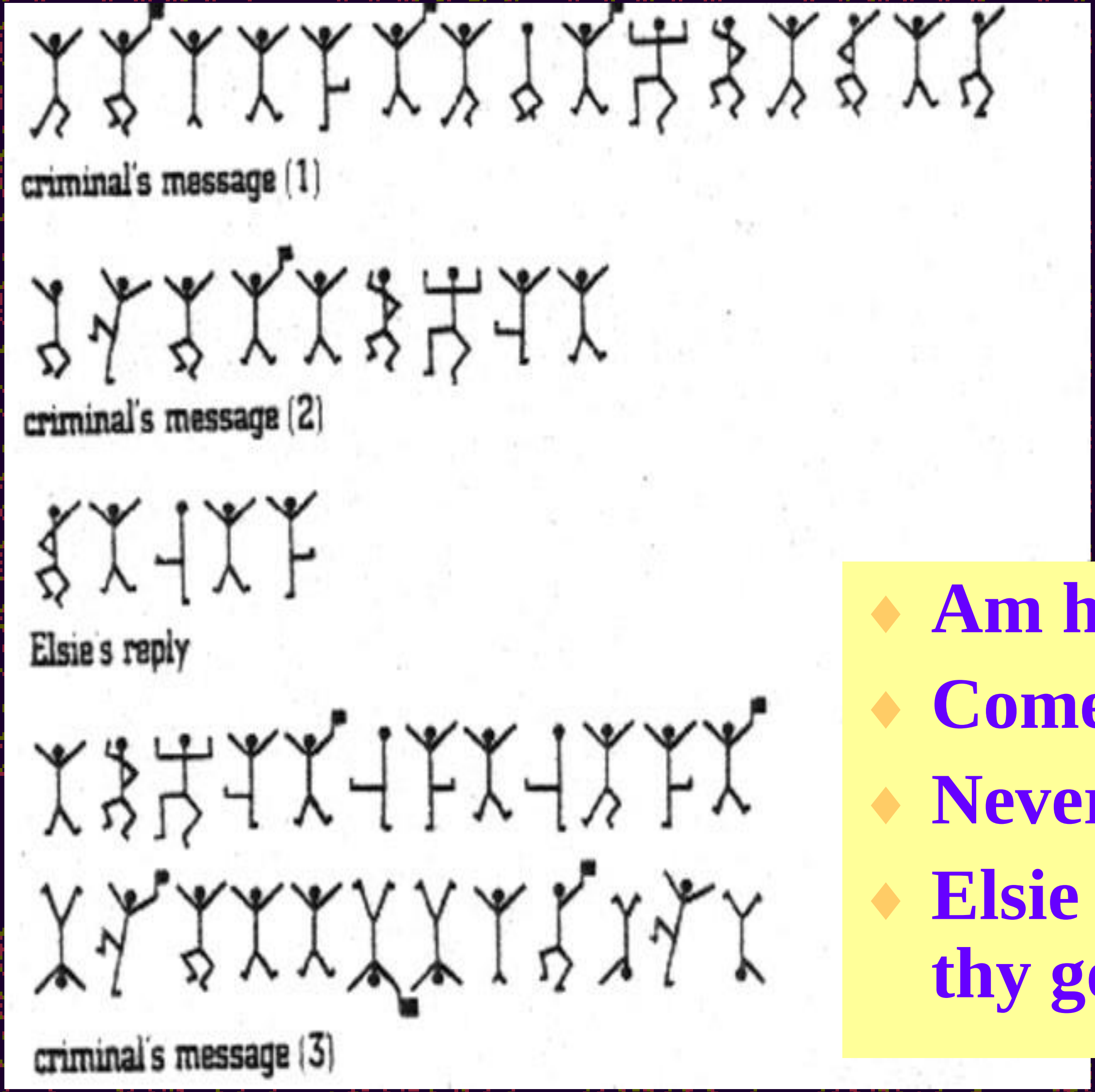
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

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

- 因此得出明碼：

A TALE TOLD BY AN IDIOT, FULL OF SOUND AND FURY, SIGNIFIYING NOTHING.

福爾摩斯探案『跳舞人形』


criminal's message (1)

criminal's message (2)

Elsie's reply

criminal's message (3)

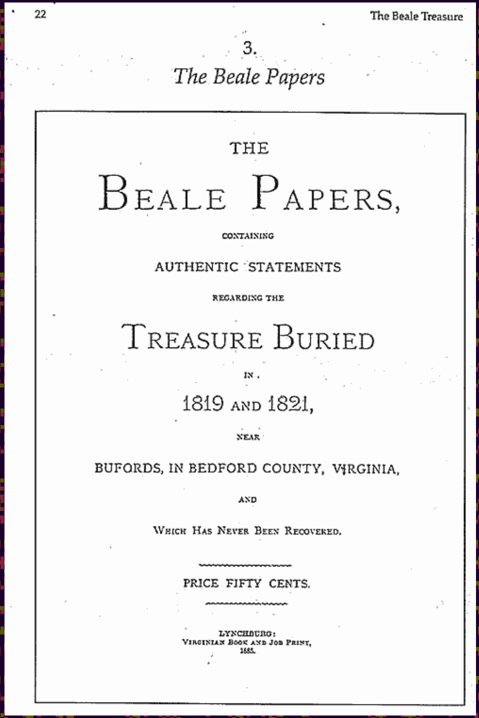
- Am here Ape Slaney
- Come Elsie
- Never
- Elsie prepare to meet thy god

無法破解的密碼

- 打敗『頻率分析法』
  - 同一個字母可變成不同的密碼。
- 畢爾寶藏(Beale Treasure)的故事

・1885年美國一位神祕人出版了一本小冊，當中記述了一個叫畢爾的人把大批黃金埋藏在維珍尼加州某處，並把祕密用密碼寫在三頁紙上，寄存在旅館老闆處，然後便失蹤了。

・這故事揭起了破解密碼和尋寶熱，直至今日仍有很多專家在嘗試。



22 The Beale Treasure

3.

The Beale Papers

THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN .

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

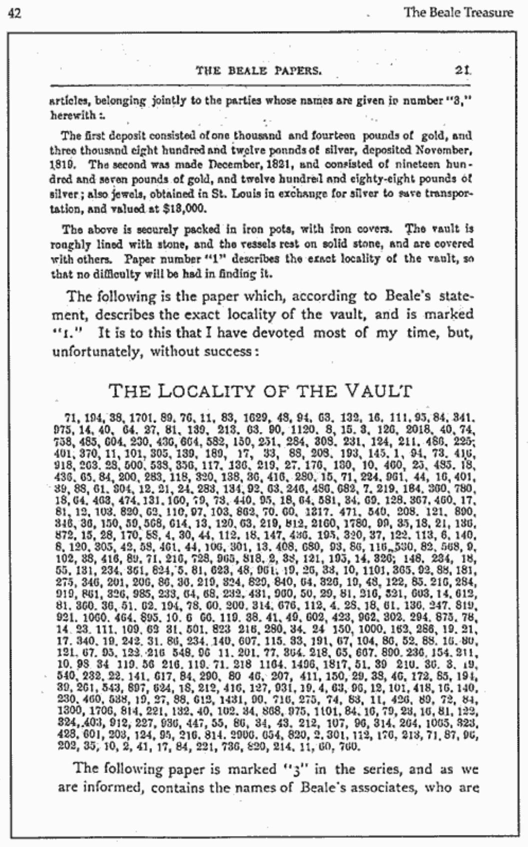
AND

WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

LYNCHBURG:
VIRGINIAN BOOK AND JOB PRINT,
1885.

- 其中第二頁己給該書的作者解破。
- 根據第二頁中講，第一頁紙是藏寶地點，第二頁紙是寶藏內容，第三頁紙他的夥伴及親人的名單。



articles, belonging jointly to the parties whose names are given in number "3," herewith :

The first deposit consisted of one thousand and fourteen pounds of gold, and three thousand eight hundred and twelve pounds of silver, deposited November, 1819. The second was made December, 1821, and consisted of nineteen hundred and seven pounds of gold, and twelve hundred and eighty-eight pounds of silver; also jewels, obtained in St. Louis in exchange for silver to save transportation, and valued at $13,000.

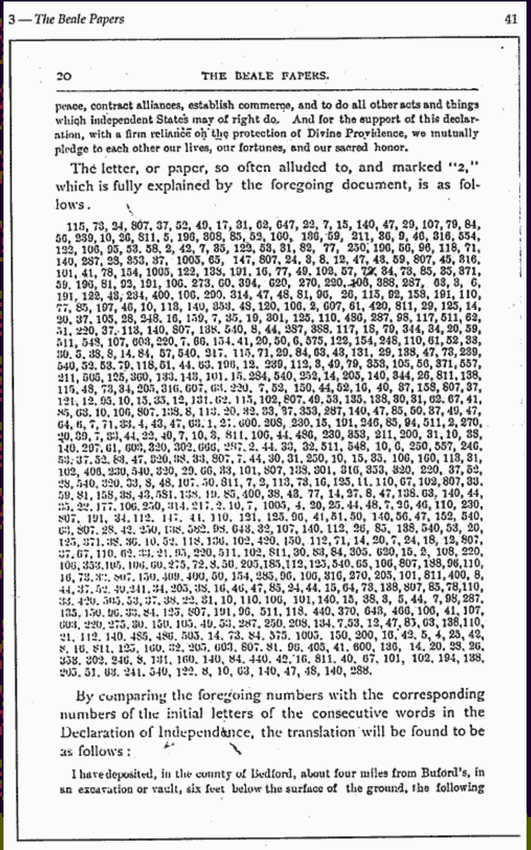
The above is securely packed in iron pots, with iron covers. The vault is roughly lined with stone, and the vessels rest on solid stone, and are covered with others. Paper number "1" describes the exact locality of the vault, so that no difficulty will be had in finding it.

The following is the paper which, according to Beale's statement, describes the exact locality of the vault, and is marked "1." It is to this that I have devoted most of my time, but, unfortunately, without success:

THE LOCALITY OF THE VAULT

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341,
975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74,
758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225;
401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416,
918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18,
436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401,
39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780,
18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17,
81, 12, 103, 820, 62, 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890,
346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136,
872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140,
8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9,
102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326; 148, 234, 18,
55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181,
275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284,
919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612,
81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819,
921, 1060, 464, 895, 10, 6 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78,
14, 23, 111, 109, 62 31, 501, 823 216, 280, 34, 24 150, 1000, 162, 286, 19, 21,
17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80,
121, 67, 95, 122, 216 548, 96 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211,
10, 98 34 119, 56 216, 119, 71, 218 1164, 1496, 1817, 51, 39 210, 36, 3, 19,
540, 232, 22, 141, 617, 84, 290, 80 46, 207, 411, 150, 29, 38, 46, 172, 85, 194,
39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140,
230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84,
1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122,
324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323,
428, 601, 203, 124, 95, 216, 814, 2900, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96,
202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.

The following paper is marked "3" in the series, and as we are informed, contains the names of Beale's associates, who are



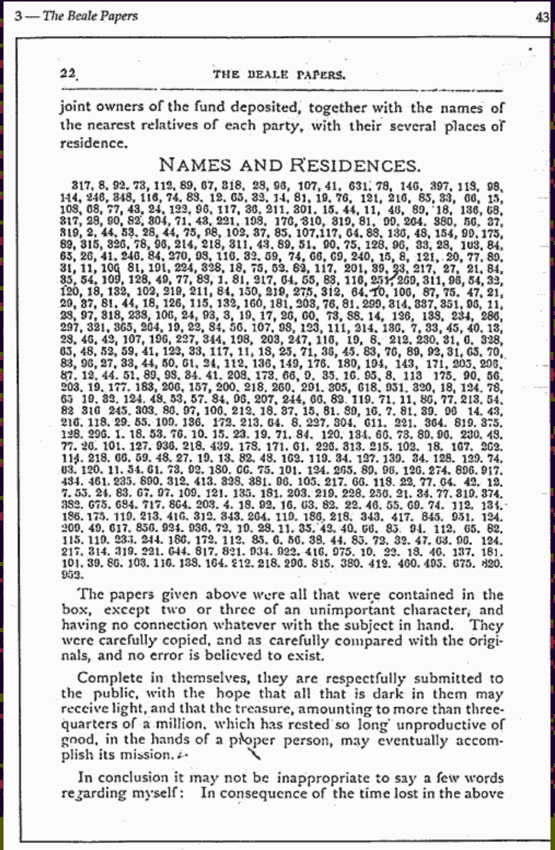
peace, contract alliances, establish commerce, and to do all other acts and things which independent States may of right do. And for the support of this declaration, with a firm reliance on the protection of Divine Providence, we mutually pledge to each other our lives, our fortunes, and our sacred honor.

The letter, or paper, so often alluded to, and marked "2," which is fully explained by the foregoing document, is as follows.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84,
56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554,
122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71,
140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316,
101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371,
59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6,
191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110,
77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14,
20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62,
51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59,
511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33,
30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239,
540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557,
211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138,
115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37,
121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47,
64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270,
20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38,
140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246,
53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31,
102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353, 320, 220, 37, 52,
28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11, 110, 67, 102, 807, 33,
59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27, 8, 47, 138, 63, 140, 44,
35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 44, 48, 7, 26, 46, 110, 230,
807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51, 50, 140, 56, 47, 152, 540,
63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140, 112, 26, 85, 138, 540, 53, 20,
125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150, 112, 71, 14, 20, 7, 24, 18, 12, 807,
37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811, 30, 83, 84, 305, 620, 15, 2, 108, 220,
106, 353, 105, 106, 60, 275, 72, 8, 50, 205, 185, 112, 125, 540, 65, 106, 807, 188, 96, 110,
16, 73, 32, 807, 150, 409, 400, 50, 154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8,
44, 37, 52, 40, 241, 34, 205, 38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110,
33, 420, 505, 53, 37, 38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287,
135, 150, 96, 33, 84, 125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107,
603, 220, 275, 30, 150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110,
21, 112, 140, 485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42,
8, 16, 811, 125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26,
353, 302, 246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138,
205, 51, 63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

By comparing the foregoing numbers with the corresponding numbers of the initial letters of the consecutive words in the Declaration of Independence, the translation will be found to be as follows:

I have deposited, in the county of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following



joint owners of the fund deposited, together with the names of the nearest relatives of each party, with their several places of residence.

NAMES AND RESIDENCES.

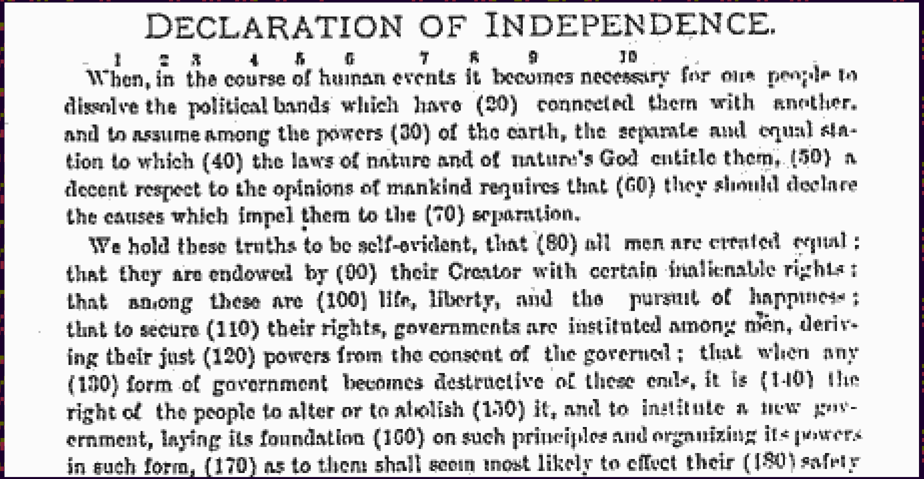
317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98,
114, 246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15,
108, 68, 77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68,
317, 28, 90, 82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37,
319, 2, 44, 53, 28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175,
89, 315, 326, 78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84,
65, 26, 41, 246, 84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89,
31, 11, 106, 81, 191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84,
35, 54, 109, 128, 49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32,
120, 18, 132, 102, 219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21,
29, 37, 81, 44, 18, 126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11,
28, 97, 318, 238, 106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286,
297, 321, 365, 264, 19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13,
28, 46, 42, 107, 196, 227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328,
65, 48, 52, 59, 41, 122, 33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70,
83, 96, 27, 33, 44, 50, 61, 24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296,
87, 12, 44, 51, 89, 98, 34, 41, 208, 173, 66, 9, 35, 16, 95, 8, 113 175, 90, 56,
203, 19, 177, 183, 206, 157, 200, 218, 260, 291, 305, 618, 951, 320, 18, 124, 78,
65 19, 32, 124, 48, 53, 57, 84, 96, 207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54,
82 316 245, 303, 86, 97, 106, 212, 18, 37, 15, 81, 89, 16, 7, 81, 39, 96 14, 43,
216, 118, 29, 55, 109, 136, 172, 213, 64, 8, 227, 304, 611, 221, 364, 819, 375,
128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71, 84, 120, 134, 66, 73, 89, 96, 230, 48,
77, 26, 101, 127, 936, 218, 439, 178, 171, 61, 226, 313, 215, 102, 18, 167, 262,
114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119, 34, 127, 139, 34, 128, 129, 74,
63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124, 265, 89, 96, 126, 274, 896, 917,
434, 461, 235, 890, 312, 413, 328, 381, 96, 105, 217, 66, 118, 22, 77, 64, 42, 12,
7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219, 228, 256, 21, 34, 77, 319, 374,
382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82, 22, 46, 55, 69, 74, 112, 134,
186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218, 343, 417, 845, 951, 124,
209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66, 85 94, 112, 65, 82,
115, 119, 233, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72, 32, 47, 63, 96, 124,
217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22, 18, 46, 137, 181,
101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412, 460, 495, 675, 820,
952.

The papers given above were all that were contained in the box, except two or three of an unimportant character, and having no connection whatever with the subject in hand. They were carefully copied, and as carefully compared with the originals, and no error is believed to exist.

Complete in themselves, they are respectfully submitted to the public, with the hope that all that is dark in them may receive light, and that the treasure, amounting to more than three-quarters of a million, which has rested so long unproductive of good, in the hands of a proper person, may eventually accomplish its mission.

In conclusion it may not be inappropriate to say a few words regarding myself: In consequence of the time lost in the above

第二頁的破解：書稿密碼 (book cipher)



DECLARATION OF INDEPENDENCE.

1 2 3 4 5 6 7 8 9 10

When, in the course of human events it becomes necessary for one people to dissolve the political bands which have (20) connected them with another. and to assume among the powers (30) of the earth, the separate and equal station to which (40) the laws of nature and of nature's God entitle them, (50) a decent respect to the opinions of mankind requires that (60) they should declare the causes which impel them to the (70) separation.

We hold these truths to be self-evident, that (80) all men are created equal: that they are endowed by (90) their Creator with certain inalienable rights; that among these are (100) life, liberty, and the pursuit of happiness; that to secure (110) their rights, governments are instituted among men, deriving their just (120) powers from the consent of the governed; that when any (130) form of government becomes destructive of these ends, it is (140) the right of the people to alter or to abolish (150) it, and to institute a new government, laying its foundation (160) on such principles and organizing its powers in such form, (170) as to them shall seem most likely to effect their (180) safety

以獨立宣言每個字的次序作為它第一個字母的密碼

I HAVE DEPOSITED IN THE COUNTY OF BEDFORD ABOUT FOUR MILES FROM BUFORDS IN AN EXCAVATION OR VAULT SIX FEET BELOW THE SURFACE OF THE GROUND … …THE FIRST DEPOSIT CONSISTED OF TEN HUNDRED AND FOURTEEN POUNDS (1014 lbs.) OF GOLD AND THIRTY EIGHT HUNDRED AND TWELVE POUNDS (3812 lbs.) OF SILVER, DEPOSITED NOV. EIGHTEEN NINETEEN.(NOV.1819)

THE SECOND WAS MADE DEC. EIGHTEEN TWENTY-ONE (DEC 1821) AND CONSISTED OF NINETEEN HUNDRED AND SEVEN POUNDS (1907lbs.) OF GOLD AND TWELVE HUNDRED AND EIGHTY EIGHT (1208 lbs.)OF SILVER; ALSO JEWELS OBTAINED IN ST. LOUIS IN EXCHANGE TO SAVE TRANSPORTATION, AND VALUED AT THIRTEEN THOUSAND DOLLARS ($13,000)……

單次密匙簿(*One-Time Pad*)加密法

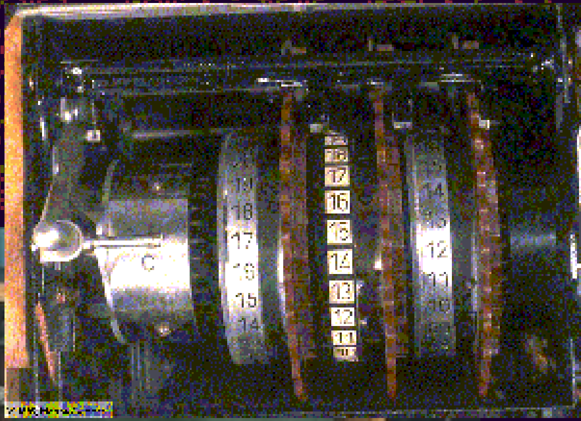
- 第一次世界大戰時，美國研究員發明單次密匙簿加密法，每次加密的密匙都不同。
- 明文：THE BRITISH HAVE FIFTY TANKS
- 密匙：SHE LOVES HIM SO VERY MUCH NOW

	T	H	E	B	R	I	T	I	S	H	H	A	V	E
	19	7	4	1	17	8	19	8	18	7	7	0	21	4
	S	H	E	L	O	V	E	S	H	I	M	S	O	V
	18	7	4	11	14	21	4	18	7	8	12	18	14	21
Add:	37	14	8	12	31	29	23	26	25	15	19	18	35	25
Mod:	11	14	8	12	5	3	23	0	25	15	19	18	9	25
	L	O	I	M	F	D	X	A	Z	P	T	S	J	Z

- 單次密匙簿加密法理論上很完美，但運作上很困難。

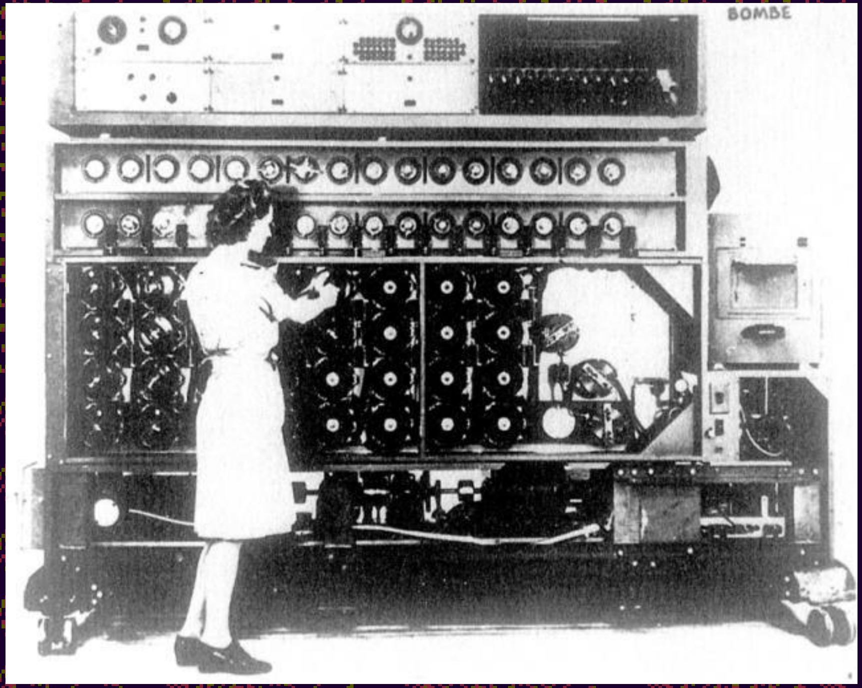
- 第一次世界大戰後，德國人發明了密碼機器『奇謎』(Enigma)。

- 二次大戰初期，依靠『奇謎』，德國的突襲戰術十分成功。



- 為了對付『奇謎』，英國人建立解碼機構柏雷屈里園(Bletchley Park)，召集一批數學家進行研究。

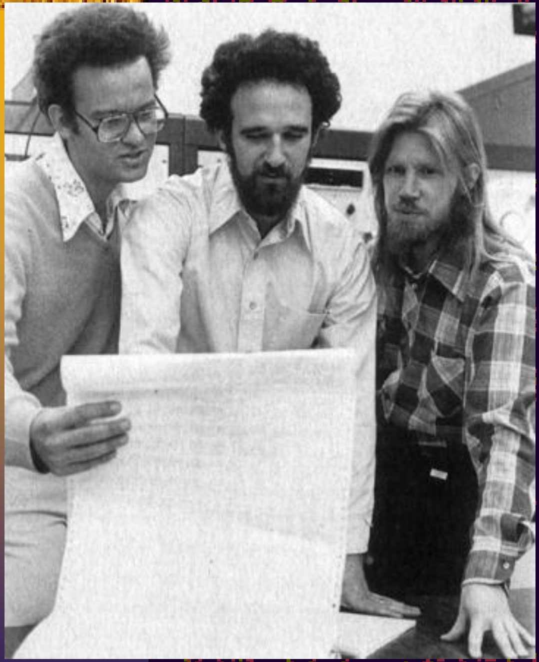
- 根據數學家圖靈(Alan Turing)的構思，英國製造了破解『奇謎』的機器—『炸彈』(The Bomb)。



- 柏雷屈里園的數學家不但破解了奇謎，也破解了義大利和日本的密碼，使戰爭提早結束。

進入電腦時代

- 互聯網的出現，大量訊息需要加密傳送，傳送密匙更做成很大困難。
- 公開密匙系統是廿世紀密碼學的最偉大成就



❖迪菲(Whitfield Diffie)

❖黑爾曼(Martin Hellman)

❖墨克(Ralph Merkle)

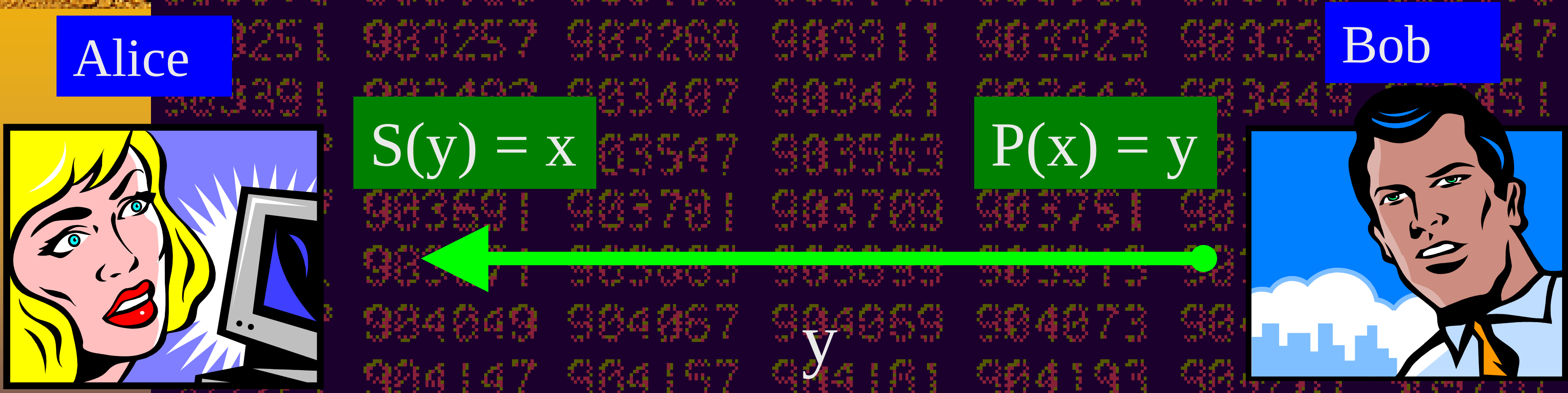
1975年發表他們的構想

甚麼是公開密匙？

例： x = 明碼；y = 密碼

P(x) 是 Alice 的公開密匙；

S(x) 是 Alice 的私人密匙。



Alice

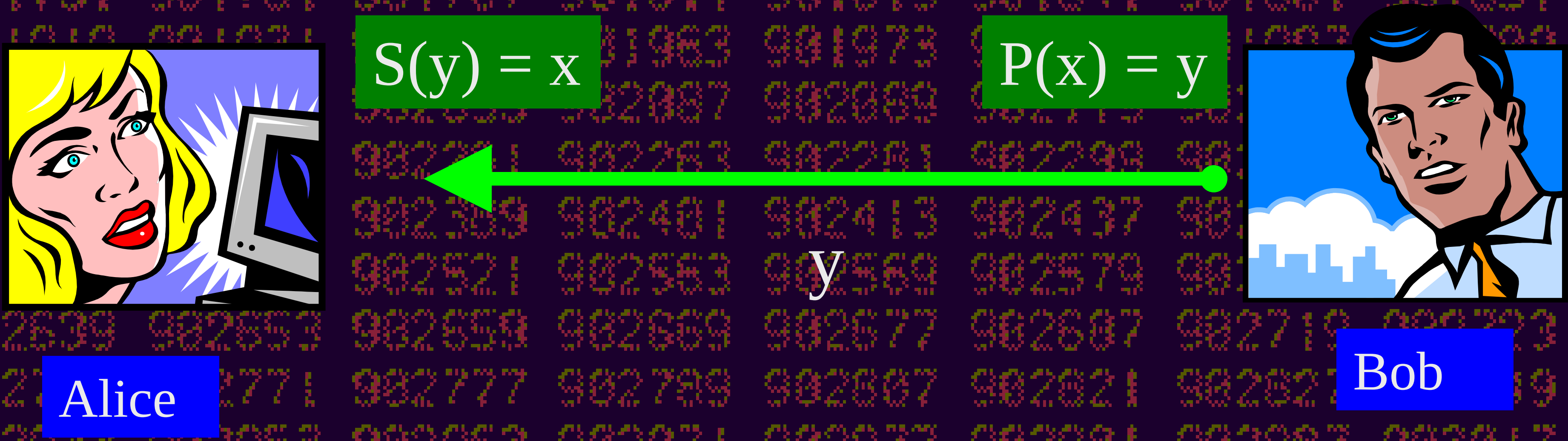
Bob

S(y) = x

P(x) = y

y

這樣，大家便毋須事前約定相同密匙，
而且全世界都可傳送密件給 Alice



S(y) = x

P(x) = y

y

Alice

Bob

S 是 P 的逆函數(Inverse function)，怎樣可以讓 Bob 知道 P 是甚麼，但他卻無法計出 S ？

如果 y = P(x) = 2x +1， 則 x = (y-1)/2 = S(x)

P(x) 必須是一種特別的單向函數(one-way function)

怎樣的函數才適合？？？？

RSA 運算法 (RSA Algorithm)

- 瑞維斯特 Ron Rivest
- 薛米爾 Adi Shamir
- 艾多曼 Leonard Adleman

- 他們在1977年發表論文，並把這運算法註冊專利。
- 20年後 RSA Data Security 公司市值超過二億美元。

RSA 運算法 (RSA Algorithm)

- RSA algorithm分成下列幾個步驟
  - 選擇『公開密匙』與『私人密匙』
    - Step 1：選擇兩個夠大的質數(prime numbers) **p**、**q**。
    - Step 2：**n** = **pq** ，**z** = (**p**-1)(**q**-1)
    - Step 3：選擇一數 **e**，**e** 需要小於 **n** 且與 **z** 互質
    - Step 4：選擇一數 **d**，使得 **ed** – 1 可以被 **z** 整除。換句話說

      ed mod **z** = 1
    - Step 5 :公開密匙 為 (**n**,**e**)，私人密匙為 (**n**,**d**)

- 將訊息 x 利用前面所計算出的 公開密匙 (n,e)加密

$$y = x^e \bmod n$$

- 利用私人密匙 (n,d)，將先前算出的 y 解密

$$x = y^d \bmod n$$

這涉及數論(Number Theory)的定理

➢要破解 RSA 密碼，就必須從 **(n,e)** 找出 **(n,d)**。

➢因為 **ed mod z = 1** 而 **z = (p-1)(q-1)**，所以只要出 p 和 q，便可找出 d 。

➢ n = p × q 而 p，q 都是質數。

➢這分解極困難，因此 RSA應用了絕佳的單向函數

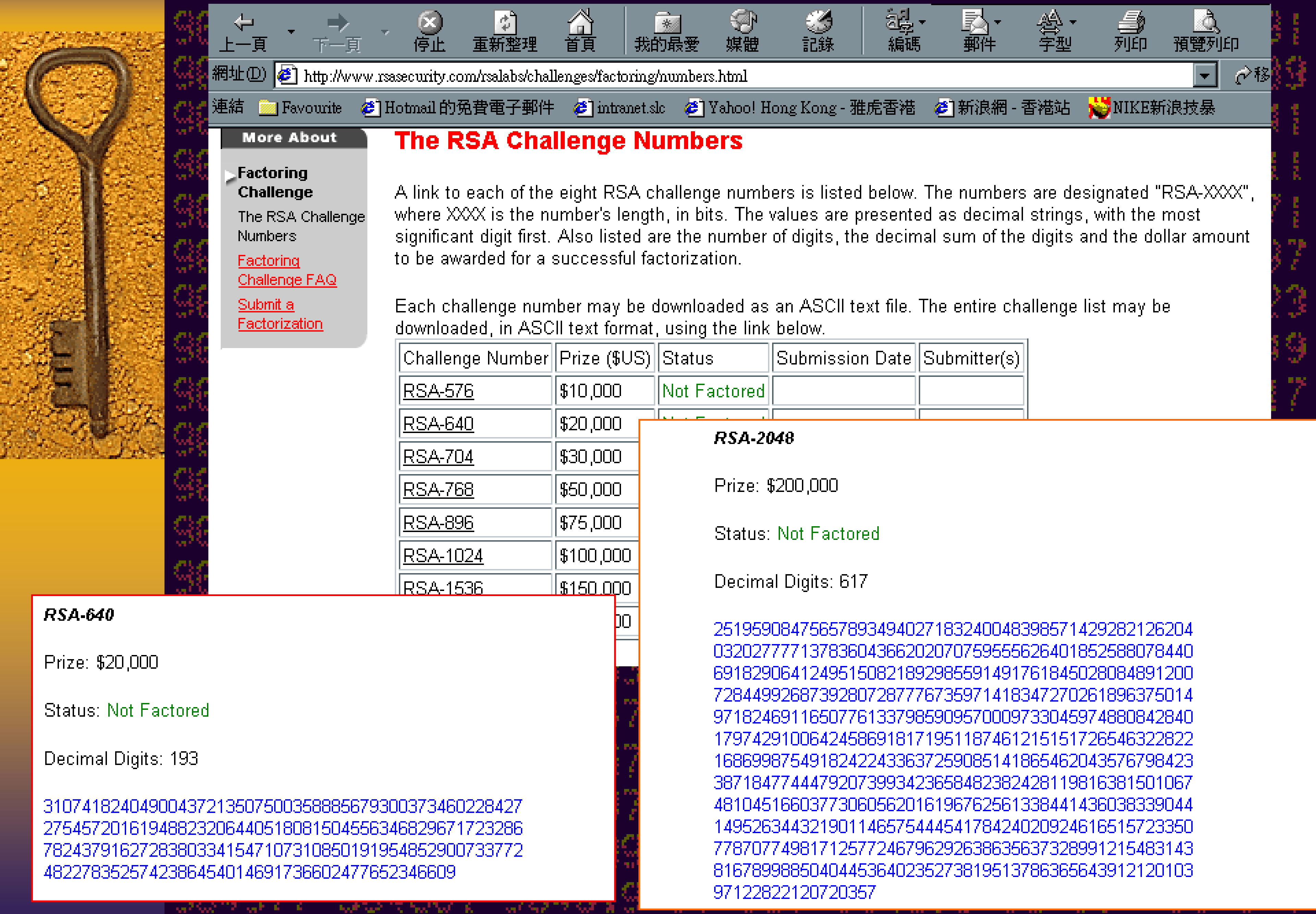
要分解 n = p x q 究竟有多難？

- 1977年 Scientific American 雜誌登出了 RSA-129，獎金是100美元。
- 17年後，超過600人利用互聯網，聯合不同地方的電腦，用了八個月時間，終於破解了 RSA – 129。

$$\begin{aligned} n = {} & 114381625757888867669235779976146 \\ & 612010218296721242362562561842935 \\ & 706935245733897830597123563958705 \\ & 058989075147599290026879543541 \end{aligned}$$

$$\begin{aligned} p = {} & 3490529510847650949147849619903898 \\ & 133417764638493387843990820577 \end{aligned}$$

$$\begin{aligned} q = {} & 3276913299326670954996198819083446 \\ & 1413177642967992942539798288533 \end{aligned}$$



http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html

The RSA Challenge Numbers

A link to each of the eight RSA challenge numbers is listed below. The numbers are designated "RSA-XXXX", where XXXX is the number's length, in bits. The values are presented as decimal strings, with the most significant digit first. Also listed are the number of digits, the decimal sum of the digits and the dollar amount to be awarded for a successful factorization.

Each challenge number may be downloaded as an ASCII text file. The entire challenge list may be downloaded, in ASCII text format, using the link below.

Challenge Number	Prize ($US)	Status	Submission Date	Submitter(s)
RSA-576	$10,000	Not Factored		
RSA-640	$20,000	Not Factored		
RSA-704	$30,000			
RSA-768	$50,000			
RSA-896	$75,000			
RSA-1024	$100,000			
RSA-1536	$150,000			
	00			

RSA-640

Prize: $20,000

Status: Not Factored

Decimal Digits: 193

```
31074182404900437213507500358885679300373460228427
27545720161948823206440518081504556346829671723286
78243791627283803341547107310850191954852900733772
4822783525742386454014691736602477652346609
```

RSA-2048

Prize: $200,000

Status: Not Factored

Decimal Digits: 617

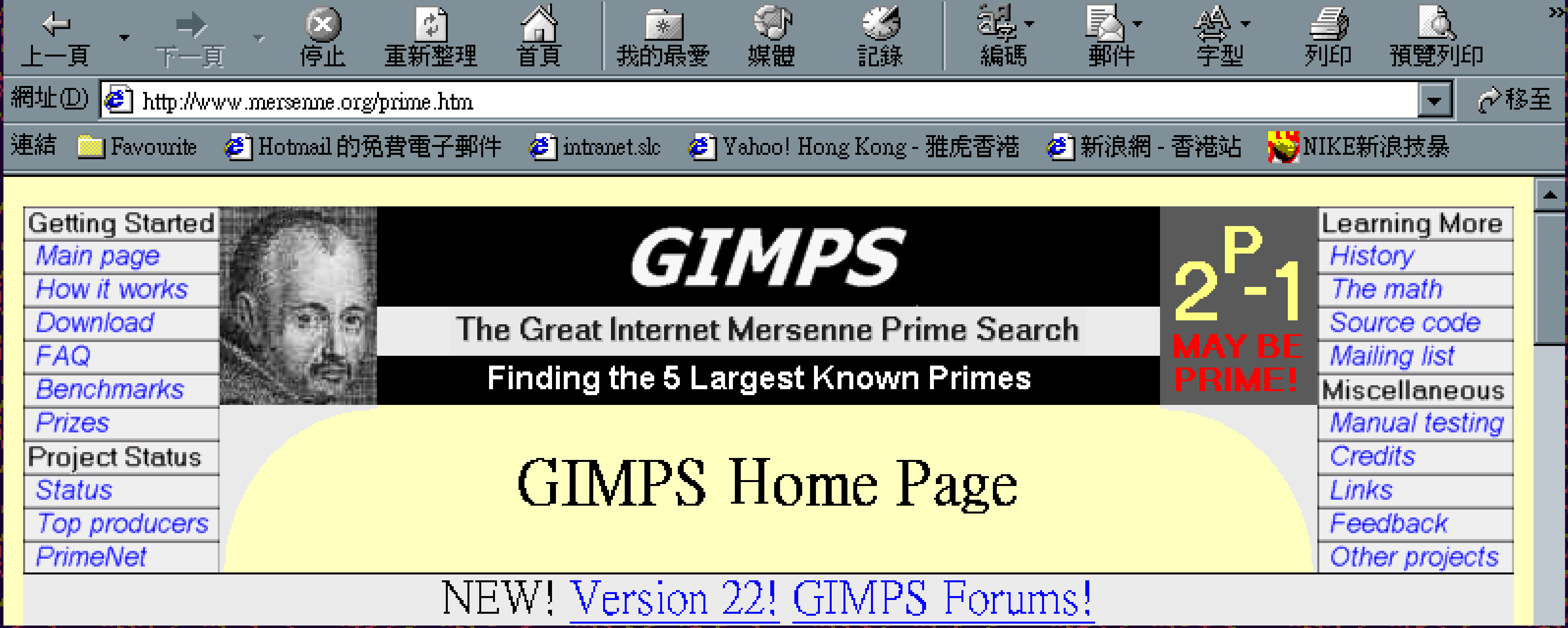
```
25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357
```

- ➢專家估計，一億台100 MHz Pentium 電腦合起來，分解一個 308 位數的 n (比129 位數大了十兆兆兆兆兆兆兆兆兆兆兆兆兆兆兆倍），大約需要一千年。

- ➢RSA的原則是：公開密匙的 n 值必須大得全球電腦聯合起來直至太陽系死亡也不能破解。

- ➢因此必須要找非常大的質數。

尋找最大的質數



The Great Internet Mersenne Prime Search

Finding the 5 Largest Known Primes

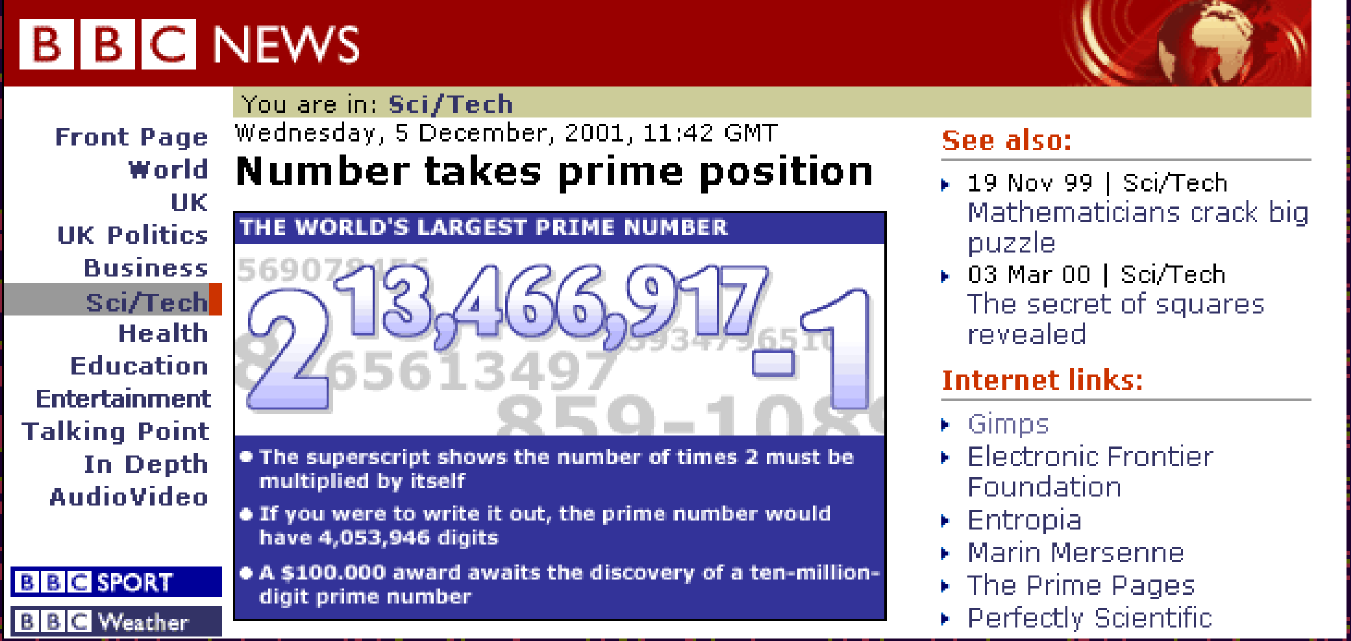
GIMPS Home Page

NEW! Version 22! GIMPS Forums!

- 梅森數（Mersenne number）

  $M_p = 2^p - 1$

- 當 p 是合數，可以証明 M_p 也是合數。
- 當 p 是質數， M_p 可能是質數，也可能是合數。
- 例如 $M_3 = 7$，$M_7 = 127$，$M_{11} = 2047$
- 把很大的質數代入 p ，然後測試答案是否質數，是現今尋找最大質數的方法。



BBC NEWS

Front Page
World
UK
UK Politics
Business
Sci/Tech
Health
Education
Entertainment
Talking Point
In Depth
AudioVideo

BBC SPORT

BBC Weather

You are in: Sci/Tech

Wednesday, 5 December, 2001, 11:42 GMT

Number takes prime position

THE WORLD'S LARGEST PRIME NUMBER

$2^{13,466,917}-1$

- The superscript shows the number of times 2 must be multiplied by itself
- If you were to write it out, the prime number would have 4,053,946 digits
- A $100.000 award awaits the discovery of a ten-million-digit prime number

See also:

- 19 Nov 99 | Sci/Tech
  Mathematicians crack big puzzle
- 03 Mar 00 | Sci/Tech
  The secret of squares revealed

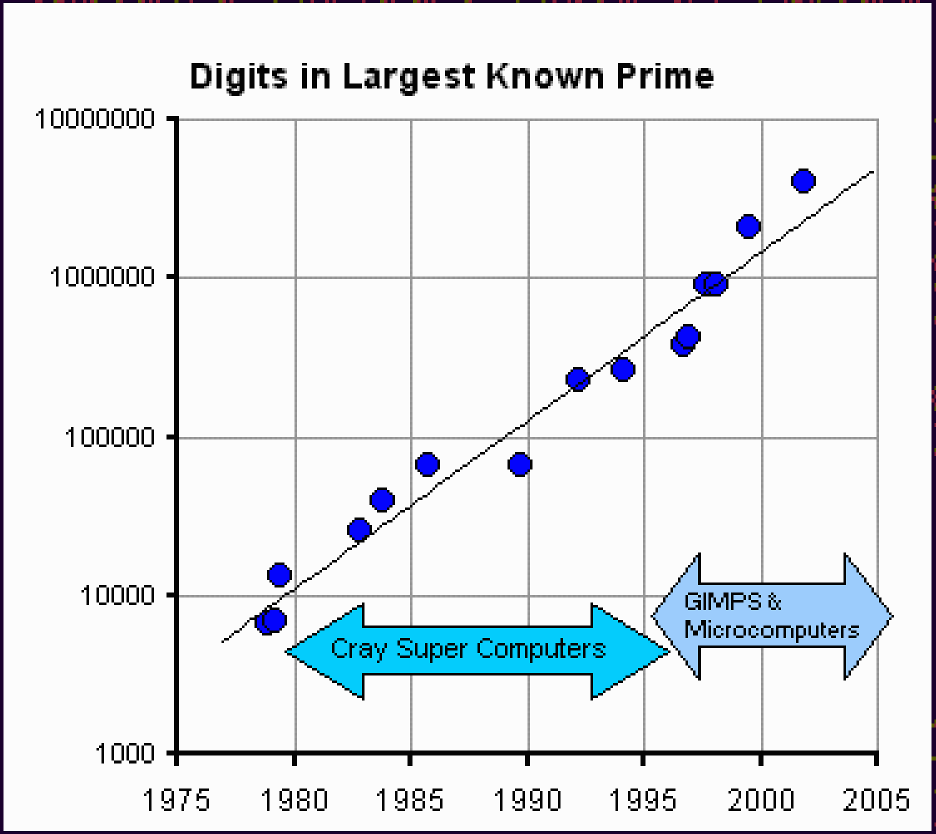
Internet links:

- Gimps
- Electronic Frontier Foundation
- Entropia
- Marin Mersenne
- The Prime Pages
- Perfectly Scientific

加拿大20歲青年 Micheal Cameron 在2001年11月發現了第39個梅森質數 $2^{13466917}-1$，它是個4053946 位數

Micheal 是GIMPS大約十二萬參加者之一，他用AMD TB 800 MHz 電腦，在餘暇時間運作了42日。

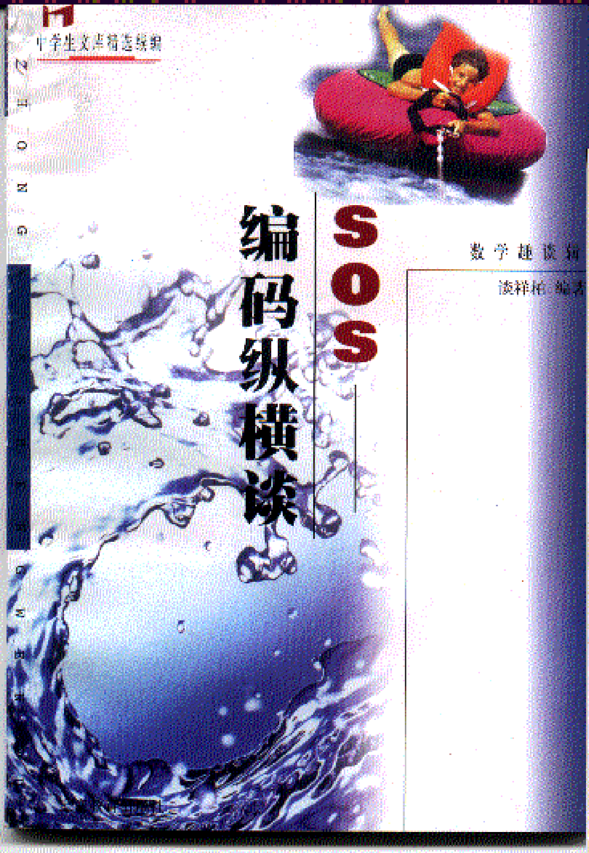
至今仍未發現有新的梅森質數。



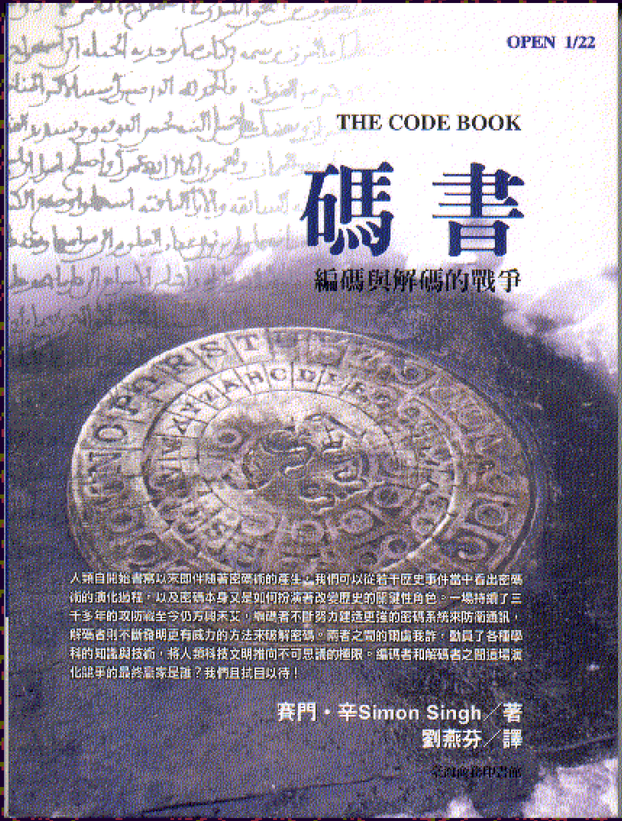
GIMPS：

首名找到一千萬位數的梅森質數，可獲十萬美元獎金！

有關密碼的書

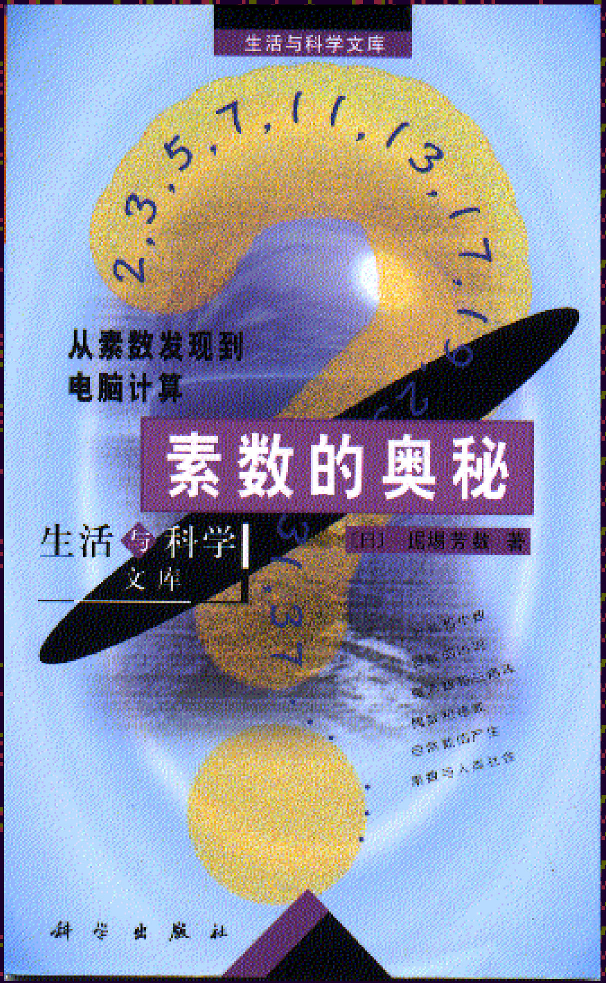


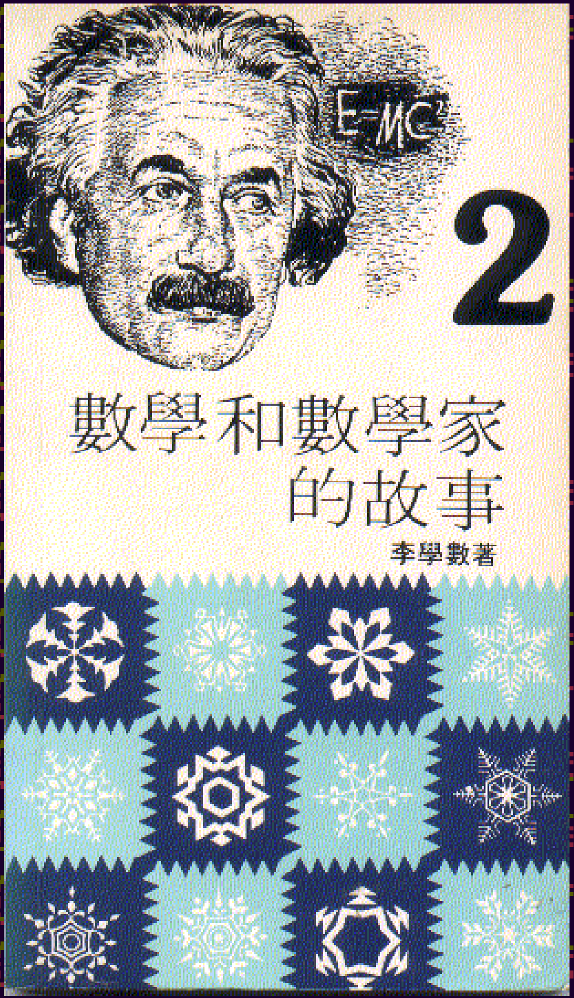
天下文化
科學文化
In Code
A Mathematical Journey
我的數學教育，
是從爸爸給的謎題開始的，
在不知不覺之中，
讓我有自信可以解決問題。
1999年愛爾蘭、歐洲青少年科學家首獎得主
數學小魔女
By Sarah Flannery
with David Flannery
葉偉文 譯



人類自開始書寫以來即伴隨著密碼術的產生。我們可以從若干歷史事件當中看出密碼術的演化過程，以及密碼本身又是如何扮演著改變歷史的關鍵性角色。一場持續了三千多年的攻防戰至今仍方興未艾，編碼者不斷努力建造更強的密碼系統來防衛通訊，解碼者則不斷發明更有威力的方法來破解密碼。兩者之間的爾虞我詐，動員了各種學科的知識與技術，將人類科技文明推向不可思議的極限。編碼者和解碼者之間這場演化競爭的最終贏家是誰？我們且拭目以待！

有關質數的書


生活与科学文库
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37
从素数发现到
电脑计算
素数的奥秘
生活与科学文库
[日] 堀场芳数 著
素数与人类社会
科学出版社


E=MC²
2
數學和數學家的故事
李學數著

再會