

獎金：\$10000 美元

◆ 只要你可以質因子分解以下數字，便可
贏取現金一萬美元：

◆ 18819881292060796383869723946165043
98071635633794173827007633564229888
59715234665485319060606504743045317
38801130339671619969232120573403187
9550656996221305168759307650257059

◆ (位數：174)



Login: Members Only

Search GO

Company Products Services Training Partners Worldwide Contact Support

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

The RSA Challenge Numbers

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

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

Challenge Number	Prize (\$US)	Status	Submission Date	Submitter
------------------	--------------	--------	-----------------	-----------

RSA-2048

Prize: \$200,000

Status: Not Factored

Decimal Digits: 617

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

密碼技術公司跟 質因子分解有何關係？

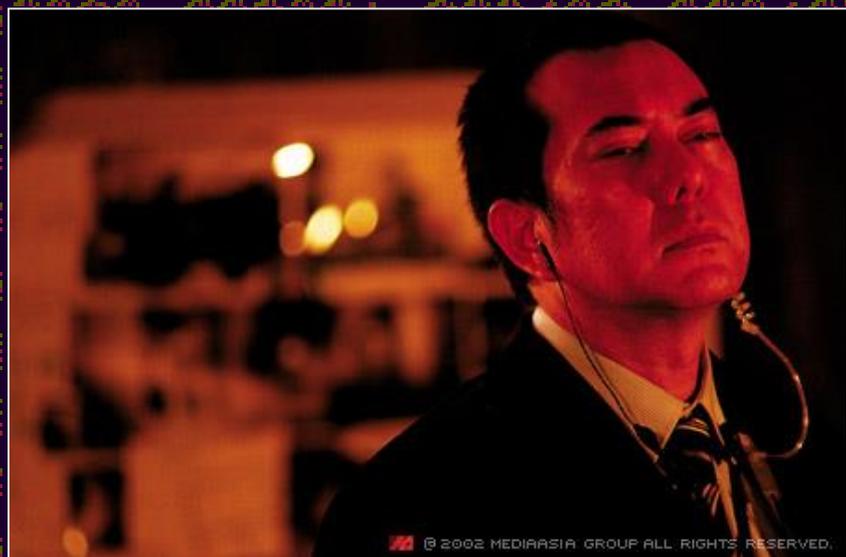


981613 981643 981657 981679 981687 981709 981717
981781 981787 981811 981819 981841 981861 981891
981931 981937 981963 981973 981993 981997 982009
982047 982053 982087 982099 982119 982137 982141
982227 982261 982277 982299 982319 982303 982311
982357 982369 982391 982417 982449 982471
982507 982521 982543 982579 982591 982597
982653 982659 982683 982677 982687 982719 982723
982771 982777 982799 982807 982821 982847 982849
982953 982963 982971 982979 982991 982997 983017
983079 983103 983101 983117 983121 983153 983179
983251 983257 983281 983299 983323 983337 983347
983391 983407 983407 983421 983443 983449 983451
983527 983541 983547 983553 983569 983587 983613
983677 983691 983701 983709 983751 983757 983761
983841 983871 983883 983899 983913 983919 983949
984027 984049 984059 984091 984103 984103 984107
984121 984147 984157 984161 984193 984201 984207
984263 984269 984287 984297 984303 984359
984483 984489 984499 984511 984513 984517 984523
984577 984601 984619 984627 984633 984637 984643

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



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



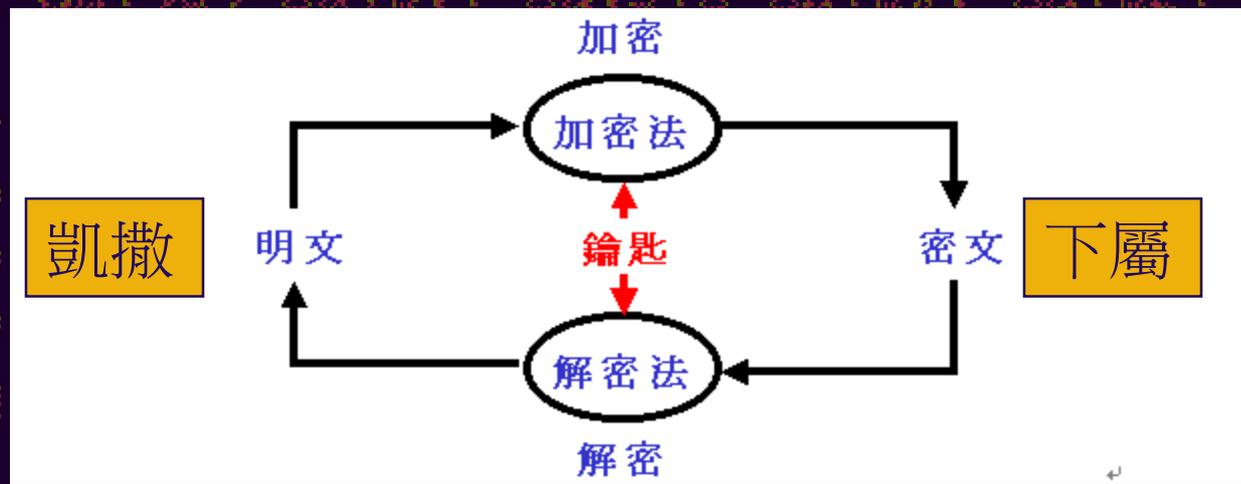
凱撒密碼 — 古老的加密法



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

$$\text{密碼} = (\text{明碼} + 3) \bmod 26$$

例：明碼 y [25]， $(25+3) \div 26$ 餘數是 2，
所以密碼是 b [2]



- ◆ 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

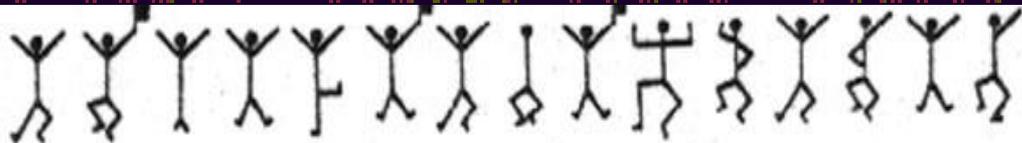
◆ 對比字母分佈，分析出密匙：

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

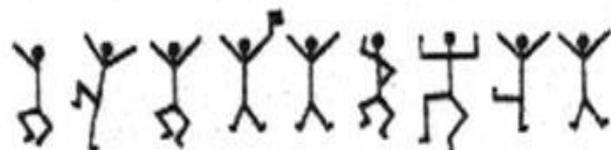
◆ 因此得出明碼：

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

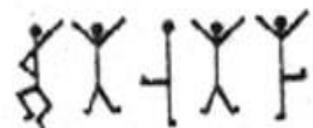
福爾摩斯探案『跳舞人形』



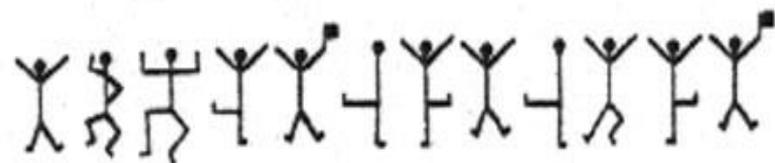
criminal's message (1)



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

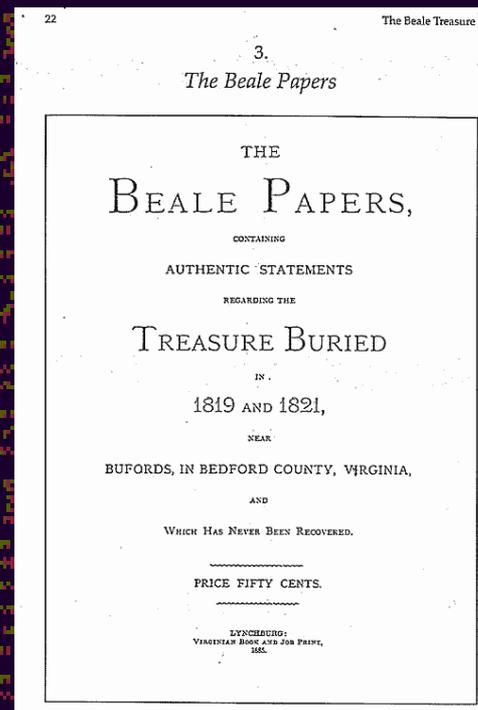
◆ 打敗『頻率分析法』

- 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。



•其中第二頁已給該書的作者解破。

•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，第二頁紙他的夥伴及親人的名單。

THE BEALE PAPERS. 21.

articles, belonging jointly to the parties whose names are given in number "8," 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, 1810. 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 \$19,000.

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, 124, 38, 1701, 89, 76, 11, 83, 1029, 48, 94, 63, 139, 16, 111, 85, 84, 841, 073, 14, 40, 64, 27, 81, 180, 219, 63, 90, 1120, 8, 15, 3, 120, 2018, 49, 74, 738, 485, 604, 230, 430, 664, 583, 150, 231, 284, 308, 231, 124, 211, 480, 229; 401, 370, 11, 101, 305, 139, 189, 37, 33, 88, 209, 193, 145, 1, 94, 73, 410, 918, 203, 23, 500, 533, 350, 17, 150, 219, 27, 170, 189, 10, 400, 23, 485, 18, 456, 65, 84, 200, 283, 118, 320, 138, 86, 410, 220, 15, 71, 224, 901, 44, 10, 401, 39, 88, 61, 304, 12, 21, 24, 283, 184, 92, 63, 246, 480, 682, 7, 219, 184, 300, 780, 18, 64, 468, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 102, 890, 62, 110, 67, 102, 893, 70, 60, 2317, 471, 840, 208, 121, 800, 348, 30, 150, 89, 365, 014, 19, 120, 63, 219, 812, 2100, 1780, 00, 83, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 193, 320, 37, 122, 113, 6, 140, 8, 150, 303, 42, 58, 461, 44, 106, 301, 13, 468, 680, 93, 86, 116, 330, 585, 508, 9, 102, 35, 416, 80, 71, 210, 728, 965, 818, 2, 83, 121, 105, 14, 300, 148, 284, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 25, 33, 10, 1101, 355, 93, 98, 181, 275, 346, 201, 206, 86, 30, 219, 824, 820, 84, 326, 10, 43, 122, 83, 216, 284, 919, 861, 826, 965, 233, 64, 68, 235, 431, 900, 50, 29, 81, 516, 521, 603, 14, 613, 81, 350, 36, 61, 62, 194, 78, 60, 300, 314, 676, 115, 4, 23, 18, 61, 139, 247, 819, 921, 1000, 464, 895, 10, 6, 60, 119, 38, 41, 49, 602, 423, 962, 303, 294, 873, 78, 14, 23, 111, 109, 63, 81, 501, 823, 216, 280, 34, 24, 150, 1000, 163, 288, 19, 21, 17, 340, 19, 242, 31, 80, 234, 140, 607, 115, 83, 191, 67, 104, 80, 52, 88, 15, 80, 121, 47, 23, 123, 216, 548, 63, 11, 211, 77, 304, 218, 65, 607, 890, 226, 154, 511, 10, 98, 34, 119, 26, 216, 119, 71, 218, 1164, 1406, 1817, 51, 30, 210, 36, 8, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 30, 261, 543, 807, 234, 18, 212, 416, 127, 501, 19, 4, 63, 96, 12, 101, 418, 10, 140, 230, 460, 348, 73, 57, 88, 618, 1431, 60, 710, 275, 74, 83, 11, 426, 89, 72, 84, 1200, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 123, 224, 403, 912, 227, 936, 447, 35, 86, 34, 43, 212, 107, 96, 314, 204, 1063, 232, 488, 601, 300, 124, 56, 216, 314, 2006, 154, 803, 3, 301, 113, 176, 219, 71, 87, 96, 202, 35, 10, 2, 41, 17, 24, 221, 736, 820, 214, 11, 60, 760.

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

20 THE BEALE PAPERS.

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, 78, 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, 808, 85, 59, 106, 196, 59, 211, 80, 9, 40, 816, 534, 123, 106, 05, 53, 58, 2, 42, 7, 35, 123, 53, 81, 82, 77, 230, 190, 66, 96, 118, 71, 140, 287, 23, 853, 37, 1003, 65, 147, 807, 24, 8, 2, 12, 47, 48, 85, 807, 45, 816, 191, 41, 78, 134, 1093, 132, 138, 131, 16, 77, 49, 102, 37, 72, 24, 78, 85, 83, 871, 56, 194, 81, 92, 191, 106, 273, 60, 394, 620, 270, 200, 300, 388, 287, 08, 8, 6, 191, 128, 48, 234, 406, 106, 299, 314, 47, 48, 81, 96, 26, 113, 62, 153, 181, 110, 77, 85, 107, 48, 10, 118, 140, 334, 48, 120, 100, 2, 007, 61, 420, 811, 29, 185, 14, 30, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 459, 287, 95, 117, 511, 62, 311, 220, 37, 118, 140, 807, 138, 540, 8, 44, 237, 888, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 608, 220, 7, 86, 154, 41, 29, 60, 6, 876, 123, 154, 248, 110, 61, 52, 53, 30, 5, 35, 8, 14, 84, 87, 540, 217, 115, 71, 29, 84, 63, 48, 131, 29, 138, 47, 73, 229, 540, 52, 53, 79, 118, 61, 44, 63, 109, 12, 289, 113, 8, 49, 79, 338, 105, 56, 371, 557, 211, 665, 125, 360, 133, 142, 101, 15, 284, 840, 232, 14, 203, 140, 344, 29, 811, 138, 115, 48, 73, 34, 205, 216, 607, 63, 220, 7, 783, 130, 54, 82, 10, 40, 87, 158, 807, 57, 121, 12, 95, 10, 15, 38, 12, 131, 62, 115, 109, 807, 40, 38, 158, 138, 30, 81, 62, 67, 41, 85, 63, 102, 106, 807, 133, 8, 113, 20, 32, 32, 37, 333, 287, 140, 47, 85, 50, 37, 49, 47, 64, 6, 7, 71, 34, 4, 43, 47, 62, 1, 2, 000, 305, 230, 15, 101, 246, 85, 84, 511, 2, 970, 20, 29, 7, 33, 44, 22, 40, 7, 110, 8, 511, 105, 44, 486, 230, 383, 211, 500, 31, 10, 85, 140, 207, 41, 603, 309, 202, 693, 247, 2, 44, 23, 32, 511, 548, 10, 6, 250, 527, 246, 53, 37, 52, 83, 47, 630, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 33, 106, 100, 113, 81, 102, 406, 230, 340, 330, 29, 60, 34, 101, 807, 313, 301, 316, 333, 820, 220, 37, 63, 38, 549, 230, 23, 8, 48, 107, 50, 811, 7, 2, 112, 73, 16, 125, 11, 110, 67, 102, 807, 39, 20, 81, 185, 28, 48, 531, 125, 10, 85, 600, 38, 42, 77, 14, 27, 8, 47, 138, 68, 140, 44, 2, 32, 177, 106, 250, 314, 21, 2, 10, 7, 1005, 4, 20, 25, 44, 48, 7, 36, 46, 110, 230, 807, 191, 34, 112, 117, 41, 910, 71, 253, 90, 41, 81, 50, 140, 36, 47, 162, 540, 63, 28, 28, 42, 250, 128, 622, 85, 643, 22, 107, 140, 119, 26, 85, 138, 240, 83, 20, 135, 271, 38, 36, 10, 52, 118, 106, 102, 430, 150, 112, 71, 14, 20, 7, 24, 18, 15, 807, 37, 67, 110, 62, 31, 21, 93, 230, 511, 102, 81, 30, 83, 84, 305, 620, 15, 2, 108, 220, 100, 339, 106, 106, 60, 375, 72, 3, 200, 183, 112, 133, 540, 65, 166, 807, 135, 96, 110, 16, 72, 37, 507, 129, 408, 499, 90, 174, 288, 86, 106, 816, 270, 205, 101, 811, 400, 8, 44, 3, 2, 49, 241, 34, 203, 38, 16, 46, 47, 83, 34, 14, 64, 73, 188, 807, 85, 78, 110, 32, 426, 505, 53, 27, 38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 133, 150, 96, 36, 24, 135, 807, 191, 56, 511, 118, 440, 270, 648, 403, 10, 41, 107, 603, 240, 255, 39, 103, 165, 46, 287, 293, 298, 134, 2, 13, 47, 83, 63, 138, 110, 21, 112, 140, 486, 486, 503, 14, 73, 84, 375, 1005, 150, 300, 16, 42, 5, 4, 23, 42, 8, 16, 811, 123, 160, 32, 205, 609, 807, 81, 95, 468, 41, 600, 136, 14, 20, 28, 36, 338, 203, 246, 8, 141, 160, 140, 84, 440, 42, 16, 811, 6, 67, 101, 102, 194, 198, 205, 31, 93, 241, 540, 122, 8, 10, 62, 140, 47, 48, 258.

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

22 THE BEALE PAPERS.

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.

217, 8, 92, 73, 118, 89, 67, 318, 28, 90, 107, 41, 631, 78, 146, 397, 113, 98, 184, 248, 348, 116, 74, 83, 15, 63, 32, 14, 81, 19, 76, 121, 216, 85, 23, 66, 15, 108, 68, 77, 43, 24, 123, 96, 117, 28, 311, 201, 19, 44, 11, 40, 59, 18, 196, 68, 817, 28, 80, 82, 304, 71, 43, 221, 108, 170, 310, 819, 81, 99, 264, 880, 56, 37, 819, 2, 44, 82, 28, 44, 75, 98, 103, 37, 85, 107, 117, 64, 88, 130, 49, 154, 90, 173, 89, 315, 326, 78, 96, 214, 216, 31, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 540, 84, 570, 88, 116, 32, 59, 74, 68, 69, 240, 15, 8, 121, 29, 77, 80, 31, 11, 104, 81, 101, 234, 828, 18, 75, 63, 63, 117, 201, 39, 33, 217, 27, 21, 84, 85, 54, 109, 128, 49, 77, 89, 1, 81, 317, 64, 55, 88, 116, 237, 260, 311, 96, 54, 33, 120, 18, 182, 102, 219, 311, 84, 150, 318, 275, 312, 64, 70, 100, 87, 76, 47, 21, 22, 87, 81, 44, 18, 156, 115, 133, 160, 181, 203, 78, 81, 229, 314, 337, 351, 68, 11, 28, 97, 318, 238, 106, 24, 98, 3, 19, 17, 26, 60, 73, 88, 14, 136, 138, 234, 286, 297, 331, 365, 364, 10, 22, 84, 56, 107, 68, 123, 111, 214, 180, 7, 33, 45, 40, 13, 23, 48, 49, 107, 150, 227, 844, 198, 203, 247, 110, 19, 8, 212, 230, 31, 6, 328, 63, 48, 52, 59, 41, 122, 83, 117, 11, 13, 25, 71, 30, 45, 83, 76, 89, 92, 81, 63, 79, 88, 96, 27, 33, 44, 60, 61, 24, 112, 136, 149, 176, 180, 194, 143, 171, 203, 208, 87, 12, 44, 51, 89, 98, 84, 41, 208, 173, 66, 9, 83, 16, 65, 8, 113, 175, 90, 66, 203, 19, 177, 188, 200, 157, 200, 216, 206, 201, 206, 618, 631, 330, 19, 124, 78, 65, 19, 33, 124, 48, 83, 57, 34, 96, 207, 244, 60, 89, 119, 71, 11, 86, 97, 215, 54, 82, 316, 245, 303, 80, 97, 106, 212, 18, 37, 1, 81, 89, 16, 65, 8, 113, 175, 90, 66, 216, 118, 29, 85, 106, 96, 176, 212, 84, 6, 237, 304, 611, 231, 364, 814, 875, 123, 200, 1, 18, 53, 76, 10, 15, 23, 19, 71, 84, 120, 184, 69, 73, 80, 56, 220, 48, 77, 26, 101, 127, 98, 218, 439, 173, 171, 61, 225, 313, 215, 102, 18, 167, 202, 114, 218, 66, 59, 48, 27, 19, 13, 82, 43, 163, 110, 34, 127, 139, 24, 128, 129, 74, 63, 150, 11, 34, 61, 73, 62, 180, 66, 79, 104, 265, 89, 96, 128, 274, 806, 917, 434, 461, 235, 800, 512, 412, 823, 391, 60, 105, 217, 69, 118, 22, 77, 64, 42, 12, 7, 53, 24, 83, 67, 97, 109, 123, 135, 181, 203, 212, 228, 250, 21, 34, 77, 810, 374, 382, 675, 694, 717, 864, 203, 4, 18, 92, 16, 16, 83, 82, 40, 55, 69, 74, 112, 131, 184, 186, 173, 119, 213, 416, 312, 843, 204, 119, 168, 82, 243, 417, 845, 951, 124, 269, 49, 617, 856, 894, 899, 73, 10, 23, 11, 23, 45, 40, 66, 83, 94, 112, 65, 82, 115, 119, 233, 244, 186, 172, 112, 85, 6, 56, 38, 44, 83, 72, 92, 47, 63, 96, 124, 217, 214, 319, 221, 644, 817, 821, 834, 922, 416, 675, 10, 22, 13, 46, 167, 181, 101, 39, 86, 109, 116, 153, 164, 212, 218, 206, 815, 380, 412, 400, 403, 675, 820, 852.

The papers given in the above were to this that they 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
GROUNDTHE 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

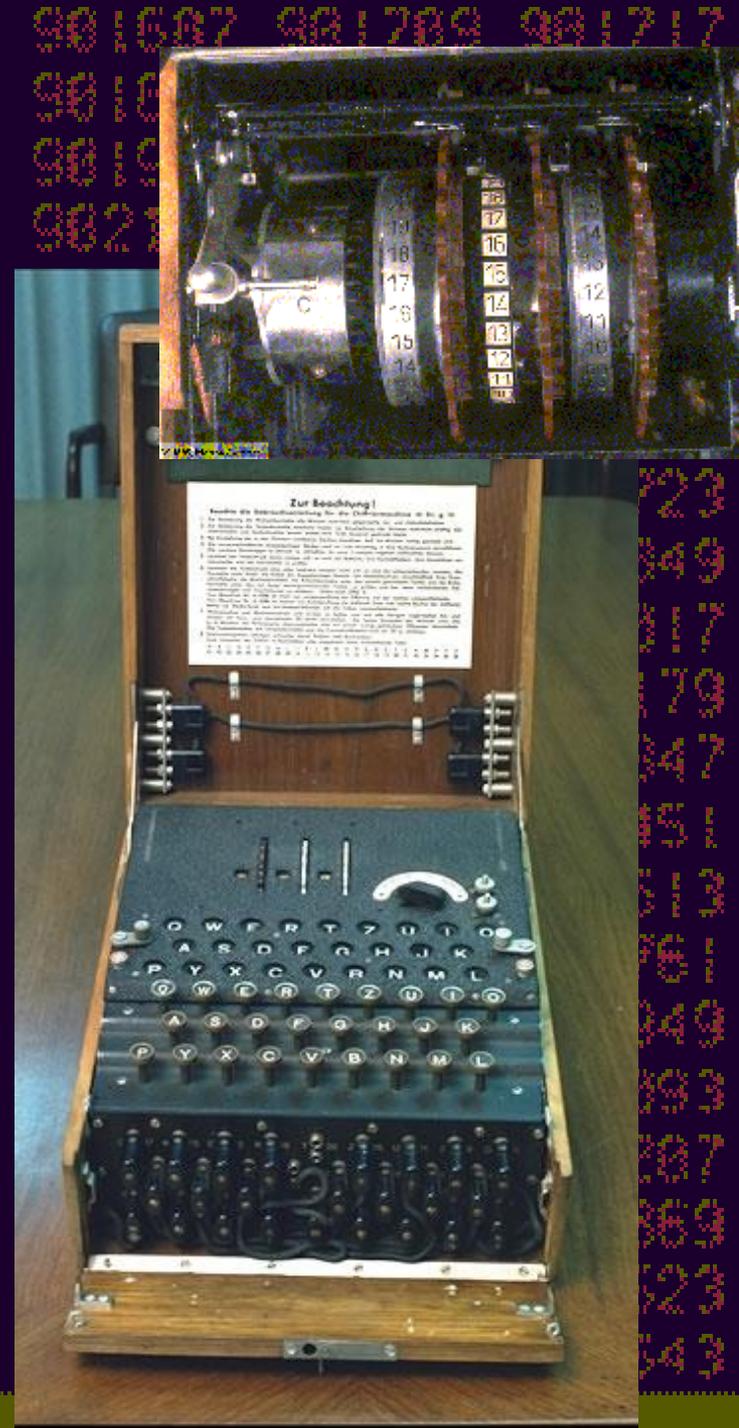
- ◆ 第一次世界大戰時，美國研究員發明單次密匙簿加密法，每次加密的密匙都不同。
- ◆ 明文：THE BRITISH HAVE FIFTY TANKS
- ◆ 密匙：SHE LOVES HIM SO VERY MUCH NOW

	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。

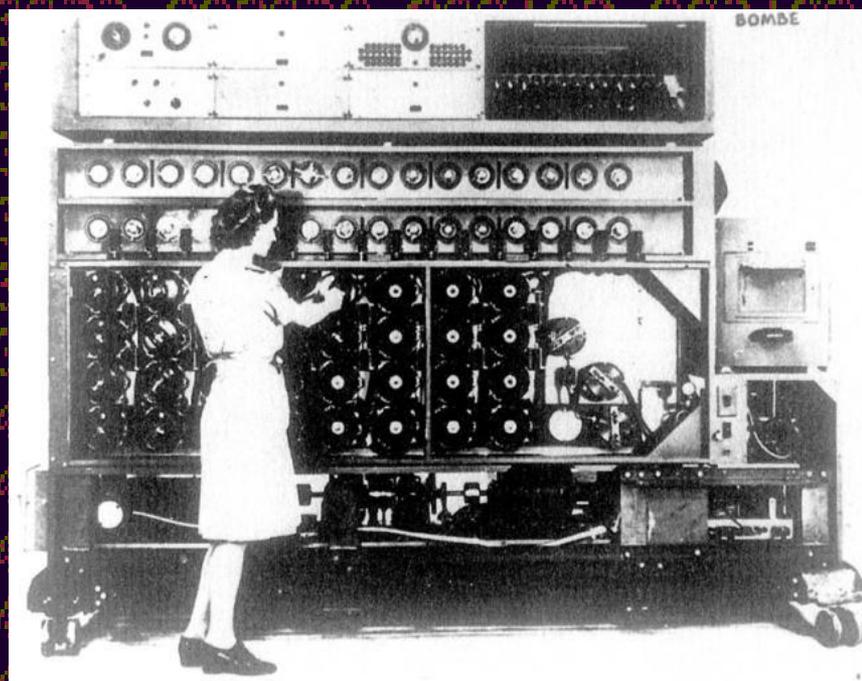
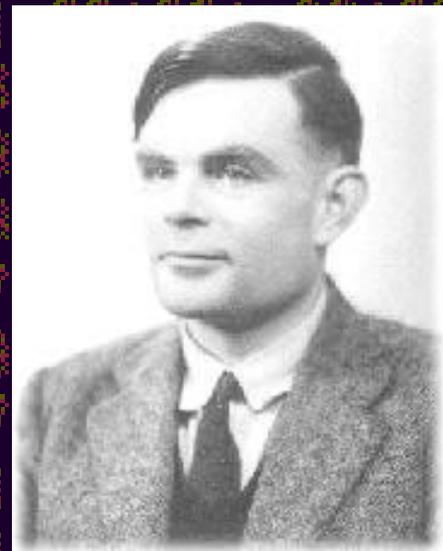
➤ 第一次世界大戰後，德國人發明了密碼機器『奇謎』(Enigma)。

➤ 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

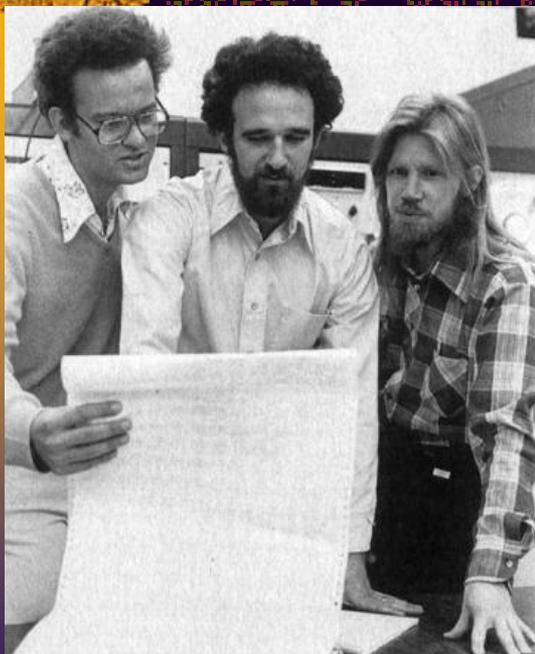
- 互聯網的出現，大量訊息需要加密傳送，傳送密匙更做成很大困難。
- 公開密匙系統是廿世紀密碼學的最偉大成就

❖ 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



Alice

$$S(y) = x$$

$$P(x) = y$$



y



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 $x = (y - 1) / 2 = S(y)$

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 演算法 (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

$$ed \bmod z = 1$$

➤ 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 $ed \bmod z = 1$ 而 $z = (p-1)(q-1)$ ，所以只要出 p 和 q ，便可找出 d 。
- $n = p \times q$ 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 $n = p \times q$ 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。

$n = 114381625757888867669235779976146$
61201021829672124236256256184293
57069352457338978305971235639587
05058989075147599290026879543541

$p = 34905295108476509491478496199038$
98133417764638493387843990820577
 $q = 327691329932667095499619881908344$
61413177642967992942539798288533



網址(D) <http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html>

連結 [Favourite](#) [Hotmail的免費電子郵件](#) [intranet.slc](#) [Yahoo! Hong Kong - 雅虎香港](#) [新浪網 - 香港站](#) [NIKE新浪技暴](#)

More About

Factoring Challenge

The RSA Challenge Numbers

[Factoring Challenge FAQ](#)

[Submit a Factorization](#)

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			
RSA-704	\$30,000			
RSA-768	\$50,000			
RSA-896	\$75,000			
RSA-1024	\$100,000			
RSA-1536	\$150,000			

RSA-640

Prize: \$20,000

Status: **Not Factored**

Decimal Digits: 193

[3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609](#)

RSA-2048

Prize: \$200,000

Status: **Not Factored**

Decimal Digits: 617

[2519590847565789349402718324004839857142928212620403202777713783604366202070759556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357](#)

➤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。



981613 981643 981657 981679 981687 981709 981717
981781 981787 981811 981819 981841 981861 981891
981931 981937 981963 981973 981993 981997 982009
982047 982053 982087 982089 982119 982137 982141
982227 982261 982263 982281 982293 982303 982311
982357 982369 982401 982413 982437 982449 982471
982507 982521 982559 982579 982581 982597
982653 982691 982727 982747 982719 982723
982749 982751 982787 982807 982811 982849
982871 982877 982911 982917
983041 983045 983046 983071 983079
983111 983125 983131 983133 983135 983137 983147
983251 983253 983255 983257 983259 983261 983263 983265 983267 983269 983271 983273 983275 983277 983279 983281 983283 983285 983287 983289 983291 983293 983295 983297 983299 983301 983303 983305 983307 983309 983311 983313 983315 983317 983319 983321 983323 983325 983327 983329 983331 983333 983335 983337 983339 983341 983343 983345 983347 983349 983351 983353 983355 983357 983359 983361 983363 983365 983367 983369 983371 983373 983375 983377 983379 983381 983383 983385 983387 983389 983391 983393 983395 983397 983399 983401 983403 983405 983407 983409 983411 983413 983415 983417 983419 983421 983423 983425 983427 983429 983431 983433 983435 983437 983439 983441 983443 983445 983447 983449 983451 983453 983455 983457 983459 983461 983463 983465 983467 983469 983471 983473 983475 983477 983479 983481 983483 983485 983487 983489 983491 983493 983495 983497 983499 983501 983503 983505 983507 983509 983511 983513 983515 983517 983519 983521 983523 983525 983527 983529 983531 983533 983535 983537 983539 983541 983543 983545 983547 983549 983551 983553 983555 983557 983559 983561 983563 983565 983567 983569 983571 983573 983575 983577 983579 983581 983583 983585 983587 983589 983591 983593 983595 983597 983599 983601 983603 983605 983607 983609 983611 983613 983615 983617 983619 983621 983623 983625 983627 983629 983631 983633 983635 983637 983639 983641 983643 983645 983647 983649 983651 983653 983655 983657 983659 983661 983663 983665 983667 983669 983671 983673 983675 983677 983679 983681 983683 983685 983687 983689 983691 983693 983695 983697 983699 983701 983703 983705 983707 983709 983711 983713 983715 983717 983719 983721 983723 983725 983727 983729 983731 983733 983735 983737 983739 983741 983743 983745 983747 983749 983751 983753 983755 983757 983759 983761 983763 983765 983767 983769 983771 983773 983775 983777 983779 983781 983783 983785 983787 983789 983791 983793 983795 983797 983799 983801 983803 983805 983807 983809 983811 983813 983815 983817 983819 983821 983823 983825 983827 983829 983831 983833 983835 983837 983839 983841 983843 983845 983847 983849 983851 983853 983855 983857 983859 983861 983863 983865 983867 983869 983871 983873 983875 983877 983879 983881 983883 983885 983887 983889 983891 983893 983895 983897 983899 983901 983903 983905 983907 983909 983911 983913 983915 983917 983919 983921 983923 983925 983927 983929 983931 983933 983935 983937 983939 983941 983943 983945 983947 983949 983951 983953 983955 983957 983959 983961 983963 983965 983967 983969 983971 983973 983975 983977 983979 983981 983983 983985 983987 983989 983991 983993 983995 983997 983999 984001 984003 984005 984007 984009 984011 984013 984015 984017 984019 984021 984023 984025 984027 984029 984031 984033 984035 984037 984039 984041 984043 984045 984047 984049 984051 984053 984055 984057 984059 984061 984063 984065 984067 984069 984071 984073 984075 984077 984079 984081 984083 984085 984087 984089 984091 984093 984095 984097 984099 984101 984103 984105 984107 984109 984111 984113 984115 984117 984119 984121 984123 984125 984127 984129 984131 984133 984135 984137 984139 984141 984143 984145 984147 984149 984151 984153 984155 984157 984159 984161 984163 984165 984167 984169 984171 984173 984175 984177 984179 984181 984183 984185 984187 984189 984191 984193 984195 984197 984199 984201 984203 984205 984207 984209 984211 984213 984215 984217 984219 984221 984223 984225 984227 984229 984231 984233 984235 984237 984239 984241 984243 984245 984247 984249 984251 984253 984255 984257 984259 984261 984263 984265 984267 984269 984271 984273 984275 984277 984279 984281 984283 984285 984287 984289 984291 984293 984295 984297 984299 984301 984303 984305 984307 984309 984311 984313 984315 984317 984319 984321 984323 984325 984327 984329 984331 984333 984335 984337 984339 984341 984343 984345 984347 984349 984351 984353 984355 984357 984359 984361 984363 984365 984367 984369 984371 984373 984375 984377 984379 984381 984383 984385 984387 984389 984391 984393 984395 984397 984399 984401 984403 984405 984407 984409 984411 984413 984415 984417 984419 984421 984423 984425 984427 984429 984431 984433 984435 984437 984439 984441 984443 984445 984447 984449 984451 984453 984455 984457 984459 984461 984463 984465 984467 984469 984471 984473 984475 984477 984479 984481 984483 984485 984487 984489 984491 984493 984495 984497 984499 984501 984503 984505 984507 984509 984511 984513 984515 984517 984519 984521 984523 984525 984527 984529 984531 984533 984535 984537 984539 984541 984543 984545 984547 984549 984551 984553 984555 984557 984559 984561 984563 984565 984567 984569 984571 984573 984575 984577 984579 984581 984583 984585 984587 984589 984591 984593 984595 984597 984599 984601 984603 984605 984607 984609 984611 984613 984615 984617 984619 984621 984623 984625 984627 984629 984631 984633 984635 984637 984639 984641 984643 984645 984647 984649 984651 984653 984655 984657 984659 984661 984663 984665 984667 984669 984671 984673 984675 984677 984679 984681 984683 984685 984687 984689 984691 984693 984695 984697 984699 984701 984703 984705 984707 984709 984711 984713 984715 984717 984719 984721 984723 984725 984727 984729 984731 984733 984735 984737 984739 984741 984743 984745 984747 984749 984751 984753 984755 984757 984759 984761 984763 984765 984767 984769 984771 984773 984775 984777 984779 984781 984783 984785 984787 984789 984791 984793 984795 984797 984799 984801 984803 984805 984807 984809 984811 984813 984815 984817 984819 984821 984823 984825 984827 984829 984831 984833 984835 984837 984839 984841 984843 984845 984847 984849 984851 984853 984855 984857 984859 984861 984863 984865 984867 984869 984871 984873 984875 984877 984879 984881 984883 984885 984887 984889 984891 984893 984895 984897 984899 984901 984903 984905 984907 984909 984911 984913 984915 984917 984919 984921 984923 984925 984927 984929 984931 984933 984935 984937 984939 984941 984943 984945 984947 984949 984951 984953 984955 984957 984959 984961 984963 984965 984967 984969 984971 984973 984975 984977 984979 984981 984983 984985 984987 984989 984991 984993 984995 984997 984999 985001 985003 985005 985007 985009 985011 985013 985015 985017 985019 985021 985023 985025 985027 985029 985031 985033 985035 985037 985039 985041 985043 985045 985047 985049 985051 985053 985055 985057 985059 985061 985063 985065 985067 985069 985071 985073 985075 985077 985079 985081 985083 985085 985087 985089 985091 985093 985095 985097 985099 985101 985103 985105 985107 985109 985111 985113 985115 985117 985119 985121 985123 985125 985127 985129 985131 985133 985135 985137 985139 985141 985143 985145 985147 985149 985151 985153 985155 985157 985159 985161 985163 985165 985167 985169 985171 985173 985175 985177 985179 985181 985183 985185 985187 985189 985191 985193 985195 985197 985199 985201 985203 985205 985207 985209 985211 985213 985215 985217 985219 985221 985223 985225 985227 985229 985231 985233 985235 985237 985239 985241 985243 985245 985247 985249 985251 985253 985255 985257 985259 985261 985263 985265 985267 985269 985271 985273 985275 985277 985279 985281 985283 985285 985287 985289 985291 985293 985295 985297 985299 985301 985303 985305 985307 985309 985311 985313 985315 985317 985319 985321 985323 985325 985327 985329 985331 985333 985335 985337 985339 985341 985343 985345 985347 985349 985351 985353 985355 985357 985359 985361 985363 985365 985367 985369 985371 985373 985375 985377 985379 985381 985383 985385 985387 985389 985391 985393 985395 985397 985399 985401 985403 985405 985407 985409 985411 985413 985415 985417 985419 985421 985423 985425 985427 985429 985431 985433 985435 985437 985439 985441 985443 985445 985447 985449 985451 985453 985455 985457 985459 985461 985463 985465 985467 985469 985471 985473 985475 985477 985479 985481 985483 985485 985487 985489 985491 985493 985495 985497 985499 985501 985503 985505 985507 985509 985511 985513 985515 985517 985519 985521 985523 985525 985527 985529 985531 985533 985535 985537 985539 985541 985543 985545 985547 985549 985551 985553 985555 985557 985559 985561 985563 985565 985567 985569 985571 985573 985575 985577 985579 985581 985583 985585 985587 985589 985591 985593 985595 985597 985599 985601 985603 985605 985607 985609 985611 985613 985615 985617 985619 985621 985623 985625 985627 985629 985631 985633 985635 985637 985639 985641 985643 985645 985647 985649 985651 985653 985655 985657 985659 985661 985663 985665 985667 985669 985671 985673 985675 985677 985679 985681 985683 985685 985687 985689 985691 985693 985695 985697 985699 985701 985703 985705 985707 985709 985711 985713 985715 985717 985719 985721 985723 985725 985727 985729 985731 985733 985735 985737 985739 985741 985743 985745 985747 985749 985751 985753 985755 985757 985759 985761 985763 985765 985767 985769 985771 985773 985775 985777 985779 985781 985783 985785 985787 985789 985791 985793 985795 985797 985799 985801 985803 985805 985807 985809 985811 985813 985815 985817 985819 985821 985823 985825 985827 985829 985831 985833 985835 985837 985839 985841 985843 985845 985847 985849 985851 985853 985855 985857 985859 985861 985863 985865 985867 985869 985871 985873 985875 985877 985879 985881 985883 985885 985887 985889 985891 985893 985895 985897 985899 985901 985903 985905 985907 985909 985911 985913 985915 985917 985919 985921 985923 985925 985927 985929 985931 985933 985935 985937 985939 985941 985943 985945 985947 985949 985951 985953 985955 985957 985959 985961 985963 985965 985967 985969 985971 985973 985975 985977 985979 985981 985983 985985 985987 985989 985991 985993 985995 985997 985999 986001 986003 986005 986007 986009 986011 986013 986015 986017 986019 986021 986023 986025 986027 986029 986031 986033 986035 986037 986039 986041 986043 986045 986047 986049 986051 986053 986055 986057 986059 986061 986063 986065 986067 986069 986071 986073 986075 986077 986079 986081 986083 986085 986087 986089 986091 986093 986095 986097 986099 986101 986103 986105 986107 986109 986111 986113 986115 986117 986119 986121 986123 986125 986127 986129 986131 986133 986135 986137 986139 986141 986143 986145 986147 986149 986151 986153 986155 986157 986159 986161 986163 986165 986167 986169 986171 986173 986175 986177 986179 986181 986183 986185 986187 986189 986191 986193 986195 986197 986199 986201 986203 986205 986207 986209 986211 986213 986215 986217 986219 986221 986223 986225 986227 986229 986231 986233 986235 986237 986239 986241 986243 986245 986247 986249 986251 986253 986255 986257 986259 986261 986263 986265 986267 986269 986271 986273 986275 986277 986279 986281 986283 986285 986287 986289 986291 986293 986295 986297 986299 986301 986303 986305 986307 986309 986311 986313 986315 986317 986319 986321 986323 986325 986327 986329 986331 986333 986335 986337 986339 986341 986343 986345 986347 986349 986351 986353 986355 986357 986359 986361 986363 986365 986367 986369 986371 986373 986375 986377 986379 986381 986383 986385 986387 986389 986391 986393 986395 986397 986399 986401 986403 986405 986407 986409 986411 986413 986415 986417 986419 986421 986423 986425 986427 986429 986431 986433 986435 986437 986439 986441 986443 986445 986447 986449 986451 986453 986455 986457 986459 986461 986463 986465 986467 986469 986471 986473 986475 986477 986479 986481 986483 986485 986487 986489 986491 986493 986495 986497 986499 986501 986503 986505 986507 986509 986511 986513 986515 986517 986519 986521 986523 986525 986527 986529 986531 986533 986535 986537 986539 986541 986543 986545 986547 986549 986551 986553 986555 986557 986559 986561 986563 986565 986567 986569 986571 986573 986575 986577 986579 986581 986583 986585 986587 986589 986591 986593 986595 986597 986599 9

◆ 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。



You are in: **Sci/Tech**
Wednesday, 5 December, 2001, 11:42 GMT

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

Number takes prime position

THE WORLD'S LARGEST PRIME NUMBER



- 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

BBC SPORT

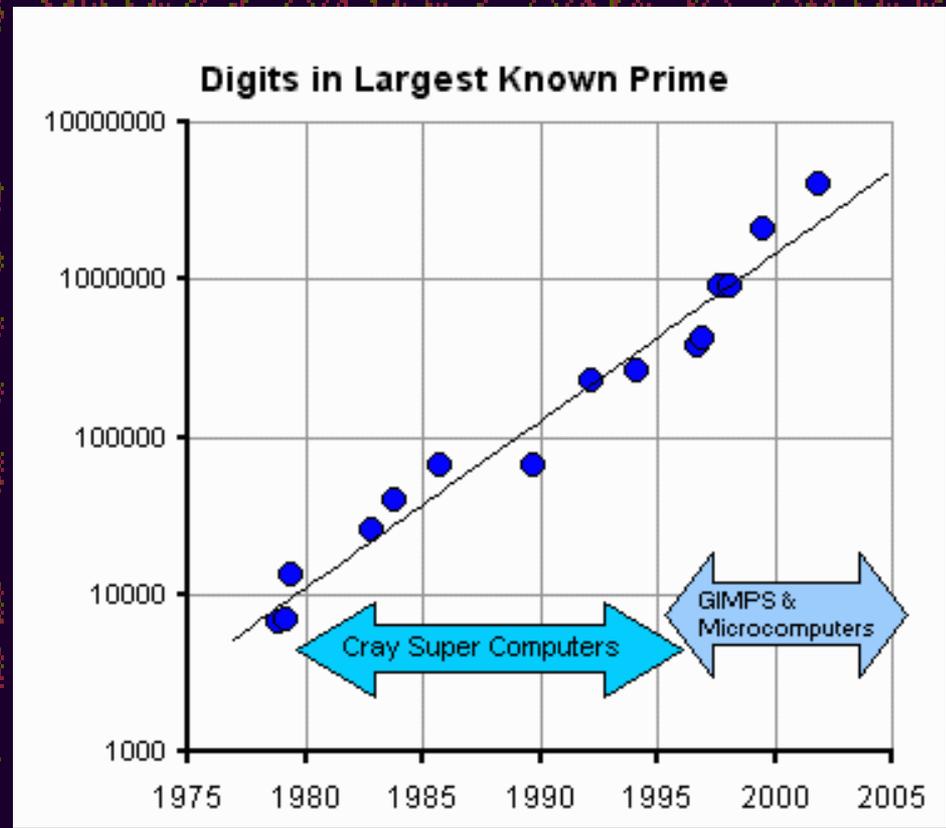
BBC Weather

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。

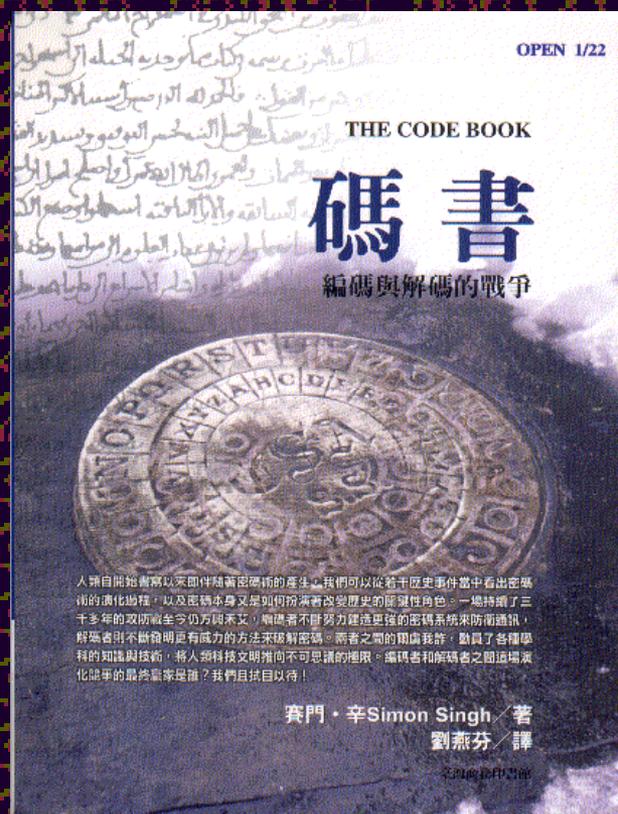
1789 981717
1061 981891
1987 982009
2137 982141
2303 982311
2449 982471
2581 982587
2719 982723
2827 982849
2987 983017



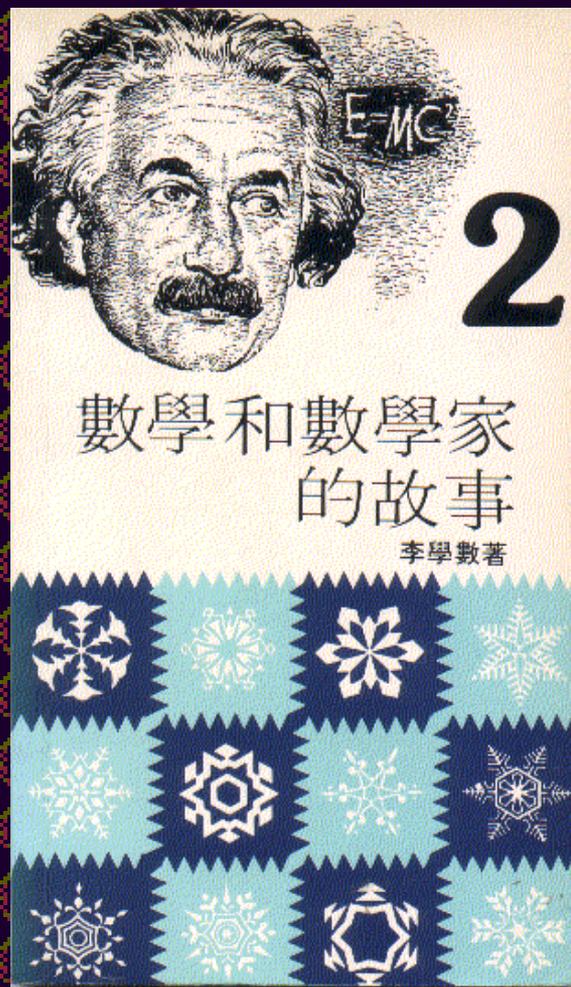
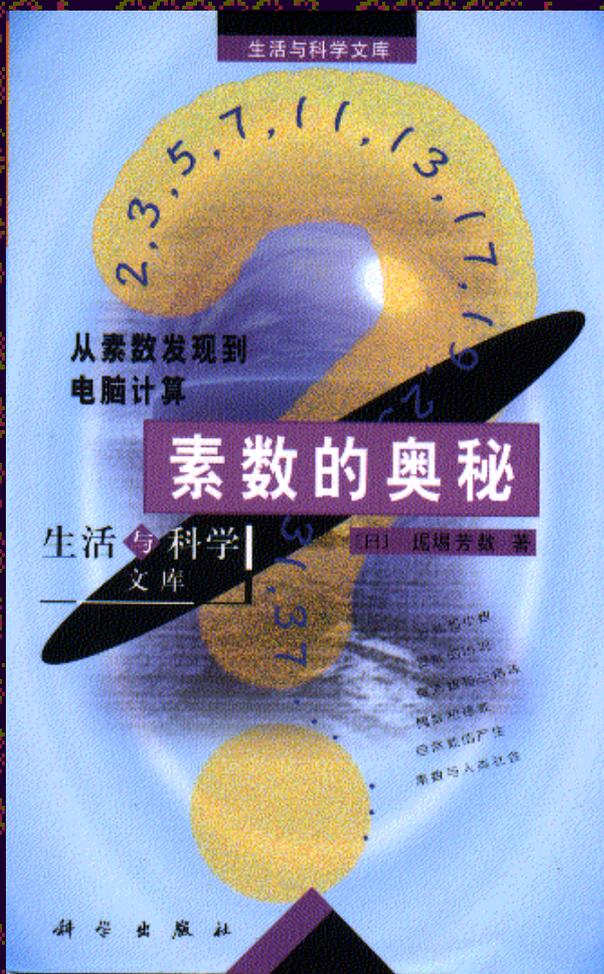
GIMPS :

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



有關質數的書





981613 981643 981657 981679 981687 981789 981717
981781 981787 981811 981819 981841 981861 981891
981931 981937 981963 981973 981993 981997 982009
982047 982053 982087 982089 982119 982137 982141
982227 982261 982263 982281 982293 982303 982311
982357 982369 982401 982413 982437 982449 982471
982507 982521 982569 982569 982579 982581 982597
982653 982659 982669 982677 982687 982719 982723
982771 982777 982807 982821 982827 982849
982953 982963 982971 982977 982981 982983 983017
983079 983083 983103 983143 983151 983163 983179
983251 983257 983289 983311 983339 983347 983347
983351 983403 983403 983421 983443 983449 983451
983527 983541 983547 983563 983569 983580 983613
983677 983691 983701 983709 983731 983735 983761
983841 983871 983887 983899 983913 983915 983949
984027 984049 984067 984069 984073 984087 984093
984121 984147 984157 984181 984193 984201 984207
984283 984289 984297 984303 984357 984361 984369
984483 984489 984499 984511 984513 984517 984523
984577 984601 984619 984627 984633 984637 984643

再會