あま　けいさん　わ
余り　計算　で 分かる

えいが　あんごう
映画『サマーウォーズ』の 暗号

オズの かんりセンターの にんしょうパスワード

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

６４÷３３＝１あまり３１

１６÷３３＝０あまり１６

６４÷３３⇒３１

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2 ÷ 3 3 ⇒ 2

2 × 2 ÷ 3 3 ⇒ 4

2 × 2 × 2 ÷ 3 3 ⇒ 8

2 × 2 × 2 × 2 ÷ 3 3 ⇒ 1 6

2 × 2 × 2 × 2 × 2 ÷ 3 3 ⇒ 3 2

2 × 2 × 2 × 2 × 2 × 2 ÷ 3 3 ⇒ 3 1

2 × 2 × 2 × 2 × 2 × 2 × 2 ÷ 3 3 ⇒ 2 9

2 を 7 つかけて ÷ 3 3 ⇒ 2 9

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2を　8つ かけて÷3 3⇒2 5

2を　9つ かけて÷3 3⇒1 7

2を10こ かけて÷3 3⇒　1

2を11こ かけて÷3 3⇒　2

2を12こ かけて÷3 3⇒　4

：

2を21こ かけて÷3 3⇒　2

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

何回もかけて ３３でわった あまり

数 \ かけた こ数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13	4
14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14	31
15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17	25
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18	27
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19	31
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

２１こ かけると

2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2÷３３⇒2

８ × ８ × ８ × ８ × ８ × ８ × ８ ÷３３⇒2

３つ かけた８は、さらに７つ かければ元の２にもどる

８があるとき、７を知っている人だけが元にもどせる

アールエスエー

ＲＳＡあんごう （ ⇔ ３３が、２つの数をかけた数）

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2
こ数 3
÷33
⇒ 8
こ数 7
÷33
⇒ 2

アール エス エー あん ごう

R S A 暗 号

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

マーチン・ガードナー

１９７７年
サイエンティフィック アメリカン

（参考:日本語版の「日経サイエンス」の最近のものは本校図書館にも所蔵あり。）

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2	？　（空白→00、A→01、B→02、C→03、…、Z→26）
こ数 3	9007
÷33	1143816257578888676692357799761466120102182967212423625625618429357 0693524573389783059712356395870505898907514759929002687954354 1
⇒　8	9686961375462206147714092225435588290575999112457431987469512093081 6298225145708356931476622883989628013391990551829945157815154
こ数 7	？
÷33	1143816257578888676692357799761466120102182967212423625625618429357 0693524573389783059712356395870505898907514759929002687954354 1
⇒　2	？

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

？
こ数３
÷33
⇒　8
こ数？
÷33
⇒　？

⇒　もし　３３が　３×11　だとわかると

３と３と11で　あるほうほうをつかって、

（かくちょうユークリッドのごじょほう）

すぐ７が計算でき、かい読

```
display2d: false;

e: 3 $
p: 3 $
q: 11 $

C: 8 $

yu(a1, a2):=block([a3],
  while 0<a2[3] do ( a3:a1-quotient(a1[3], a2[3])*a2, a1:a2, a2:a3 ),  a1[2]) $
d:yu([1, 0, (p-1)*(q-1)], [0, 1, e]) $
while 0>d do d:d+(p-1)*(q-1) $ "Kaisuu " ; d ;

ka(a,b,n):=block([r:1, m],
  while 1<=b do block( [b,m]:divide(b, 2),
    if m=1 then r:mod(r*a,n),  a:mod(a^2, n)  ),  r) $
"Kaidoku Kekka" ;ka(C, d, p*q) ;



(%o1) false
(%o9) "Kaisuu "
(%o10) 7

(%o12) "Kaidoku Kekka"
(%o13) 2
```

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

アトキンスらが、ネット上でよびかけて、

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

のもとになった２つの数

3490529510847650949147849619903898133417764638493387843990820577

と

32769132993266709549961988190834461413177642967992942539798288533

をもとめた。

（おおよそ20か国、600人、1600台のｺﾝﾋﾟｭｰﾀ、８か月）

9007とこれらをつかって、かい読。1994年にはっぴょう。

```
e: 9007 $
p: 34905295108476509491478496199038981334177646384933878439908205 77 $
q: 32769132993266709549961988190834461413177642967992942539798288533 $

C: 96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154 $

yu(a1, a2):=block([a3],
  while 0<a2[3] do ( a3:a1-quotient(a1[3], a2[3])*a2, a1:a2, a2:a3 ),  a1[2]) $
d:yu([1, 0, (p-1)*(q-1)], [0, 1, e]) $
while 0>d do d:d+(p-1)*(q-1) $ "Kaisuu " ; d ;

ka(a,b,n):=block([r:1, m],
  while 1<=b do block( [b,m]:divide(b, 2),
    if m=1 then r:mod(r*a,n),  a:mod(a^2, n)  ),  r) $
"Kaidoku Kekka" ;ka(C, d, p*q) ;



(%o21) "Kaisuu "
(%o22)
1066986143685780244428687713289201547807099066339378628012262244966310631259117744708733401685974623065539685445132771090536060 95

(%o24) "Kaidoku Kekka"
(%o25) 2008050013010709030023151804190001180500191721050113091908001519190906180107 05
```

参考　富岳(ふがく)は、日本のコンピュータで、現在世界最速。

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2	？　（空白→00、A→01、B→02、C→03、…、Z→26）
こ数 3	9007
÷33	1143816257578888676692357799761466120102182967212423625625618429357 0693524573389783059712356395870505898907514759929002687954354 1
⇒　8	9686961375462206147714092225435588290575999112457431987469512093081 6298225145708356931476622883989628013391990551829945157815154
こ数 7	1066986143685780244428687713289201547807099066339378628012262244966 3106312591177447087334016859746230655396854451327710905360609 5
÷33	1143816257578888676692357799761466120102182967212423625625618429357 0693524573389783059712356395870505898907514759929002687954354 1
⇒　2	2008050013010709030023151804190001180500191721050113091908001519190906180107 05

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2008050013010709030023151804190001180500191721050113091908001519190906180107O5

もともと、クイズでは

空白→00、A→01、B→02、C→03、D→04、E→05、
F→06、G→07、H→08、I→09、J→10、K→11、L→12、
M→13、N→14、O→15、P→16、Q→17、R→18、S→19、
T→20、U→21、V→22、W→23、X→24、Y→25、Z→26、

ということだったので

20、08、05、00、…、05 は

⇒THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2	？　（空白→00、A→01、B→02、C→03、…、Z→26）
こ数 3	9007
÷33	1143816257578888676692357799761466120102182967212423625625618429357069352457338978305971235639587050589890751475992900268795435 41
⇒　8	9686961375462206147714092225435588290575999112457431987469512093081629822514570835693147662288398962801339199055182994515781515 4
こ数 7	？
÷33	1143816257578888676692357799761466120102182967212423625625618429357069352457338978305971235639587050589890751475992900268795435 41
⇒　2	？

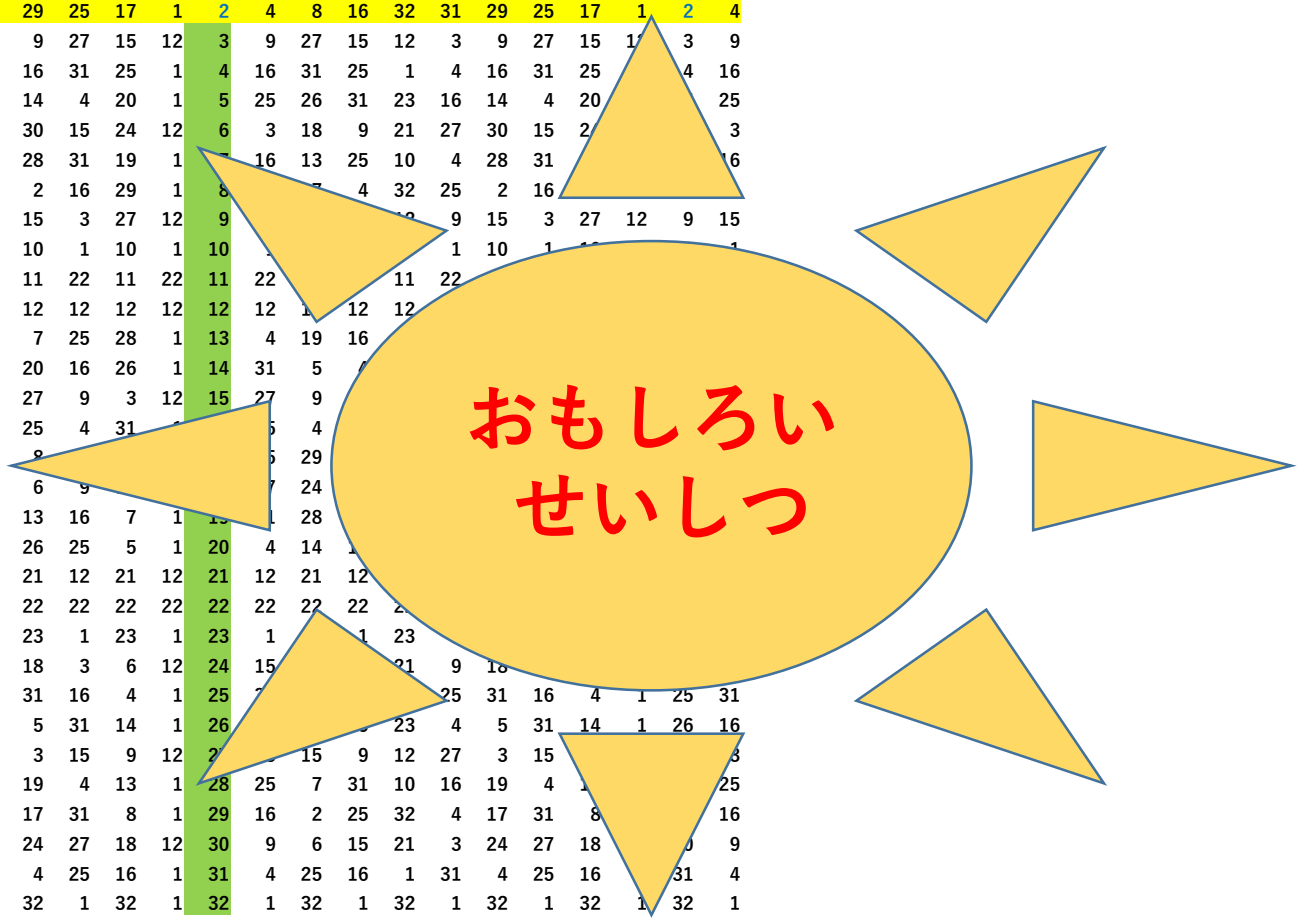
２０５６けた

The magic words are squeamish ossifrage …

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

何回もかけて ３３でわった あまり

数 \ かけた こ数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	1	3	9
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25		4	16
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20			25
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	2			3
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1		16	13	25	10	4	28	31				16
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1				4	32	25	2	16				
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9					9	15	3	27	12	9	15
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10					1	10	1				
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22			11	22						
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12		1	12	12						
13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13	4	19	16								
14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14	31	5									
15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9									
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31			5	4									
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16						5	29									
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6					7	24									
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1		1	28									
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14									
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12								
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	2							
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1		1	23							
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15			21	9	18					
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25					25	31	16	4	1	25	31
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26				23	4	5	31	14	1	26	16
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	2		15	9	12	27	3	15				3
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	1			25
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8			16
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18		0	9
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16		31	4
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1



あまり せいしつ あんごうへ クイズ かんたんく えいがで おまけ

キモ

２１こ かけると

2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2÷３３⇒2

８ × ８ × ８ × ８ × ８ × ８ × ８ ÷３３⇒2

３こ かけた８なら、７こ かければ元の２にもどる

８があるとき、７を知っている人だけが元にもどせる

アールエスエー

ＲＳＡあんごう

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

えんざん
モジュロ演算　：　あまりをもとめる計算

年、月、日　⇒　よう日

日～土 ⇄ ０～６

２０２１、　１、　１　⇒　５（→金）

こうしき　　こうしき
（　ツェラーの 公式、　フェアフィールドの 公式　）

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

ショア
（ Ｓｈｏｒ ）

りょうし
（ 量子 コンピュータ ）

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

Ｓｈｏｒ

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

$2\times2\times2\div33$

$8\times8\times8\times8$
$\times8\times8\times8\div33$

おくりて ひらぶん　　あんごうか　　あんごうぶん　　ふくごう　　ひらぶん　うけとりて

送り手 平文 ⇒ 暗号化 ⇒ 暗号文 ⇒ 復号 ⇒ 平文 *受け取り手*

2　　↑3,33　　8　　↑7,33　　2

暗号鍵
あんごうかぎ

復号鍵
ふくごうかぎ

あま けいさん わ えいが あんごう

余り 計算 で 分かる映画『サマーウォーズ』の 暗号

じっさい あんごう アールエスエーあんごう

実際 の 暗号 （ＲＳＡ暗号）、

じっさい あんごう かいどく

実際 の 暗号 クイズ と 解読

あま　けいさん　わ
余り　計算　で 分かる

えいが　あんごう
映画『サマーウォーズ』の 暗号

参考文献

『サマーウォーズ』は
　映画　細田守 原作・監督, サマーウォーズ製作委員会, 2009/8.
　小説　岩井恭著, 細田守 原作, 角川書店, 2009/7.
　絵コンテ　アニメスタイル編集部編:サマーウォーズ絵コンテ細田守, スタイル, 2009/8.
　他にも、小説やコミックスがある.
RSA暗号は
　R.L. Rivest, A. Shamir, L. Adelman: “A Method for Obtaining Digital Signature and Public-key Cryptsystems, ” MIT-LCS-TM-082, 1977.
暗号クイズは
　Martin Gardner:“A new kind of cipher that would take millions of years to break,” Mathematical Games, Scientific American, 237(2), 120-124, 1977.
アトキンスらの解読は
　D.Atkins, M.Graff, A.K.Lenstra, P.Leyland:“THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE,” Advances in Cryptology – ASIACRYPT ‘94.

参考文献

Webページは
いぶき:映画サマーウォーズの暗号を京大生が解いてみた結果,
https://reistenza.com/entame/summer-wars.html

HKNEET:【本気で考えてみた】サマーウォーズのパスワードの暗号の解き方2056桁の暗号は解けるのか?,
http://win32programmer.seesaa.net/article/421790350.html

サルにも分かるRSA 暗号,http://www.maitou.gr.jp/rsa/rsa10.php
以上3 件の参照は2017/12
他にも、日本語で解説しているWebページは多数存在する。