Nikolaus Castell-Castell
MUDr. Tom Tietken

Prague Research Institute

Possibilities to identify prime numbers without RSA decryption algorithm and to decipher RSA encryptions indirectly (using a special list)

Initial situation:

In a certain part of the logic (where many identical individual parts are not changed or destroyed, but only rearranged), a result that comes about using a simple basic calculation should also be able to be traced back using a simple basic calculation.
If it is easy to get a certain result when you multiply two numbers (factors) together, it should not be difficult to "recalculate" this result back to its two factors with an equally simple basic calculation.

For 44 years, the so-called RSA code has been used for encryption in the western world, especially for messages, online trading and payment transactions, including that of insubstantial and manipulated crypto currency.
This is based on the phenomenon that so-called "large numbers" can be produced from prime numbers by multiplication, but that there is no procedure to reverse these large numbers back to their factors (i.e. to "factor them").
The term "large number" goes back to the fact that for RSA encryption relatively large prime numbers are multiplied with one another, which accordingly produce "large numbers" as products. In terms of definition, however, every multiplication product (no matter how small) is called a "large number" if it is made up of two (no matter how small) prime numbers.

In accordance with the requirements mentioned at the beginning, we have developed a very simple procedure for making such a calculation.
The previous reaction of the cryptologists confronted with this claim (in particular Ron Rivest and his two RSA co-inventors) was disbelief, which was justified by the fact that our (not yet published) scientifically held representation was not available in the form of a computer program and was therefore in practice could not be demonstrated.

Such practical evidence, including annual show fights by the RSA and NSA, are certainly exciting and serve to evaluate the RSA code, especially since they have not brought any noteworthy results for 44 years. And they are also advantageous for a participant because he can present knowledge without having to reveal his source code.

If, however, for whatever reason, we have (until now) preferred not to write a computer program and not take part in zero knowledge challanges, then interested number theorists will have to make the effort to read our work and (what everyone would be able to understand without problems). This causes the effort to think along and, if necessary, to rethink, but would have the advantage for a prospective customer of having got to know a new (simpler and in our opinion much closer) approach for a change.

This present work explicitly does not deal with the above-mentioned procedure, how a number, which has arisen from the multiplication of two numbers (in the practice of cryptography, these are prime numbers), is again broken down into these two prime numbers ("factored") !
The present manuscript is only intended to illustrate what is possible with the application of the basic calculation types, which are accessible to everyone.

For this purpose we have asked ourselves how one can even without an algorithm that directly breaks down (factored) "large numbers" (products),
can come to similarly useful results.
A suggested solution could be: You can also indirectly identify the prime numbers from which large products have arisen by creating lists in which all the numbers in question are stored in an orderly manner, continuously increasing.

The basic idea of the register proposed here:

The basic idea for this compromise here (we call it the "light" solution) is to determine prime numbers indirectly! Because if prime numbers, which are defined by the fact that they are not divisible by anything (except by 0 and 1), can only be recognized with great effort until now, then it makes sense to use neighboring numbers that also have the final digits 1, 3, 7 or 9, and which, in contrast to the prime numbers, can be divided by other numbers.

There are probably expert associations who have already created very extensive registers of prime numbers. In order to be sure that you have not "overlooked" or skipped any smaller prime numbers up to this highest prime number found up to now, this method that we have found here is required, only with numbers (ie also non-prime numbers!) calculate that have 1,3, 7, 9 as the last digits, and to count up these numbers of all kinds without gaps!

The divisible numbers are recognizable if you count them all up from bottom to top and note which numbers are multiplied with each other in order to finally (usually after many further multiplications) result in the present number.
There are three types of numbers:

a) Numbers that have arisen from the multiplication of non-prime numbers, especially if these have previously been multiplied with one another several times, are numbers that have nothing to do with the RSA encryption.

b) Numbers that have been multiplied from only 2 prime numbers are so-called "large numbers", for which their prime numbers are searched for (and found in the register) when deciphering.

c) And all numbers that in this regular series of natural numbers from 1 to 20001 etc. with 1, 3, 7 or 9 as the final digit, have no factors, i.e. no numbers that were previously multiplied together to produce this number , are prime numbers!

All of these three types of numbers can be seen in the proposed register.

More about the seamless register numbers ending with 1, 3, 7 and 9:

Our first algorithm from February 2020 breaks down so-called large numbers directly into their two prime factors (ie into one of the two, the other factor is then obtained by dividing the large number by the determined first factor) and assumes that it is these factors are prime numbers. If the decomposition (factorization) does not work, it can only be assumed that the present number was not a so-called "large number", but a prime number itself.

The addition of a register presented here solves the questions more reliably and clearly,
a) whether the factors are actually prime numbers in both cases and
b) whether the number to be factored is actually a "large number" that has been created by multiplying two prime numbers ..

This uniqueness is made possible especially by means of this self-assembling register, since all the numbers relevant for the present procedure are guaranteed to be contained in this register due to the regular incrementing! This basically unlimited register is suitable for deciphering a so-called large number, e.g. with a size of 2,000 digits, and can be set up independently with an extremely simple algorithm. Because for the construction and use of such a register no large computer systems are necessary, which try out all the numbers according to the so-called "brute force" method and need luck to come across a suitable result at some point (possibly before the static mean).

This number register, which you have to develop yourself, is in any case without gaps, since all the numbers are already available in it in advance. Because these numbers are not only incremented cardinally (whereby only the numbers with 0, 5, 2, 4, 6 and 8 are excluded as the last digit), but are limited to numbers with the final digits 1 in every 10-a-row, 3, 7 and 9. This means that the so-called counting up within ascending tens lines in only four categories (1, 3, 7, 9) is very easy for the program and always unequivocal. No number can be forgotten.
Because the register contains all existing natural numbers with the last digits 1, 3, 7 or 9. And all prime numbers and so-called "large numbers" always only have the last digits 1, 3, 7 or 9.

If a natural person or the machine used can count, the numerical structure required here is possible without computing power. Because the numbers always look like this:

(1)	3	7	9	(1. row with the 4 final digits 1,3,7,9)
11	13	17	19	(2. row with the 4 final digits 1,3,7,9)
21	23	27	29	(3. row with the 4 final digits 1,3,7,9)

etc.

2001	2003	2007	2009	(201. row with the 4 final digits 1,3,7,9)
2011	2013	2017	2019	(202. row with the 4 final digits 1,3,7,9)
2021	2023	2027	2029	(203. row with the 4 final digits 1,3,7,9)

etc.

All numbers (including the prime numbers to be determined and the "large numbers" to be factored) are practically completely present in this register. They just have to be defined:
It has to be recognized which of these numbers are prime numbers, which of these numbers are products (and if that is what they are and have arisen from prime numbers, then these are the so-called "large numbers"), and which numbers are not or no longer associated with these two belong to the aforementioned groups and are therefore referred to here as "other numbers".

The determination of the numbers:

There are in this register, beginning with the number "3" (because the "1" is omitted here in the units, because otherwise 1 * 3 would have to be calculated and then the result "3" would no longer be a prime number, but a so-called. "large number", which was created by multiplying 1 * 3) up to, for example, 2,000 or more of the following types of numbers:

a) Prime numbers (which can be recognized within the table by the fact that the numbers in the table on the left, i.e. mathematically preceding, side do not contain any factors that indicate the respective prime number),
b) so-called "large numbers", which are indicated by two prime factors multiplied with one another and
c) other numbers that are neither prime numbers nor so-called large numbers (i.e. products of prime factors), but also have the endings 1, 3, 7 or 9.
They could have been prime numbers and / or large numbers before, but now, after further partial multiplications, they are only "other numbers" and will always remain in the register. They fill up the register, but can no longer be used even for RSA encryption.

In addition, there are double assignments for many "other numbers", i.e. such numbers are the product of 2 or more pairs of factors. The number of pairs of factors is less important than the fact that factors refer to this number at all. Because then this number cannot be a prime number. Even as a "large number", such a double-assigned number is of no interest, because with double-assignment of factors it is not one of the large numbers that is required for a decryption.

What the finding of the present, in our opinion new, idea of calculating with all kinds of numbers as long as they have the last digits 1, 3, 7 and 9, could have made it difficult up to now:

What makes access to this obviously new and obvious method difficult is the non-matching of definitions of what a prime number is and the partial deviation of prime numbers and prime digits from one another.

1, 3, 7 and 9 are so-called prime end digits. However, all other types of numbers (prime numbers, so-called "large numbers" and other odd numbers, even those other numbers that have already been multiplied many times by the numbers in the register) can have these final digits.
The "9" is also a prime end digit, although it is a so-called "large number" as the product of the two prime numbers 3 * 3.
But the aforementioned definition is also questionable if it is considered that the prime number "3" could also be viewed as a "large number", which arose from 1 * 3.
For a "large number", however, two prime factors are required, and the "1" is expressly not one of the prime numbers. However, it is an important final prime digit.
Instead, "2" was declared the prime number, which according to our own (officially incorrect) definition is nothing less than a prime number, but an even number. It is also useless as a prime end digit, since all numbers to which the "2" is appended as the end digit become even numbers.
According to our own definition that no two factors should indicate a prime number in the register proposed here, the "5" is actually a prime number (because "5" divided by the "3" on the left is not possible with an even result). But it has been banned from our register, as it makes every number (including a trillion and 5) immediately divisible by 5 as the final digit.

What confirms the strict use of numbers with the endings 1, 3, 7 and 9 in our register is the order that numbers with these endings (regardless of what numbers they are) always have these endings 1, 3, Keep 7 or 9.

A helpful phenomenon of the aforementioned idea that all numbers (regardless of which of the three named types they belong to or how big they are numerically) always keep their final digits 1, 3, 7 and 9:

The following 4 calculation examples show how the final digits 1, 3, 7 and 9 (regardless of which numbers they are appended as final digits) only produce 1, 3, 7 or 9 as final digits through multiplication. For the sake of simplicity, only the single-digit end digits are multiplied here, but the same thing would also happen with multi-digit numbers:
For example, 3 * 7 = 21, i.e. a result with the last digit "1". This principle also applies to all numerically larger numbers. Also e.g. 27689473 * 56287 result with = 1.558.557.366.751 a result with "1" as the last digit.

1st row, in which the numerator "1" multiplies the final digits 1, 3, 7 and 9:
1*1=1;   1*3=3;   1*7=7;   1*9=9;

3-way row, in which the numerator "3" multiplies the final digits 1, 3, 7 and 9:
3*1=3; 3*3=9; 3*7=(2)1; 3*9=(2)7;

7-way row, in which the numerator "7" multiplies the final digits 1, 3, 7 and 9:
7*1=7; 7*3=(2)1; 7*7=(4)9; 7*9=(6)3;

9-way row, in which the numerator "9" multiplies the final digits 1, 3, 7 and 9:
9*1=9; 9*3=(2)7; 9*7=(6)3; 9*9=(8)1;

In the above calculation example, the counters 1, 3, 7, 9 are vertical from top to bottom, and the counted end digits 1, 3, 7, 9 are in horizontal positions, counting from left to right.
The final digits of the aforementioned results are repeated here in the following to show their order and always the same final digits:

1	3	7	9
3	9	1	7
7	1	9	3
9	7	3	1

The beginning of the register from 3 to 293 (the beginning of the 3, 7, 9, 11, 13 and 17 series):

a)
The following register (source: local institute) begins with the "1" at the top left.
The first multiplications are 3 * 3, 7 * 7, 9 * 9, 11 * 11 etc., i.e. multiplications in which the two multipliers are identical. Such a multiplication with itself results in a series of numbers in which the numerator remains constant for the duration of the series.
In the 3-way row, "3" is the constant counter. This row looks like this: 3 * 3, 3 * 7; 3 * 9, 3 * 11, etc.
In the 7-series, the "7" is the constant counter: 7 * 7, 7 * 9; 7 * 11; 7 * 13 etc.

If a number in the register is informed of the multiplication from which it was created, the multipliers e.g. 3 * 7 can also be written as 7 * 3 (or the 3 * 9 as 9 * 3 etc.).
But for reasons of space, and above all in order not to disorder the order of the successive counting from bottom to top, the smaller factor is always mentioned first in this register.
In addition, it is not the order of the factors that is of interest here, but the question of
a) whether there are any factors at all (if this is not the case, the number at hand is a prime number), and if this is the case, you are interested in
b) whether both factors are prime.

Further "forecasts" could also be written on the right-hand side of each number in the register. So instead of just writing 3 * 3 = 9 to the right of the "3", you could also write 3 * 7 = 21, 3 * 9 = 27, 3 * 11 = 33 to the right of the "3"; 3 * 13 = 39 etc. stand. Or instead of just having 7 * 7 = 49 to the right of the "7", there could also be 7 * 9 = 63, 7 * 11 = 77; 7 * 13 = 9; 7 * 17 = 119 etc. are written.
The latter is not possible for reasons of space, especially since every row of numbers starting with the multiplication with itself is unlimited in length.

What makes up the meaning of the following register are the three facts:

1) The numbers on which the register is based are easy to obtain, as they are only
a) must be counted cardinally in increments of ten and
b) Only the numbers with the last digits in the order 1, 3, 7 and 9 have to be shown per decade.
This method ensures that all numbers ending in 1, 3, 7 or 9 are recorded in the register.

2) Since prime numbers always end with 1, 3, 7 or 9, it is ensured that all prime numbers are also contained in the register.

3) Since the products of prime numbers always end with 1, 3, 7 or 9, it is ensured that these products (which are called "large numbers" and represent the numbers that are available during RSA deciphering) are completely contained in the register are.

All other numbers ending with 1, 3, 7 and 9 that are not prime numbers or so-called "large numbers" (or are no longer because the repeated multiplications change them) and are called "other numbers" here can be used with the RSA encryption are not used and inflate the register. But they are necessary for the completeness of all numbers with the last digits 1, 3, 7 and 9. Without it, it would not be possible to determine where a prime number or so-called "large number" is numerically.

1 **PRIME 3** (3*3=9) **PRIME 7** (7*7=49) (3*3=9) **9** (9*9=81)
PRIME 11 (11*11=121) **PRIME 13** (13*13=169) **PRIME 17** (17*17=289) **PRIME 19** (19*19=361)
(3*7=21) **21** (21*21=441) **PRIME 23** (23*23=529) (3*9=27) **27** (27*27=729) **PRIME 29** (29*29=841)
PRIME 31 (31*31=961) (3*11=33) **33** (33*33=1089) **PRIME 37** (37*37=1369)
(3*13=39) **39** (39*39=1521)
PRIME 41 (41*41=1681) **PRIME 43** (43*43=1849) **PRIME 47** (47*47=2209)
(7*7=49) **49** (49*49=2401)
(3*17=51) **51** (51*51=2601) **PRIME 53** (53*53=2809) (3*19=57) **57** (57*57=3249)
PRIME 59 (59*59=3481)
PRIME 61 (61*61=3721) (3*21=63 and 7*9=63) **63** (63*63=3969) **PRIME 67** (67*67=4489) (3*23=69) **69** (69*69=4761)

PRIME 71 (71*71=5041) **PRIME 73** (73*73=5329) (7*11=77) **77** (77*77=5929) **PRIME 79** (79*79=6241)

(3*27=81 and 9*9=81) **81** (81*81=6561) **PRIME 83** (83*83=6889) (3*29=87) **87** (87*87=7569) **PRIME 89** (89*89=7921)

(7*13=91) **91** (91*91=8281) (3*31=93) **93** (93*93=8649) **PRIME 97**(97*97=9409) (3*33=99 and 9*11=99) **99** (99*99=9801)

PRIME 101 (101*101=10.201) **PRIME 103** (103*103=10609) **PRIME 107** (107*107=11449) **PRIME 109** (109*109=11881)

(3*37=111) **111** (111*111=12321) **PRIME 113** (113*113=12769) (3*39=117 and 9*13=117) **117** (117*117=13689) (7*17=119) **119** (119*119=14161)

(11*11=121) **121** (121*121=14641) (3*41=123) **123** (123*123=15129) **PRIME 127** (127*127=16129) (3*43=129) **129** (129*129=16641)

PRIME 131 (131*131=17161) (7*19=133) **133** (133*133=17689) **PRIME 137** (137*137=18769) **PRIME 139** (139*139=19321)

(3*47=141) **141** (141*141=19881) (11*13=143) **143** (143*143=20449) (3*49=147 and 7*21=147) **147** (147*147=21609) **PRIME 149** (149*149=22201)

PRIME 151 (151*151=22801) (3*51=153 and 9*17=153) **153** (153*153=23409) **PRIME 157** (157*157=24649) (3*53=159) **159** (159*159=25281)

(7*23=161) **161** (161*161=25921) **PRIME 163** (163*163=26569) **PRIME 167** (167*167=27889) (13*13=169) **169** (169*169=28561)

(3*57= 171 and 9*19=171) **171** (171*171=29241) **PRIME 173** (173*173=29929) (3*59=177) **177** (177*177=31329) **PRIME 179** (179*179=32041)

PRIME 181 (181*181=32761) (3*61=183) **183** (183*183=33489) (11*17=187) **187** (187*187=34969) (3*63=189 and 7*27=189 and 9*21=189) **189** (189*189=35721)

PRIME 191 (191*191=36481) **PRIME 193** (193*193=37249) **PRIME 197** (197*197=38809) **PRIME 199** (199*199=39601)

(3*67=201) **201** (201*201=40401) (7*29=203) **203** (203*203=41209) (3*69=207 and 9*23=207) **207** (207*207=42849) (11*19=209) **209** (209*209=43681)

PRIME 211 (211*211=44521) (3*71=213) **213** (213*213=45369) (7*31=217) **217** (217*217=47089) (3*73=219) **219** (219*219=47961)

(13*17=221) **221** (221*221=48841) **PRIME 223** (223*223=49729) **PRIME 227** (227*227=51529) **PRIME 229** (229*229=52441)

(3*77=231 and 7*33=231 and 11*21=231) **231** (231*231=53361) **PRIME 233** (233*233=54289) (3*79=237) **237** (237*237=56169) **PRIME 239** (239*239=57121)

PRIME 241 (241*241=58081) (3*81=243 and 9*27=243) **243** (243*243=59049) (13*19=247) **247** (247*247=61009) (3*83=249) **249** (249*249=62001)

PRIME 251 (251*251=63001) (11*23=253) **253** (253*253=64009) **PRIME 257** (257*257=66049) (7*37=259) **259** (259*259=67081)

(3*87=261 and 9*29=261) **261** (261*261=68121) **PRIME 263** (263*263=69169) (3*89=267) **267** (267*267=71289) **PRIME 269** (269*269=72361)

PRIME 271 (271*271=73441) (3*91=273 and 7*39=273 and 13 *21=273) **273** (273*273=74529) **PRIME 277** (277*277=76729) (3*93=279 and 9*31=279) **279** (279*279=77841)

PRIME 281 (281*281=78961) **PRIME 283** (283*283=80089) (7*41=287) **287** (287*287=82369) (17*17=289) **289** (289*289=83521)

(3*97=291) **291** (291*291=84681) **PRIME 293** (293*293=85849)

...... and so on indefinitely

b)
The following additional table is suitable (source: authors) to show the order of the multiplications and their results and the recognition of prime numbers even more plausibly:

You connect graphically (in a kind of matrix) all natural numbers with the last digits 1, 3, 7 and 9 in the order described above in a horizontal row with exactly the same numbers in the same order in the vertical column on the left and leave one of these for the multiplications both rows of numbers (in this case the numbers in the vertical column on the left) act as counters.
You get objects (products) that also end in 1, 3, 7 or 9.

1	**3**	**7**	**9**	**11**	**13**	**17**	**19**	**21**	**23**	**counted factors**
3	9	21	27	33	39	51	57	63	69	3-s row
7		49	63	77	91	119	133	147	161	7-es row
9			81	99	117	153	171	189	207	9-s row
11				121	143	187	209	231	253	11-s row
13					169	221	247	273	299	13-s row
17						289	323	357	391	17-s row
19							361	399	437	19-s row
21								441	483	21-s row
23									529	23-s row
counting factors										**etc.**

Explanations to the previous table:

On the diagonal of "1, 9, 49, 81, 121, 169, 289, 361 etc." (in the direction to the bottom right) would be exactly the same multiplication results on the right side at the analogous positions as on the left side of this diagonal. That is why they are omitted from this graphic.
The starting numbers on this diagonal are created by multiplying by themselves.

In order to avoid the same products on the right and left side of the diagonal, a series of numbers always begins with the number that introduces this series of numbers by multiplying this number by itself.
Since each new row of numbers begins with the multiplication of the initial number by itself, it is avoided that, for example, a multiplication in the order 7 * 3 has to be carried out. The "7" is only multiplied from "7", namely with itself (7 * 7 = 49). The "21" previously arose from the multiplication in the 3-ary row by 3 * 7 (and not 7 * 3).

This table clearly shows the possible sequences:
You could first "finish" the series of 3 numbers that begin with the self-multiplication 3 * 3 (3 * 7 = 21, 3 * 9 = 27, 3 * 11 = 33, 3 * 13 = 39, etc.), which is not possible because of its endlessness.
And after 7 * 7 = 49 you could continue with the 7-digit series (7 * 9 = 63; 7 * 11 = 77; 7 * 13 = 91; 7 * 17 = 119 etc.).
And then it would be the turn of the 9-series of numbers and other series of numbers (such as 11-series, 13-series, 17-series, etc.).
But such a procedure is impractical because of the unlimited length of each row of numbers.

Even if multi-digit numbers in registers and tables cannot be represented graphically, according to the theory presented here, all numbers with the last digits 1, 3, 7, 9 are always ordered in exactly the way described here! So also in the imagination (without registers and tables).
The numbers are counted up cardinally, whereby only the 4 numbers with the last digits 1, 3, 7, 9 are recorded for each incrementally increasing 10-series.

There are 5 theses:

1) At the beginning of this counting, all these numbers, determined in the manner described here, begin with the last digits 1, 3, 7, 9 with the prime numbers 3 and 7.
These prime numbers continue after the exception "9" (11, 13, 17, 19).
The next exception is "21" (from the prime factors "3" and "7"), and then continues with the prime number "23".

2) Since all prime numbers are also multiplied by all prime numbers, this number series of prime numbers is interrupted by products that result from these multiplications of prime numbers with one another and are called "large numbers" in cryptography (large integers).

3) Since, according to the postulate of this work, all numbers are multiplied by all numbers with one another, it happens more and more frequently in later places that numbers are multiplied with one another
a) are no longer prime numbers and accordingly are no longer "large numbers" (products of prime numbers), but rather
b) after a few more steps, become "other numbers" as you name them.
These are products of a prime number and a "large number" or products of 2 "large numbers" or products of the remainder, i.e. two "other numbers".

4) According to the logic it is conceivable that these "other numbers", relative to the other numbers, occur more and more frequently, especially since they are constantly being multiplied

with one another.

5) Since the latter also always have the final digits 1, 3, 7, 9, it would be obvious to claim that it is this growing number of "other numbers" that is increasingly displacing the prime numbers and thus also the so-called "large numbers".

At position 81, 2 so-called "large numbers" were multiplied together for the first time (9 * 9). This is followed by other such products (from 21 * 21, 27 * 27, etc.).
And if afterwards their products (from large numbers), e.g. 21 (large number) * 21 (large number) = 441 (other number) and then 441 (other number) * 441 (other number) = 194,481 (other number) to factors for further multiplications (and always immediately), it is again just "other numbers".
However, from "other numbers" that have arisen from an unclearly large number of multiplications.
We do not name the so-called "other numbers" more precisely, as these other numbers have no meaning for cryptography.

The order of the processing steps and the successive recognition of the prime numbers:

This additional table makes it clear that the series of numbers (3, 7, 9, 11, 13, 17, 19, etc.) should not be processed one after the other, but that first the immediate vicinity of the number at hand should always be completed in order to identify the prime numbers and thus the so-called "large numbers" as early as possible.

It is the diagonal in the table that specifies the cardinal order of the steps and indirectly clarifies which numbers are prime numbers:

a) In the horizontal line at the top, which shows the counted factors, and in the vertical column at the far left, the numbers 3 and 7 appear. Since these numbers do not appear in the rows inside the field, 3 and 7 can be recognized as prime numbers.

b) Between 9 and 23, the numbers 11, 13, 17, 19, 23 are missing in the field, which means that these are recognized as prime numbers.

c) Exactly in this way one can continue indefinitely:
On the diagonal between 49 and 81 the numbers are missing: 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79.The numbers 51, 57, 63, 69 (not visible here in the table, since 69 = 23 * 3 only appears in the 23rd position of the left vertical counter) and 77 again, so that the numbers 53, 59, 61, 67, 71, 73, 79 remain as prime numbers etc.

Divisions as a way to get the same results without registers and tables:

If there are no visually visible or otherwise accessible registers or tables of the type described here, one can also start directly from the one available number and either ask: "Is this a large

number that has to be broken down into two prime numbers for deciphering?".
Or, in the case of encryption, you start from two numbers and ask before they are multiplied with each other: "Are these two numbers both prime numbers?"
Both questions can be answered by divisions, which are carried out in the same way as the one described here (i.e. only count with numbers ending with 1, 3, 7, 9).

Numerical example for division:

Assuming there is a multi-digit number that has the final digits 1, 3, 7 or 9, but it cannot be seen whether it is a prime number, a so-called "large number" or an "other number":

By dividing this multi-digit number by all the numbers shown here (3, 7, 9, 11, 13, 17, 19, 21, 23, etc.) in exactly this order, you arrive "sometime" (according to the probability, 50% of all Possibilities, but in practice much earlier, since only two of several possibilities are being sought: Is the present number a prime number or is a present number a so-called "large number" from two prime numbers?) to the desired solution.

The number of divisions required for clarification is shortened by the fact that the only aim is to find out
1) whether it is a prime number. Even with the first divisibility, it is clear that there is no prime number and that this number is not suitable for creating an encryption.
2) If, however, a decryption is to be carried out, a so-called "large number" must be broken down into its two prime factors. Normally it can be assumed that the factors found are prime numbers. However, if there are any doubts about this, an attempt can be made to divide the factors obtained further times.

Here is a randomly chosen numerical example, which, due to the constant laws of the decimal system, also applies to unlimited multi-digit natural numbers:

-) If, for example, the number "7843" is present, divisions by 3, 7, 9, 11, 13, 17 etc. can help to find out whether 7843 is a prime number. Since it can be divided by the divisor "11" and results in the quotient "713", it is not a prime number. So it would not be useful for an encryption.

-) When deciphering the question could be what the second resulting factor, the "713", is: Whether it is an "other number" or a so-called "large number (ie a product of two prime numbers). Because one of them Both divisors, the previously known "11" is a prime number. If it were not a prime number, but a product of factors, the lowest of these factors would have already made itself noticeable as a divisor.

For this, this current dividend "713" is also divided one after the other by the numbers 3, 7, 9, 11, 13, 17, 19, 21, 23 etc. and results in "31" with the successful divisor "23".
This shows that the number "713" was not a prime number either. However, "713" is a so-called large number from the prime factors "23" and "31".

-) That "23" and "31" are prime numbers can again be determined with the same method as above: In fact, however, neither "23" nor "31" can be divided by 3, 7, 9, 11, so they are prime numbers.

-) As an overall result, with the help of these aforementioned divisions, it turns out that the number "7843" is an "other number" that has arisen from several multiplication steps, so it is neither suitable for encryption nor decryption.

Conclusion:

The complete presence of all numbers with the endings 1, 3, 7 and 9 and their incremented cardinal arrangement and the process of multiplying all these numbers by all these numbers individually result in the theoretical possibilities of a) identifying all prime numbers and b) all " large numbers ".

Bibliography:

No citations and sources can be given here, as we are not aware of any sources for this approach or parts of them.
We developed this approach ourselves with the simplest means and obvious considerations.

Nikolaus Graf zu Castell-Castell
Dipl. Vw. (Universitaet Hamburg)

Tom Hermann Tietken
MUDr. (Charles-University Prague)

Prague Research Institute
Zug (CH) und Prague (CR)
mob. 00420 778 037 633
fix line 00420 226 223 026