雑感　新時代の暗号

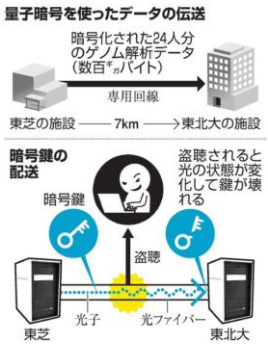
■　276069853871622551497390234491079316684587161426206011699548030008033 29
この数を素因数分解してください．お願いします．
おそらく素因数の数は 2 つになります．
　過日の知恵袋の質問．

■　手作業は無理．愛用の数式処理ソフト DERIVE で factor として計算させるが，いつまでも青い丸がぐるぐる回っている．
　WolframAlpha は，すぐにタイムアウトした．(有料の)Pro 版を使えとのメッセージが出るが，それとて果たしてやり切れるかどうか怪しい．
　GeoGebra の Factors では，瞬時に「未定義」とされてしまった．桁数制限でもあるのだろうか．
　Maxima では「処理中」がずっと続く．どんな処理をしているのだろうか．まさか，エラトステネスの篩？

■　多分有名な値であろうと，ググれば何件目かで見つかる．
　162259276829213363391578010288127
*170141183460469231731687303715884105727
＝ $(2^{107}-1) * (2^{127}-1)$
　という 2 つのメルセンヌ素数の積である．
　http://www.log-in-verlag.de/service/2010/LOG-IN-Service_166-167_(2010)/107-114_Zeit-Experimente/Tabelle_4.pdf
　には，こういった難解な素因数分解がたくさん載っている．

■　よく知られたことだが，複雑な合成数の素因数分解が暗号と関係している．Wikipedia によれば，
　「RSA 暗号は次のような方式である： 鍵ペア（公開鍵と秘密鍵）を作成して公開鍵を公開する．まず，適当な正整数 e（通常は小さな数．$65537\,(=2^{16}+1)$ がよく使われる）を選択する．また，大きな 2 つの素数 $\{p,q\}$ を生成し，それらの積 $n\,(=pq)$ を求めて，$\{e,n\}$ を平文の暗号化に使用する鍵（公開鍵）とする」
　この n の素因数分解が暗号の復号に必要になるが，桁数が大きく素因数分解が難しい．

■　2020 年 1 月 14 日の朝日新聞．
　「「究極の暗号」で遺伝情報を伝送　東芝と東北大，初成功」と題する記事が載った．
　一部を転載すると



　盗聴が原理的に不可能な「究極の暗号」である量子暗号を使い，24 人分のヒトゲノム（全遺伝情報）を伝送することに東芝と東北大が成功したと，14 日発表した．送ったデータ量は映画 10 本分に相当する数百ギガバイト．ゲノムのような高い秘匿性が求められるデータをこれほど大容量で伝送できたのは世界初といい，東芝は「量子暗号が実用レベルになった」としている．

　現在広く使われている暗号は，整数を素数のかけ算の形にする素因数分解は，整数が非常に大きいと困難になるという性質を利用している．しかし，量子コンピューターが実現すると短時間で解読できるとされ，それまでに量子暗号を実用化しようと各国が開発を急いでいる．量子暗号は盗聴を必ず検知でき，暗号を解く鍵を作り直すことで第三者による解読を避けられるからだ．（途中略）

　量子暗号では，データを暗号化して送り，暗号を解く鍵の情報を非常に弱い光に乗せて別に伝送し，受け取った側がその鍵で暗号を解く．伝送中に盗聴があると，量子力学の原理で光の状態が変化するため，盗聴されたことがわかる．

　ただ，光が弱いので，長距離では減衰したり，ノイズが入ったりして鍵が使えなくなる．このため，中継装置を配置したり，光が減衰しない宇宙空間を使ったりして通信距離を延ばす試みが進んでいる．（以下略）

■　暗号にメルセンヌ素数の出番がなくなる日が，遠からずやってくるのだろうか．

2020 年 02 月 01 日