https://fr.wikipedia.org/wiki/Gypaète_barbu https://en.wikipedia.org/wiki/Bearded_vulture (ossifrage))

Joyeux Noël et **Merry Christmas, and**

Meilleurs voeux pour
Best wishes for
$x = pq$

où p et q sont deux nombres premiers. Ils sont assez proches l'un de l'autre, ce qui semble une bonne façon de rendre difficile la recherche des facteurs d'un grand nombre N. Mais on trouva rapidement une parade en examinant si un des nombres $N, N+1, N+4, \ldots$ est le carré d'un entier: si $N+a^2 = b^2$, alors $N = (b-a)(b+a)$, *Yes!* Mieux (Fermat): essayez b tel que $b^2 - N$ soit le carré d'un entier. G.H. Hardy était bien certain que de telles recherches mathématiques, qui furent très considérablement développées, ne trouveraient jamais, jamais, d'application commerciale ou militaire.

Martin Gardner expliqua dans sa rubrique de jeux mathématiques du numéro d'août 1977 de *Scientific American* comment déchiffrer un message, où tout est rendu public... sauf les facteurs d'un nombre donné $N = uv$. Le déchiffrement nécessite la connaissance de $\phi(N) = (u-1)(v-1)$, ce qui ne semble possible que si u et v sont connus. Des centaines d'ordinateurs traitèrent séparément des parties du problème (comme les a et b ci-dessus, mais en plus compliqué) et on arriva à u et v en 1994, voir "RSA-129". La solution contient les mots "squeamish ossifrage", qui veut dire "un oiseau charognard briseur d'os dégoûté", et semble venir d'une littérature assez *late gothic*. Une bonne approximation est "Haut dans le ciel vide, un œsophage solitaire dormait sur une aile immobile", dans *Une histoire policière à double détente* de Mark Twain, 1902.

Pour notre problème, nous partons de x et ... Eh! x est ce qu'il faut trouver! Très bien, soit u et v les deux seuls facteurs premiers de $N = (2^{58}+1)/5$ (pas trouvé? cherchez le nom "Aurifeuille"),et y le nombre formé des quatre derniers chiffres décimaux de $\phi(N)$. Alors, $x = y$ XOR k, où la clé $k = 1013_{10} = 03F5_{16} = 0000001111110101_2$. L'opération XOR est définie chiffre binaire par chiffre binaire par

	0	1
0	0	1
1	1	0

. Cette opération s'écrit ^ en `c`, `c++` et `Python`.

where p and q are prime numbers. They are rather close together, which seems a good way to make the factorization of a large number N a difficult problem. But this was easily outwitted by looking if $N, N+1, N+4, \ldots$ is the square of an integer: if $N + a^2 = b^2$, then $N = (b-a)(b+a)$, *Voilà!* Better yet (Fermat): try b such that $b^2 - N$ is the square of an integer number. G.H. Hardy was absolutely sure that such mathematical research, which went to a very high level of sophistication, would never, never, be used in the business world or the military.

Martin Gardner's Mathematical Games column in the August 1977 issue of *Scientific American* gave a full example of a secret message depending only on the factorization $N = uv$ of a given large number! Deciphering needs $\phi(N) = (u-1)(v-1)$ found only if u and v are known, so it seems. Hundreds computers were set on independent tests (something like the a and b above, but much more sophisticated) and u and v were finally produced in 1994, see "RSA-129". The message contained the words "squeamish ossifrage", meaning "a disgustef bone-breaking bird", suggesting a *fin de siècle* poetry origin. A close approximation is "far in the empty sky a solitary oesophagus slept upon motionless wing" in Mark Twain's *A double barrelled detective story* (1902).

For our problem we just start with x and... Hey! x is what is to be found! All right, let u and v be the sole prime factors of $N = (2^{58}+1)/5$ (clue if you don't find: search "Aurifeuille"), and y the number made with the four last decimal digits of $\phi(N)$. Then find $x = y$ XOR k, where the key $k = 1013_{10} = 03F5_{16} = 0000001111110101_2$. The bitwise XOR operation is

	0	1
0	0	1
1	1	0

. This operation is written ^ in `c`, `c++` and `Python`.

Alphonse Magnus,
Institut de Mathématique Pure et Appliquée,
Université catholique de Louvain,
Chemin du Cyclotron,2, B-1348 Louvain-la-Neuve (Belgium)
alphonse.magnus@uclouvain.be , http://perso.uclouvain.be/alphonse.magnus