RSA 暗号の「懸賞問題」

"A new kind of cipher that would take millions of years to break", Scientific American, August 1977

Martin Gardner and Scientific American

RSA-129

- n = 1 1438 1625 7578 8886 7669 2357 7997 6146 6120 1021 8296 7212 4236 2562 5618 4293 5706 9352 4573 3897 8305 9712 3563 9587 0505 8989 0751 4759 9290 0268 7954 3541
- e = 9007
- 9686 9613 7546 2206 1477 1409 2225 4355 8829 0575 9991 1245 7431 9874 6951 2093 0816 2982 2514 5708 3569 3147 6622 8839 8962 8013 3919 9055 1829 9451 5781 5154

法ｎと指数ｅが公開され、暗号文 9686 … 5154 をもとの英語の平文にする懸賞問題が RSA の発明者３人から出題された。懸賞金はたった 100 ドル。

符号化は、 A=01,B=02,C=03, … Space=00 の 27 個の記号のみ。

1977, Rivest, Shamir and Adleman

- １２９桁（４２５ビット）
- 11438 20102 35245 07514 16257 18296 73389 75992 57888 72124 78305 90026 86766 23625 97123 87954 92357 79976 14661 62561 84293 57069 56395 87050 58989 3541
- この１２９桁の公開鍵ｎを２つの素数の積に分解する。

Squeamish Ossifrage

Date: Wed, 27 Apr 94 22:03:30 PDT

To: Fun People

Subject: R.S.A. 129 falls

Using volunteers on the Internet, who downloaded portions of the problem using ftp and ran them on otherwise idle machines, an international effort using more than 1600 machines for 8 months managed to factor the number:

The two factors are
34905 29510 84765 09491 47849 61990 38981
33417 76463 84933 87843 99082 0577
and
32769 13299 32667 09549 96198 81908 34461
41317 76429 67992 94253 97982 88533

Decoding the phrase
THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE
（魔法の言葉はキーキー鳴くはげ鷲）

RSA cracked!!

This feat was widely reported in the popular press - in particular one issue of the New York Times had the factorization printed across the entire front page.

One unfortunate side-effect of popular coverage was that the reports often mutated from “RSA-129 has been cracked” into “RSA has been cracked”.

Factoring RSA-129 just means that one particular key has been cracked. Of course if you were unlucky enough to using that particular value of n as your public key, then you would have to change.

In general however, it means that if you have a 425-bit modulus, then you can expect it to take 1600 machines about 8 months to crack. Simply changing your modulus to a 1024-bit modulus makes a factorization attack completely infeasible (at the moment).

The New York Times, 1994-03-22

The Assault on 114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,271,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541

By GINA KOLATA

Published: March 22, 1994

MATHEMATICIANS say they are close to breaking a cryptographic stronghold that was not expected to fall for many years.

The item is a 129-digit number that was first described in 1977 as proof of the security of a new public cryptographic system.

http://www.nytimes.com/1994/03/22/science/assault.html?pagewanted=all

RSA 暗号システム

1. Select two large prime numbers p and q (100 or more digits).

2. Compute the product $n = pq$ and the value $\varphi(n) = (p - 1)(q - 1)$.

3. Choose a small odd integer e that is relatively prime to $\varphi(n)$.

4. Use Euclid's extended algorithm to solve the equation $ed \equiv 1 \pmod{\varphi(n)}$.

5. The public key is (n, e), which can be distributed, and the private key is d.

解説：リベストらの実例

- ITS ALL GREEK TO ME
- 0920190001121200071805051100201500130 5
- e=9007
- (0920190001121200071805051100201500130 5) を 9007 乗して　(mod n) をとる。
- これで暗号化される。
- 199935131497805100452317122740260647423204017058391463103703717406259716089489275043099209626725826750128935544613538237697480 26

１字の簡単な暗号の RSA 例題

- 公開鍵 :　 *n=209 (= 11×19),　e=7*
- 秘密鍵 :　 *p=11, q=19 と d=13*
- 平文　 :　 46
- 暗号文を平文から計算する： 46 ^ 7 (mod 209). すなわち４６を７乗し、それを２０９で割った余りを求める。
- 暗号文 :　 計算の結果は、 84 となる。
- 復号、すなわち暗号文８４から平文を求めるには秘密鍵ｄ＝１３を使う。計算方法は、 84 ^ 13 (mod 209) である。

公開鍵 e と復号用秘密鍵 d の関係

- 例題の復習： e=7, d=13
- m^e ≡ c (mod n)
- c^d ≡ m (mod n)
- n=p×q

素数 p, q の選定のしかた。
実際に RSA-129 では :

p=
34905 29510 84765 09491 47849 61990 38981
33417 76463 84933 87843 99082 0577
q=
32769 13299 32667 09549 96198 81908 34461
41317 76429 67992 94253 97982 88533

比較的近くて１けたくらい違う
素数をペアにする。
また、 p-1 と q-1 は、偶数だが公約数が２
だけが望ましい。
さらに、指数 e は、 p-1 とも q-1 とも互いに
素でなければならない。

これらも詳細は、別稿に示す。

e の逆数 d は、互除法によって計算できる。