Mathematics 124 (Winter 2009)
RSA-129

In August 1977, a problem appeared in Martin Gardner's *Mathematical Games* column in *Scientific American*. It was posed by Rivest, Shamir, and Adleman, and consisted of the following information.

Alice broadcasts her public exponent e and her modulus m where $e = 9007$ and

$$m = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.$$

Eve has intercepted the ciphertext

$$y = 968696137546220614771409225435588290575999112457431987469512093081629822514570835693147662288398962801339199055182994515781515 4.$$

What is the plaintext?

In order to decipher the message, one must factor the 129-digit m into the product of primes. This number became known as RSA-129.

In April 1994, a team consisting of Derek Atkins, Michael Graff, Arjen Lenstra, and Paul Leyland succeeded in factoring RSA-129. They used the *double large prime variation of the multiple polynomial quadratic sieve factoring method*. The sieving step was carried out in 8 months by about 600 volunteers from more than 20 countries. The end result was

$$\begin{aligned}\text{RSA-129} &= pq \\ &= 3490529510847650949147849619903898133417764638493387843990820577 \\ &\quad \times 327691329932667095499619881908344614131776429679929425397982885 33.\end{aligned}$$

When decrypted with the secret exponent

$$\begin{aligned}d &= e^{-1} \operatorname{MOD}(p-1)(q-1) \\ &= 106698614368578024442868771328920154780709906633937862801226224496631 \\ &\quad 063125911774470873340168597462306553968544513277109053606095\end{aligned}$$

the plaintext $x = y^d \operatorname{MOD} m$ reads

$$200805001301070903002315180419000118050019172105011309190800151919090618010705.$$

Exercise. Write the plaintext as

20 08 05 00 13 01 07 09 03 00 23 15 18 04 19 00 01 18 05 00
19 17 21 05 01 13 09 19 08 00 15 19 19 09 06 18 01 07 05.

Using the following numerical equivalents of the letters

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

with 00 corresponding to a space, decode the message.

Remark. It seems that Martin Gardner's article can be read at

http://www.fortunecity.com/emachines/e11/86/cipher1.html