Martin Gardner

Scientific American **August 1977**

A new kind of cipher that would take millions of years to break

This trapdoor ciphers column introduced RSA cryptography, a new "public key" method of secret communication previously not believed possible. It was based on an MIT memo by Ron Rivest, Adi Shamir and Leonard Adleman from April 1977, which they sent to Gardner. He was so impressed that he broke his usual rule of planning his column several months in advance, and quickly wrote it up for publication.

The basic idea is to secretly take two very large prime numbers (p, q) at least 40 digits long each, and form their product $r = pq$, assuming that it would be an insurmountable task for an outsider to factor r. Its considered safe to reveal r, as well as a related odd number s, to all and sundry; that's the public key. Anyone wishing to send a secret numerical "word" w to the person who selected p and q does the following: find the remainder e when w is divided by r, and communicate e openly. An easy mathematical trick allows a person who knows e to reconstruct w from it provided they know the factors p and q of n, but it seems unlikely that somebody not knowing p and q would have a chance.

To prove the point, the RSA team provided Gardner with a 128-digit coded message e, computed using a specified 129-digit n, which was the product of mysterious top-secret, 64-digit and 65-digit primes p and q, respectively. They also indicated that $s = 9007$. A prize of $100 was offered for anyone who could recover the original message w from which e had been computed. Given the title of the column, it was assumed

that no one would crack it anytime soon. In fact, Gardner hedged his bets and prefaced the piece with an Edgar Allan Poe quote: "Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

RSA cryptography became an industry standard and variations of it are still in use today, though in recent times the question of how secure it is has been revisited. Despite the groundbreaking nature of Gardners column, it didn't quite live up to its title. The challenge message posed in it was successfully decoded as early as April 1994.