8. Pretty good privacy

On September 20, 1983 the Massachusetts Institute of Technology was granted U.S. Patent 4,405,829 for a *Cryptographic communications system and method*. The patent lists Ron Rivest, Adi Shamir, and Leonard Adleman as the inventors of the method. The patent abstract states:

> The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by encoding the message as a number M in a predetermined set. That number is then raised to a first predetermined power (associated with the intended receiver) and finally computed. The remainder or residue, C, is... computed when the exponentiated number is divided by the product of two predetermined prime numbers (associated with the intended receiver).

US export laws at the time prohibited export of this and similar cryptographic inventions. The patent has now expired and the export laws have been relaxed. So we are free to divulge the mathematical invention covered by the patent. In fact, since the UK based mathematician Clifford Cocks had already invented the method in 1973, it is likely that neither MIT nor the US government could every have won a court battle against anyone for using this mathematics outside of the USA.

To explain the invention let us suppose that we are working with plaintext over an N-letter alphabet, and that we have decided to split the plaintext up into k-letter message units and to split the ciphertext up into ℓ-letter message units. For existence, we might be using the finite alphabet

$$A \leftrightarrow 0,\ B \leftrightarrow 1,\ C \leftrightarrow 2,\ \ldots,\ Z \leftrightarrow 25$$

consisting of $N = 26$ letters, with a correspondence between the alphabet letters and the numbers in $\mathbb{Z}_{27}$. We might be using $k = 3$ so that plaintext such as

MEETMETONIGHTOK

would be split into a list

MEE, TME, TON, IGH, TOK

of six 3-letter message units. We might be using $\ell = 4$ so that ciphertext such as

XYABZTAA

would be split into a list

XYAB, ZTAA

of two 4-letter message units. We choose bijections:

$$\text{plaintext message units} \longleftrightarrow \text{integers } 0 \leq i < N^k \tag{8.1}$$

$$\text{ciphertext message units} \longleftrightarrow \text{integers } 0 \leq i < N^\ell \tag{8.2}$$

Convenient bijections are obtained by regarding message units as polynomials in N, as in the following example.

$$Y\ E\ S \longleftrightarrow 24.\mathbf{26}^2 + 4.\mathbf{26} + 18.\mathbf{26}^0 = 16346 \tag{8.3}$$

With thses preliminaries out of the way, we now describe the RSA public key cryptosystem.

8.1 RSA cryptosystem

- A user chooses two distinct random prime numbers p and q (each of around 1000 digits to be safe against current computer capabilities).
- The user chooses an integer e that is not divisible by either p or q, and uses the Euclidean algorithm to compute:

$$d \equiv e^{-1} \mod (p-1)(q-1) \tag{8.4}$$

- The user computes the product:

$$n = pq \tag{8.5}$$

- The user publishes the enciphering key $E = (n, e)$ and keeps secret the second component of the deciphering key $D = (n, d)$.
- A plaintext message unit, corresponding to an integer a, is enciphered as:

$$f_E(a) \equiv a^e \mod n \tag{8.6}$$

- A ciphertext message unit, corresponding to an integer a, is deciphered as:

$$f_D(a) \equiv a^d \mod n \tag{8.7}$$

Lemma (7.3.1) ensures that $f_D(f_E(a)) = a$. That is, the ciphertext gets deciphered into the original plaintext.

To illustrate the cryptosystem let us continue with the above alphabet of $N = 26$ letters, plaintext message units of length $k = 3$ and ciphertext message units of length $\ell = 4$.cryptosystem let us continue with the above alphabet of $N = 26$ letters, plaintext message units of length $k = 3$ and ciphertext message units of length $\ell = 4$.

Suppose that Bob wants to send Alice the message YES . He looks up Alice's public key, which we take to be

$$E_{Alice} = (N, e) \tag{8.8}$$

$$= (46927, 39423) \tag{8.9}$$

where the value of n is kept unrealistically small for illustrative purposes. Bob computes

$$\begin{aligned} f_{E_{Alice}}(\text{YES}) &\leftrightarrow f_{E_{Alice}}(16346) && (8.10)\\ &= 16346^{39423} \mod 46927 && (8.11)\\ &= 21166 && (8.12)\\ &= 1.\mathbf{26}^3 + 5.\mathbf{26}^2 + 8.\mathbf{26} + 2.\mathbf{26}^0 && (8.13)\\ &\leftrightarrow \text{BFIC} && (8.14) \end{aligned}$$

Bob thus sends the ciphertext BFIC to Alice.

On receiving thr ciphertext Alice deciphers it using her secret deciphering key.

8.2 Two remarks

1. Currently the only known method for the task of calculating $d \equiv e^{-1} \mod \phi(n)$ involves factoring $n = pq$ to determine the primes p and q that Alice chose when constructing her keys.
2. Currently the task of factoring n as a product of primes is prohibitively time consuming when p and q are well-chosen large primes.

The search for new mathematics relating to these two tasks is an active area of current research.