MA2C03 Mathematics
School of Mathematics, Trinity College
Hilary Term 2016
Lecture 59 (April 1, 2016)

David R. Wilkins

The RSA encryption scheme works as follows. In order to establish the necessary public and private keys, one first chooses two distinct large prime numbers p and q. Messages to be sent are to be represented by integers n satisfying $0 \leq n < m$, where $m = pq$. Let $s = (p-1)(q-1)$, and let e be any positive integer that is coprime to s. Then there exists a positive integer d such that $ed \equiv 1 \pmod{s}$ (see Lemma 41.12). Indeed there exist integers d and t such that $ed - st = 1$ (Corollary 41.3), and appropriate values for d and t may by found using the Euclidean algorithm. Moreover d and t may be chosen such that $d > 1$, for if d' and t' satisfy the equation $ed' - st' = 1$, and if $d = d' + ks$ and $t = t' + ke$ for some integer k, then $ed - st = 1$. Thus, once a positive integer e is chosen coprime to s, standard algorithms enable one to calculate a positive integer d such that $ed \equiv 1 \pmod{s}$.

Now suppose that p, q, m, s, e and d have been chosen such that p and q are distinct prime numbers, $m = pq$, $s = (p-1)(q-1)$, e and d are coprime to s and $ed \equiv 1 \pmod{s}$. Let

$$I = \{n \in \mathbb{Z} : 0 \leq n < m\}.$$

Then for each integer x belonging to the set I, there exists a unique integer $E(x)$ that belongs to I and satisfies the congruence $E(x) \equiv x^e \pmod{m}$. Similarly, for each integer y belonging to the set I, there exists a unique integer $D(y)$ that belongs to I and satisfies the congruence $D(y) \equiv y^d \pmod{m}$. Now it follows from standard properties of congruences (Lemma 41.9) that if y and z are integers, and if $y \equiv z \pmod{m}$, then $y^d \equiv z^d \pmod{m}$. It follows that $D(E(x)) \equiv D(x^e) \equiv x^{ed} \pmod{m}$ for all integers x belonging to I. But $ed \equiv 1 \pmod{s}$, where $s = (p-1)(q-1)$. It follows from Theorem 42.1 that $x^{ed} \equiv x \pmod{m}$. We conclude therefore that $D(E(x)) \equiv x \pmod{m}$ for all $x \in I$. But every congruence class modulo m is represented by a single integer in the set I. It follows that that $D(E(x)) = x$ for all $x \in I$.

On reversing the roles of the numbers e and d, we find that $E(D(y)) = y$ for all $y \in I$. Thus $E\colon I \to I$ is an invertible function whose inverse is $D\colon I \to I$.

On order to apply the RSA cryptographic method one determines integers p, q, m, s, e and d. The pair (m, e) of integers represents the *public key* and determines the encryption function $E\colon I \to I$. The pair (m, d) of integers represents the corresponding *private key* and determines the decryption function $D\colon I \to I$. The messages to be sent are represented as integers belonging to I, or perhaps as strings of such integers. If Alice publishes her public key (m, e), but keeps secret her private key (m, d), then Bob can send messages to Alice, encrypting them using the encryption function E determined by Alice's public key. When Alice receives the message from Bob, she can decrypt it using the decryption function D determined by her private key.

Note that if the value of the integer s is known, where $s = (p-1)(q-1)$, then a private key can easily be calculated by means of the Euclidean algorithm. Obviously once the values of p and q are known, then so are the values of m and s. Conversely if the values of m and s are known, then p and q can easily be determined, since these prime numbers are the roots of the polynomial $x^2 + (s - m - 1)x + m$. Thus knowledge of s corresponds to knowledge of the factorization of the composite number m as a product of prime numbers. There are known algorithms for factoring numbers as products of primes, but one can make sure that the primes p and q are chosen large enough to ensure that massive resources are required in order to factorize their product pq using known algorithms. The security of RSA also rests on the assumption that there is no method of decryption that requires less computational resources than are required for factorizing the product of the prime numbers determining the public key.

It remains to discuss whether it is in fact feasable to do the calculations involved in encrypting messages using RSA. Now, in order determine the value of $E(x)$ for any non-negative integer x less than m, one needs to determine the congruence class of x^e modulo m. Now e could be a very large number. However, in order to determine the congruence class of x^e modulo m, it is not necessary to determine the value of the integer x^e itself. For given any non-negative integer x less than m, we can determine a sequence $a_0, a_1, a_2, a_3, \ldots$ of non-negative integers less than m such that $a_0 = x$ and $a_{i+1} \equiv a_i^2 \pmod{m}$ for each non-negative integer i. Then $a_i \equiv x^{2^i}$ for all non-negative integers i. Any positive integer e may then be expressed in the form

$$e = e_0 + 2e_1 + 2^2 e_2 + 2^3 e_3 + \cdots$$

where e_i has the value 0 or 1 for each non-negative integer i. (These numbers e_i are of course the digits in the binary representation of the number e.)

Then x^e is then congruent to the product of those integers a_i for which $e_k = i$. The execution time required to calculate $E(x)$ by this method is therefore determined by the number of digits in the binary expansion of e, and is therefore bounded above by some constant multiple of $\log m$ (assuming that e has been chosen so that it is less than s, and thus less than m).

Moreover the execution time required by the Euclidean algorithm, when applied to natural numbers that are less than m is also bounded above by some constant multiple of $\log m$. For in order to apply the Euclidean algorithm, one is required to calculate a decreasing sequence $r_0, r_1, r_2, r_3, \ldots$ such that, for $k \leq 2$, the non-negative integer r_k is the remainder obtained on dividing r_{k-2} by r_{k-1} in integer arithmetic, and therefore satisfies the inequality $r_k \leq \frac{1}{2} r_{k-2}$. (To see this, consider separately what happens in the two cases when $r_{k-1} \leq \frac{1}{2} r_{k-2}$ and $r_{k-1} > \frac{1}{2} r_{k-2}$.)