MAT 3343, APPLIED ALGEBRA, FALL 2003

Handout 3: The RSA Cryptosystem

Peter Selinger

1 Background

1.1 The group of units

Let $(R, +, \cdot)$ be a ring. Then R forms an abelian group under addition. R does not in general form a group under multiplication, because not every element has a multiplicative inverse. However, we obtain a multiplicative group if we restrict attention to the *invertible* elements. For a ring R, we define R^* to be the set of invertible elements, i.e.,

$$R^* = \{a \in R \mid \exists a' \in R \,.\, aa' = 1 = a'a\}.$$

An invertible element in a ring is also called a *unit* of the ring; thus, R^* is called the *group of units* of R.

Lemma 1.1. *R^* is a group under multiplication.*

Proof. First, we need to show that multiplication is well-defined on R^*. Let $a, b \in R^*$. Then $ab \in R$. We must show that ab is invertible. Since $a, b \in R^*$, there exist $a', b' \in R$ such that $aa' = 1 = a'a$ and $bb' = 1 = b'b$. Then $abb'a' = a1a' = aa' = 1$ and $b'a'ab = b'1b = b'b = 1$, hence ab is invertible, thus $ab \in R^*$.

Next, we need to show that R^* satisfies the group axioms. The fact that multiplication is associative with unit 1 follows from the fact that this is true in R (note that $1 \in R^*$). Finally, if $a \in R^*$, then $aa' = 1 = a'a$ for some $a' \in R$; but this implies that $a' \in R^*$, thus every $a \in R^*$ has an inverse in R^*. □

Examples. The only invertible element in $\mathbb{Z}$ are 1 and -1; thus $\mathbb{Z}^* = \{-1, 1\}$. In $\mathbb{Q}$, all elements except 0 are invertible, thus $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. Similarly, $\mathbb{R}^* = \mathbb{R} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$. In $\mathbb{Z}_5$, there are four invertible elements, namely $\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. In $\mathbb{Z}_6$, only $\bar{1}$ and $\bar{5}$ are invertible, so $\mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$.

More generally, recall that $\bar{a}$ is invertible in $\mathbb{Z}_n$ if and only if a and n are relatively prime (Theorem 5, p.54). Thus, the elements of $\mathbb{Z}_n^*$ are in one-to-one correspondence with the numbers in $\{1, \ldots, n-1\}$ which are relatively prime to n.

Definition (Euler's φ function). Euler's φ function is defined as follows: $\varphi(n)$ is the number of invertible elements in $\mathbb{Z}_n$, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$. Equivalently, $\varphi(n)$ is the number of integers in $\{1, \ldots, n-1\}$ which are relatively prime to n.

Remark. Let $n > 0$. Then n is prime if and only if $\varphi(n) = n - 1$. Because: if n is prime, then all numbers in the set $\{1, \ldots, n-1\}$ are relatively prime to n, thus $\varphi(n) = n - 1$. On the other hand, if n is not prime, then $a|n$ for some $1 < a < n$. Thus, $a \in \{1, \ldots, n-1\}$ is not relatively prime to n, and $\varphi(n) < n - 1$.

Lemma 1.2. *(1) If p is prime, then $\varphi(p) = p - 1$.*

(2) If $p \neq q$ are two primes, then $\varphi(pq) = (p-1)(q-1)$.

Proof. (1) See the previous remark. (2) Let $n = pq$, and let us count the numbers in $\{1, \ldots, n-1\}$ which are *not* relatively prime to n. These numbers are: the multiples of p (there are $q - 1$ of them), and the multiples of q (there are $p - 1$ of them). Thus, the total number of integers in $\{1, \ldots, n-1\}$ which are not relatively prime to n is $p + q - 2$. The remaining numbers are relatively prime; there are $n - 1 - (p + q - 2) = pq - p - q + 1 = (p-1)(q-1)$ such numbers. □

Next, we recall some important facts from group theory.

Lemma 1.3. *Let G be a finite group. Then*

(1) If H is a subgroup of G, then $|H|$ divides $|G|$.

(2) If $x \in G$ is any element, then $H = \{x^i \mid i \in \mathbb{Z}\}$ is a subgroup of G.

(3) If $|G| = n$ and $x \in G$, then $x^n = 1$.

Proof. From group theory. (1) is proved by showing that the cosets aH form a partition of G. (2) It is clear that H is closed under multiplication and inverses. (3) Let H be as in (2). Since G is finite, H must be finite, so $x^i = x^j$ for some $i < j$. Dividing by i, we find that $1 = x^{j-i}$. Let k be smallest such that $x^k = 1$. Then $H = \{1, \ldots, x^{k-1}\}$ has exactly k elements. By (1), $k|n$. It follows that $x^n = 1$. □

Lemma 1.4 (Fermat's Little Theorem). *If $p, x \in \mathbb{Z}$, p is prime, and $p \nmid x$, then*

$$x^{p-1} \equiv 1 \pmod{p}.$$

Proof. By Lemma 1.2(1), $|\mathbb{Z}_p^*| = p - 1$. By Lemma 1.3(3), $x^{p-1} = 1$ in $\mathbb{Z}_p$. □

Lemma 1.5 (Fermat's Little Theorem generalized). *If $n, x \in \mathbb{Z}$ and n, x are relatively prime, then*
$$x^{\varphi(n)} \equiv 1 (\operatorname{mod} n).$$

Proof. This follows directly from Lemma 1.3(3), applied to $\mathbb{Z}_n^*$. ☐

1.2 The Chinese Remainder Theorem

Theorem 1.6 (Chinese Remainder Theorem). *Let n_1, n_2 be integers such that $\gcd(n_1, n_2) = 1$, and let $n = n_1 n_2$. Given integers a_1, a_2, there exists a unique $a \in \mathbb{Z}_n$ such that $a \equiv a_1 (\operatorname{mod} n_1)$ and $a \equiv a_2 (\operatorname{mod} n_2)$.*

Proof. Consider the function $f : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ defined by
$$f([a]_n) = \langle [a]_{n_1}, [a]_{n_2} \rangle.$$

Since $n_1, n_2 | n$, this is a well-defined function. We show that f is one-to-one: suppose $f([a]_n) = f([b]_n)$. Then $[a]_{n_i} = [b]_{n_i}$, thus $n_i | (a - b)$ for $i = 1, 2$. Since n_1, n_2 are relatively prime, it follows that $n_1 n_2 | (a - b)$ by Theorem 5(1), p.41. Thus $a \equiv b (\operatorname{mod} n)$, hence $[a]_n = [b]_n$. Therefore, f is one-to-one. But f is a function between finite sets of equal cardinality, and therefore if it is one-to-one, it is also onto. It follows that for any $\langle a_1, a_2 \rangle \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, there exists a unique $a \in \mathbb{Z}_n$ with $f(a) = \langle a_1, a_2 \rangle$. This is equivalent to the claim. ☐

Exercise 1.1. As a matter of fact, there is a more general version of the Chinese Remainder Theorem, using integers $n_1, \ldots, n_k$, pairwise relatively prime, and $a_1, \ldots, a_k$. State and prove this more general version.

Corollary 1.7. *Let $p \neq q$ be two different primes, and let $x \in \mathbb{Z}$. If $x \equiv 1 (\operatorname{mod} p)$ and $x \equiv 1 (\operatorname{mod} q)$, then $x \equiv 1 (\operatorname{mod} pq)$.*

Proof. By the Chinese Remainder Theorem, there exists a unique number x in $\mathbb{Z}_{pq}$ such that $x \equiv 1 (\operatorname{mod} p)$ and $x \equiv 1 (\operatorname{mod} q)$. Since 1 is such a number, it follows that $x = 1$ in $\mathbb{Z}_{pq}$. ☐

1.3 Square roots of unity

A *square root of unity* in a ring R is an element $b \in R$ such that $b^2 = 1$.

Lemma 1.8. *(1) If p is an odd prime, then there are exactly two roots of unity in $\mathbb{Z}_p$, namely $b = \pm 1$.*

(2) If p, q are two different odd primes, then there are exactly four roots of unity in $\mathbb{Z}_{pq}$, namely $b = \pm 1$, and $b = \pm x$, where x is the unique element such that $x \equiv 1 (\operatorname{mod} p)$ and $x \equiv -1 (\operatorname{mod} q)$.

Proof. (1) Suppose that b is a square root of unity in $\mathbb{Z}_p$. Then $b^2 \equiv 1 (\operatorname{mod} p)$, or equivalently, $b^2 - 1 \equiv 0 (\operatorname{mod} p)$. But $b^2 - 1 = (b - 1)(b + 1)$, thus it follows that $p | (b - 1)(b + 1)$. By Theorem 6(1), p.41, we have $p | b - 1$ or $p | b + 1$, thus $b \equiv \pm 1 (\operatorname{mod} p)$.

(2) Let $b \in \mathbb{Z}$. Then $b^2 \equiv 1 (\operatorname{mod} pq)$ iff $b^2 \equiv 1 (\operatorname{mod} p)$ and $b^2 \equiv 1 (\operatorname{mod} q)$ by Corollary 1.7. Thus, b is a square root of unity in $\mathbb{Z}_{pq}$ iff it is a square root of unity in $\mathbb{Z}_p$ and in $\mathbb{Z}_q$. Using (1) and the Chinese Remainder Theorem, this leaves the following four possibilities:

$$\begin{array}{llll}
b \equiv +1 (\operatorname{mod} p) & \text{and} & b \equiv +1 (\operatorname{mod} q), & \text{or} \\
b \equiv +1 (\operatorname{mod} p) & \text{and} & b \equiv -1 (\operatorname{mod} q), & \text{or} \\
b \equiv -1 (\operatorname{mod} p) & \text{and} & b \equiv +1 (\operatorname{mod} q), & \text{or} \\
b \equiv -1 (\operatorname{mod} p) & \text{and} & b \equiv -1 (\operatorname{mod} q), & \text{or}
\end{array}$$

☐

2 Public key cryptography

The idea of public key cryptography was first (publicly) introduced in 1976 by Diffie and Hellman. The idea is to work with two separate keys e and d. The key e is used for encryption, and the key d is used for decryption. A person who wishes to receive encrypted messages generates a pair of keys (e, d), publishes e (the "public key") and keeps d secret (the "private key"). Therefore, everybody who wishes to do so may use e to encrypt a message, but only the authorized recipient who has the key d is able to decrypt the message.

For this scheme to be secure, it needs to be designed in such a way that the secret key d cannot easily be computed from the public key e. The encryption function must be a "one-way function", which is a function that is easily computable, and also invertible, but whose inverse is not easy to compute. It is not known whether such functions exist; however, there are some functions which are *believed* to have this property.

Several mathematical schemes have been proposed for implementing public key cryptography. The best-known (and most widely used) is the RSA cryptosystem, developed by Rivest, Shamir, and Adleman in 1978. Its security rests on the fact that it is difficult to factor large numbers into primes. Another system, the ElGamal cipher, was proposed in 1985 by ElGamal. Its security rests on the difficulty of computing *discrete logarithms*. This means, given numbers x, y and a prime p, it is difficult to compute an exponent e such that $x^e \equiv y (\bmod p)$. A third system that has been proposed early in 1978, the so-called Knapsack cipher by Merkle and Hellman, was later found to be insecure ("cracked").

There are a number of other systems that have been proposed over the years. McEliece proposed a cipher in 1978 based on algebraic coding theory. More recently, a class of ciphers has been proposed which is based on hard problems in the theory of elliptic curves.

3 The RSA cryptosystem

3.1 Description of the cipher

To generate a key pair, do the following: let p and q be two different, large primes chosen at random (typically p and q will have 500 binary digits each). Let $N = pq$. Recall that $\varphi(N) = (p-1)(q-1)$ from Lemma 1.2. Let e be a randomly chosen number with $1 < e < N$, and compute d such that $ed \equiv 1 (\bmod \varphi(N))$ (this amounts to finding the inverse of e in $\mathbb{Z}_{\varphi(N)}$, which can be done efficiently by Euclid's algorithm. In the unlikely event that e has no inverse, just pick a different e at random).

The public key is the pair (N, e).

The private key is the pair (N, d).

The number N is called the *modulus*, and it is public. The primes p and q must be kept secret, or else it is possible to compute $\varphi(N)$, and thus d, from (N, e).

A *message* is an element $M \in \mathbb{Z}_N$. To encrypt M, compute

$$C \equiv M^e (\bmod N).$$

The encrypted message C is also called the *ciphertext*, and the original message M is called the *plaintext*. Note that, to perform the encryption, one only needs to know (N, e), and of course, the message M.

To decrypt a ciphertext C, compute

$$M' \equiv C^d (\bmod N).$$

3.2 Correctness

Theorem 3.1. *The decrypted message M' is the same as the original message $M \in \mathbb{Z}_N$.*

Proof. We have

$$M' \equiv C^d \equiv M^{ed} (\bmod N).$$

Thus, we need to show $M^{ed} \equiv M (\bmod N)$. We first prove that $M^{ed} \equiv M (\bmod p)$. First, in case $p|M$, this is trivial. In case $p \nmid M$, we have $M^{p-1} \equiv 1 (\bmod p)$ by Fermat's Little Theorem. But $(p-1)|\varphi(N)|(ed-1)$, so $M^{ed-1} \equiv 1 (\bmod p)$, hence $M^{ed} \equiv M (\bmod p)$ as desired. By a similar argument, $M^{ed} \equiv M (\bmod q)$. Finally, by Corollary 1.7, $M^{ed} \equiv M (\bmod pq)$. □

3.3 Feasibility

The operation of the RSA cipher rests on the fact that the following problems are computationally easy to solve:

1. exponentiation modulo N, i.e., calculating x^e in $\mathbb{Z}_N$, for large N, x, and e,
2. finding large prime numbers.

The second problem will be the subject of the next lecture. For the first problem, note that the naive algorithm for calculating x^e, namely multiplying x by itself e times, is not feasible when e is very large. Instead, we use the following *method of repeated squaring*: Suppose $e = 2^{a_0} + 2^{a_1} + \ldots, 2^{a_m}$, where $a_0 < a_1 < \ldots < a_m$. Such a representation of e can always be found by looking at the binary expansion of e. Then

$$x^e = x^{2^{a_0}} \cdot x^{2^{a_1}} \cdots x^{2^{a_m}}.$$

The individual factors $x^{2^{a_i}}$ can be found by repeated squaring, i.e., by computing the sequence x, x^2, x^4, x^{16} and so forth in $\mathbb{Z}_N$, each member being the square of the previous one. What is the computational cost of computing x^e in this way? Assuming that $N \approx 2^{1000}$, then we have $m \leqslant a_m \leqslant 1000$, thus the calculation of x^e involves computing at most 1000 squares and at most 1000 multiplications modulo N, or a total of 2000 multiplications. On a modern computer, this can be computed very fast.

3.4 Security

The security of the RSA cryptosystem has not been proven for sure; it rests on the assumption that certain mathematical problems are computationally difficult to solve. The particular problem in question is the problem of factoring the number N into the two primes p, q.

We note the following: As $\langle N, e\rangle$ is the public key, the number N will be publicly known. If the factors p, q were also known, then one could easily compute $\varphi(N) = (p-1)(q-1)$, and thus one could compute d from the given information by using the algorithm for finding inverses in $\mathbb{Z}_N$. Thus, the cipher would be broken. It follows that the RSA cipher is only secure as long as an attacker cannot efficiently find the prime factors of N.

In a certain sense, a converse to this statement also holds. Given N and e, knowing d is at least as hard as knowing p, q, as shown by the following theorem:

Theorem 3.2. *Given N, e, and d as above, one can efficiently find p and q.*

Proof. It is known that $N = pq$ for some unknown primes p and q. It is also known that $ed \equiv 1 (\operatorname{mod} \varphi(N))$, where $\varphi(N) = (p-1)(q-1)$. Compute $k = ed - 1$. Then $\varphi(N)|k$. Because $\varphi(N)$ is even, we have $k = 2^t r$ for some odd r and $t \geqslant 1$. Then for all $g \in \mathbb{Z}_N^*$, we have $g^k = \bar{1}$. It follows that $g^{k/2}$ is a square root of unity in $\mathbb{Z}_N$. By Lemma 1.8(2), $\bar{1}$ has exactly four square roots in $\mathbb{Z}_N$, of which two are ± 1. The other two are $\pm x$, where $x \equiv 1 (\operatorname{mod} p)$ and $x \equiv -1 (\operatorname{mod} q)$. Using either one of these roots, compute $\gcd(x-1, N)$. Since either $p|x-1$ or $q|x-1$ (but not both), this gcd reveals either p or q.

If g is chosen at random from $\mathbb{Z}_N^*$, then with probability at least $1/2$, one of the elements in $g^{k/2}, g^{k/4}, \ldots, g^{k/2^t}$ is a square root of unity which reveals the factorization of N. Thus, the factorization of N can be found by repeatedly choosing g at random.

The last claim about probabilities can be seen as follows. Let s be the smallest integer such that there exists some $g \in \mathbb{Z}_N^*$ with $g^{k/2^s} \neq 1$. Note that since $k/2^t$ is odd, we always have $(-1)^{k/2^t} \neq 1$ in $\mathbb{Z}_N^*$, thus, such an integer s always exists. Now let $G = \{g \in \mathbb{Z}_N^* \mid g^{k/2^s} = \pm 1\}$. Then G is a subgroup of $\mathbb{Z}_N^*$. We show that $G \neq \mathbb{Z}_N^*$: by definition of s, there exists some $g \in \mathbb{Z}_N^*$ such that $g^{k/2^s} \neq 1$. Then either $g^{k/2^s} \neq -1$, in which case $g \notin G$, or else, $g^{k/2^s} = -1$. In this latter case, by the Chinese Remainder Theorem, there exists some $g' \in \mathbb{Z}_N^*$ such that $g' \equiv g (\operatorname{mod} p)$ and $g' \equiv 1 (\operatorname{mod} q)$. This implies $(g')^{k/2^s} \equiv -1 (\operatorname{mod} p)$ and $(g')^{k/2^s} \equiv 1 (\operatorname{mod} q)$, thus $(g')^{k/2^s} \not\equiv \pm 1 (\operatorname{mod} N)$. It follows that $g' \notin G$. So in either case, G is a proper subgroup of $\mathbb{Z}_N^*$. By Lemma 1.3(1), it follows that $|G|$ divides $\mathbb{Z}_N^*$, thus $|G| \leqslant \frac{1}{2}|\mathbb{Z}_N^*|$. It follows that if we pick a random element $g \in \mathbb{Z}_N^*$, then $g \notin G$ with probability at least $1/2$, and in this case, $g^{k/2^s}$ will be a root of unity other than ± 1. □

Remark. The above argument shows that computing d is at least as difficult as factoring N, if N and e are given, and N is the product of two primes. As factoring is assumed to be difficult, this provides some circumstantial evidence about the security of RSA.

It is important to note, however, that this does not provide conclusive proof of the security of RSA, even if one takes for granted that factoring is difficult. First, it might be possible to break the RSA cryptosystem without first computing d. Second, even if factoring is difficult in general, it is possible that it is easier in special cases, for instance, if N is known to be a product of exactly two primes. Third, even if the RSA cryptosystem is secure in the general case, there might be some special cases, such as badly chosen parameters, for which the system is insecure. There are in fact several known weaknesses of RSA of this latter kind. We will discuss them in the next section.

3.5 Known weaknesses of RSA, and how to avoid them

While the RSA cryptosystem is believed to be secure in the general case, there are several known attacks which work in special cases, i.e., for certain badly chosen parameters N, e, and/or d. When implementing the RSA cryptosystem in practice, it is therefore necessary to be acquainted with these well-known exploits and to avoid them. In other words, **RSA is not secure unless it is properly implemented**.

Common modulus. Since finding large prime numbers can be time-consuming, it is tempting to fix p and q once and for all, and to re-use the same modulus N, only changing e and d when generating new key pairs. This, however, is not secure. If a user knows one such pair $\langle e, d\rangle$, this is enough to recover p and q, and thus to find the private keys to all public keys using the same modulus.

Badly chosen parameters. In order for RSA to be secure, one should chose p, q such that $p, q \equiv 3 (\bmod 4)$. Otherwise, there is a known attack.

The numbers p, q must be chosen so that $p - 1$ and $q - 1$ must not have odd small prime factors (note that if p is chosen at random, it is quite likely that $p - 1$ has a small odd prime factor; such situations give rise to an attack and are to be avoided).

The private key d must not be chosen too small. It should be at least $\frac{1}{3}N^{1/4}$, or else there is a known attack.

The public key e must be at least 65537.

Blinding attacks. So-called *blinding attacks* are based on the idea that an attacker might attempt to decrypt a message by fooling the legitimate holder of the secret key into decrypting it without that person's knowledge. Suppose that Bob has generated a public/private key pair e, d with some modulus N. Suppose Alice wants to fool Bob into decrypting some ciphertext C, where $C \equiv M^e (\bmod N)$, and C, but not M, is known to Alice. She can pick a random number $r \in \mathbb{Z}_N^*$ and compute $C' \equiv r^e C$. She can then ask Bob to decrypt C'. Bob will compute $M' \equiv (C')^d \equiv (r^e C)^d \equiv r^{ed} C^d \equiv rM (\bmod N)$. Since the number r is random, the message M' will appear as a meaningless string of random data to Bob. Bob may foolishly decide to let Alice have this apparently worthless data. But now Alice can use M' to compute the real original message M: namely, she computes $r^{-1}M' \equiv r^{-1}rM \equiv M (\bmod N)$.

Blinding attacks are possible because of algebraic properties of the RSA cryptosystem, namely the property that multiplication of plaintexts corresponds to multiplication of ciphertexts.

Further Reading

The above list of known weaknesses of the RSA cryptosystem is incomplete. Because from time to time, additional potential attacks are discovered, it is important that real-life implementations of RSA are done by experts who are familiar with these weaknesses and who know how to avoid them. More information on known attacks on the RSA cryptosystem can be found in the following article:

Dan Boneh, *Twenty years of attacks on the RSA cryptosystem*. In Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203–213, 1999. Also available from http://crypto.stanford.edu/~dabo/abstracts/RSAattack-survey.html