The RSA Public-Key Cryptosystem

Andreas Klappenecker
CPSC 629 Analysis of Algorithms

We will discuss in this lecture the basic principles of the RSA public-key cryptosystem, a system that is used in countless e-commerce applications. The RSA public-key cryptosystem nicely illustrates the number-theoretic principles that we have learned so far. Furthermore, the basic algorithm used in RSA will motivate us to study several other fundamental algorithms.

Basic Principles. Suppose that Alice seeks a way that people can send her confidential messages by e-mail. The RSA cryptosystem allows her to publish a key that everyone can use to send her an encrypted message, but that is hard to decipher without a secret that is only known to her.

Key Generation:

- Alice selects two distinct large prime numbers p and q, and computes their product $n = pq$.
- She selects an odd integer $e > 0$ such that $\gcd(e, (p-1)(q-1)) = 1$, and computes positive integers d and k such that $ed - k(p-1)(q-1) = 1$.
- Alice publishes the pair $P = (e, n)$, her public key. She carefully guards as a secret the factorization of n, the product $(p-1)(q-1)$, the integer k, and her secret key $S = (d, n)$.

Encryption and Decryption:

- For simplicity, we assume that a message is encoded as an integer M in the range $2 \leq M < n$.
- If Bob wants to send a message M to Alice then he looks up Alice's public key and sends her the number

$$\boxed{C = M^e \bmod n}$$

- Alice uses her secret key to compute

$$\boxed{C^d = M^{ed} \bmod n}$$

  It turns out that $M^{ed} \equiv M \bmod n$, so she recovers Bob's message.

Remark. In the key generation phase, Alice is faced with the problem to calculate *positive integers* d and k such that $ed - k(p-1)(q-1) = 1$. Since $\gcd(e, (p-1)(q-1)) = 1$, she can use the extended Euclidean algorithm to find integers x and y such that $ex + y(p-1)(q-1) = 1$. By adding $0 = \ell e(p-1)(q-1) - \ell e(p-1)(q-1)$ to the left hand side, she obtains

$$e(x + \ell(p-1)(q-1)) + (y - e\ell)(p-1)(q-1) = 1.$$

If she chooses ℓ such that $d = x + \ell(p-1)(q-1) > 0$, then $-k = y - e\ell$ must be negative, so $k > 0$.

Fermat's Little Theorem. We need to prove one interesting fact about integers modulo a prime p that is enormously useful. The theorem was stated by Fermat and later formally proved by Euler.

Theorem 1 (Fermat)**.** *Let p be a prime. If a is an integer, then*

$$a^p \equiv a \bmod p.$$

Proof. The statement is certainly true if $a \equiv 0 \bmod p$. Suppose that a is not divisible by p. Recall that

$$(a_1 + \cdots + a_k)^n = \sum_{\substack{n_1, n_2, \ldots, n_k \geq 0 \\ n_1 + n_2 + \cdots + n_k = n}} \frac{n!}{n_1! n_2! \cdots n_k!} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$$

by the multinomial theorem. Therefore,

$$\begin{aligned} a^p = (\underbrace{1 + \cdots + 1}_{a \text{ times}})^p &= \textstyle\sum_{\substack{n_1, n_2, \ldots, n_a \geq 0 \\ n_1 + n_2 + \cdots + n_a = p}} \frac{p!}{n_1! n_2! \cdots n_a!} 1^{n_1} 1^{n_2} \cdots 1^{n_a} \\ &\equiv 1^p + \cdots + 1^p \equiv a \bmod p, \end{aligned}$$

because the coefficient $p!/(n_1! n_2! \cdots n_a!)$ is congruent 0 modulo the prime p unless $n_k = p$ for some k. □

Corollary 2. *Let p be a prime. If a is an integer that is not divisible by p, then*

$$a^{p-1} \equiv 1 \bmod p.$$

Proof. The hypothesis implies that $\gcd(a, p) = 1$; hence, there exist integers x and y such that $ax + py = 1$. Therefore, $ax \equiv 1 \bmod p$. It follows from $a^p \equiv a \bmod p$ that $a^{p-1} \equiv xa^p \equiv xa \equiv 1 \bmod p$ holds. □

Correctness of RSA. The correctness of the RSA algorithm follows from the following theorem.

Theorem 3. *$M^{ed} \equiv M \bmod n$ holds for all integers M.*

Proof. Recall that the integers $e > 0$ and $k > 0$ are chosen such that

$$ed = 1 + k(p-1)(q-1).$$

It suffices to show that the two congruences

$$M^{ed} \equiv M \bmod p \quad \text{and} \quad M^{ed} \equiv M \bmod q$$

hold. Indeed, p and q are distinct primes, so $\gcd(p, q) = 1$, and the above congruences imply $M^{ed} \equiv M \bmod n$ by the Chinese Remainder Theorem.

If $M \equiv 0 \bmod p$, then certainly $M^{ed} \equiv M \bmod p$. If $M \not\equiv 0 \bmod p$, then $M^{p-1} \equiv 1 \bmod p$ by Corollary 2; hence,

$$M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv M(M^{p-1})^{k(q-1)} \equiv M\,1^{k(q-1)} \equiv M \bmod p.$$

Therefore, $M^{ed} \equiv M \bmod p$ holds *for all* integers M. Replacing p by q in the previous argument shows that $M^{ed} \equiv M \bmod q$ for all integers M. $\square$