

# The RSA Public-Key Cryptosystem

Andreas Klappenecker

CPSC 411

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 basic number-theoretic principles. Furthermore, the basic algorithm used in RSA will motivate us to study several other fundamental number-theoretic algorithms.

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.

We need some notation before stating the protocol. Euler's **totient function**  $\varphi: \mathbf{N} \rightarrow \mathbf{N}$  is defined as

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product ranges over all primes dividing  $n$ . If  $n = pq$  is the product of two distinct primes  $p$  and  $q$ , then  $\varphi(n) = (p-1)(q-1)$ .

## 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  $\gcd(e, \varphi(n)) = 1$ , and computes positive integers  $d$  and  $k$  such that  $ed - k\varphi(n) = 1$ .
- Alice publishes the pair  $P = (e, n)$ , her public key. She carefully guards as a secret the factorization of  $n$ , the product  $\varphi(n) = (p-1)(q-1)$ , 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

$$C \equiv M^e \pmod{n}.$$

- Alice uses her secret key to compute

$$C^d \equiv M^{ed} \pmod{n}.$$

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

**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*

$$a^p \equiv a \pmod{p}.$$

*Proof.* The assertion holds for  $a = 0$  and  $a = 1$ . Assuming that the assertion is true for  $a$ , then, by induction,  $(a + 1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ . Therefore, the assertion holds for every natural number. If  $p = 2$ , then the assertion holds for all integers. If  $p$  is odd and  $a^p \equiv a \pmod{p}$  holds, then  $(-a)^p \equiv -a^p \equiv -a \pmod{p}$ . Therefore, the theorem holds for all integers.  $\square$

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

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

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

**The Chinese Remainder Theorem.** The second ingredient that we need in our correctness proof of the RSA protocol is a statement about the simultaneous solvability of congruences.

**Theorem 3 (Chinese Remainder Theorem).** *Let  $q$  and  $p$  be positive integers such that  $\gcd(q, p) = 1$ . For given integers  $x$  and  $y$  there exists an integer  $a$  such that*

$$\begin{aligned} a &\equiv x \pmod{p}, \\ a &\equiv y \pmod{q}. \end{aligned}$$

*If  $a'$  satisfies  $a' \equiv x \pmod{p}$  and  $a' \equiv y \pmod{q}$ , then  $a \equiv a' \pmod{pq}$ .*

*Proof.* Since  $\gcd(p, q) = 1$ , there exist integers  $p'$  and  $q'$  such that

$$\gcd(q, p) = 1 = pp' + qq'.$$

In particular, we have  $qq' \equiv 1 \pmod{p}$  and  $pp' \equiv 1 \pmod{q}$ . Therefore, the integer  $a = ypp' + xqq'$  satisfies

$$a \equiv xqq' \equiv x \pmod{p} \text{ and } a \equiv ypp' \equiv y \pmod{q}.$$

Since  $a \equiv a' \pmod{p}$ , we have  $a - a' = kp$  for some integer  $k$ . However,  $a - a'$  is divisible by  $q$  as well, hence  $kp$  is divisible by  $q$ . As  $\gcd(p, q) = 1$ , it follows that  $q$  must divide  $k$ . Therefore,  $a - a'$  is divisible by  $pq$ , so  $a \equiv a' \pmod{pq}$ , as claimed.  $\square$

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

**Theorem 4.** *Let  $n = pq$  be a product of two distinct primes  $p$  and  $q$ . Let  $e$ ,  $d$ , and  $k$  be positive integers satisfying  $ed = 1 + k\varphi(n)$ . Then*

$$M^{ed} \equiv M \pmod{n}$$

*holds for all integers  $M$ .*

*Proof.* It suffices to show that the two congruences

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

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

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

$$M^{ed} \equiv M^{1+k\varphi(n)} \equiv M(M^{p-1})^{k(q-1)} \equiv M 1^{k(q-1)} \equiv M \pmod{p}.$$

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