TD2 :: Number theory and the RSA scheme

Université Sorbonne Paris Nord, M1. Sergey Dovgal
dovgal@lipn.fr

1 Prerequisites

1.1 Generalised Euclid's algorithm

Exercise 1. Using Euclid's algorithm, compute

1. $gcd(1071, 462)$
2. $gcd(2020, 2017)$

Hint. Use the fact that $gcd(x, y) = gcd(x - y, y)$.

Exercise 2. Find integers x and y such that

1. $1071x - 462y = 1$
2. $2020x - 2017y = 1$
3. $2020x - 2017y = 5$

Hint. On the last step of Euclid's algorithm for coprime numbers you obtain $gcd(n, 1) = 1$. This corresponds to the case $a = n$, $b = 1$ with a solution $x = 0, y = 1$. On each step of Euclid's algorithm $gcd(a, b) = gcd(a - b, b)$ the solution for $\widehat{a} = a - b$ and $\widehat{b} = b$ can be converted into the solution for a and b. Proceed with Euclid's algorithm backwards.

1.2 Euler's totient function

Definition. $\phi(n)$ is equal to the number of positive integers from 1 to n that are relatively prime to n.

Exercise 3. Compute $\phi(10)$ and $\phi(1997)$.

Theorem. $\phi(n)$ has the following properties

1. If p is prime then $\phi(p) = p - 1$;

2. If p is prime and $n = p^k$ then $\phi(n) = p^k - p^{k-1} = n(1 - \frac{1}{p})$;

3. If n and m are relatively prome then $\phi(nm) = \phi(n)\phi(m)$;

4. If $p_1, \ldots, p_k$ are distinct primes and $n = p_1^{r_1} \cdots p_k^{r_k}$ then

$$\phi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_k^{r_k} - p_k^{r_k-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Exercise 4. Compute $\phi(3^{2020})$, $\phi(100)$, $\phi(6^{2020})$.

Exercise 5. Compute the last digits of $3^1, 3^2, \ldots, 3^9$, then $7^1, 7^2, \ldots, 7^9$, repeat for powers of $2, 4, 5, 6, 8, 9$. Do you notice any pattern?

Euler's theorem. If a and n are relatively prime, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Exercise 6. Compute the last two digits of 1993^{2041}. How to compute high powers when a and n are not relatively prime?

Exercise.* Prove that $\sum_{d|n} \phi(d) = n$.

2 RSA ENCRYPTION SCHEME

- Pick two large prime numbers p and q. Keep these numbers secret. Compute the *modulus* $n = pq$.

- Pick a number $e \in [1, \phi(n) - 1]$ coprime with $\phi(n)$. Compute a number d such that $d \cdot e \equiv 1 \pmod{\phi(n)}$.

- A *message* is a number $m \pmod{n}$ *relatively prime to* n.

- An encrypted message is $m^e \pmod{n}$.

Exercise 7. How to decrypt the message m?

Exercise 8. Which parts of the key $\{p, q, n, e, d\}$ should be public and which should be private?

Exercise 9. Let $p = 101$, $q = 19$, and $e = 7$. Encrypt the message $m = 5$. Decrypt the message $s = 2$.

2.1 RSA DIGITAL SIGNATURE SCHEME

Use the same parameters as in the encryption scheme. Compute *the signature* $m^d \pmod{n}$. Transmit the pair $(m, m^d) \pmod{n}$.

Exercise 10. Let $p = 101$, $q = 19$, and $e = 7$. Sign the message $m = 5$.