HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

13/11/2023. Lecture 9.

1 Asymmetric encryption

In the class we rediscussed the scheme RSA, where the encryption is done with a public key (n, k), and decryption with the matching private key (n, d). (Let us recall that n is chosen as a product of two large prime numbers, $n = p \cdot q$, and k and d are chosen so that $k \cdot d = 1 \mod \phi(n)$, where $\phi(n) = (p-1) \cdot (q-1)$).

We discussed the possibility of an attack on the scheme RSA: to convert the *public key* (n, k) in the *secret key* (n, k) it is enough to factorise n, i.e., find the prime factors of the number n.

In the naive algorithm of factorisation we try all possible factors of n, i.e., all numbers between 2 and $\sqrt{n}$. If $2^{n-1} \leq n < 2^k$ (the binary expansion of n consists of k binary digits), this algorithm runs in time that is at least $\sqrt{n} = 2^{k/2}$, which is exponential in the size of the inputs. More advanced algorithms factorise n in time $2^{O(k^{1/3}(\log k)^{2/3})}$, which is much faster than the naive approach but still too slow for k that is several thousand bits in size. We do not know any poly-time algorithm (deterministic or even randomised) for the problem of integer factorisation. The scheme RSA is believed to be safe large enough k. (The usual practical recommendation is to take k of length 2K bits or greater).

2 Density of prime numbers.

A natural number $p \in \mathbb{N}$ is called prime if it has exactly to natural divisors: 1 and p. The list of prime numbers begins with

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31, 37,\ 41,\ 43,\ 47, 53,\ 59, \ldots$$

There are quite *many* prime numbers. This statement can be mode more precise in different ways:

- the set of prime numbers is infinite (demonstrated by Euclid)
- for every integer number $n > 0$, there exists a prime number p such that $a \leq p < 2p$ (this property is called Bertrand's postulate; it was proven by Chebyshev)

Denote $\pi(n)$ the prime-counting function (the number of primes less than or equal to N). Then

- there exist numbers $c_1 > 0$ and $c_2 > 0$ such that for all n

  $$c_1 \cdot \frac{n}{\ln n} < \pi(n) < c_2 \cdot \frac{n}{\ln n}$$

  (Chebyshev's bounds)

- for every $\epsilon > 0$ there exists an $n_0 = n_0(\epsilon)$ such that for all $n > n_0$

  $$(1-\epsilon)\frac{n}{\ln n} < \pi(n) < (1+\epsilon)\frac{n}{\ln n}$$

  (proven by Hadamard and de la Vallée Poussin).

In the class we used the bound proven by Hadamard and de la Vallée Poussin to deduce the following property:

Proposition 1. *There exist a $c > 0$ and a $k > 0$ such that for all integer numbers $k > k_0$ the number of primes between 2^{k-1} and 2^k is greater or equal to $c \cdot 2^k/k$.*

This proposition means that if we choose at random an integer number x with k binary digits (a number between 2^{k-1} and 2^k), then it will turn out to be prime with a probability of at least $\Omega(1/k)$. Thus, if take at random **const** $\cdot\, k$ integer numbers with k binary digits (for a large enough factor **const**), then with a probability of > 0.99 at least one of these numbers is prime.

This observation shows that we can produce large prime numbers: we pick up a random integer number and test its primality). What remains missing in this scheme is an efficient test of primality. We will discuss such a test in the next lecture.

3 Groups and subgroups

Definition 1. Let $(G, *)$ be a group with the neutral element e, and let H be a subset in G. The set H is called a *subgroup* in $(G, *)$ if

- for all $x, y \in H$ the element $x * y$ belongs to H,
- foe all $x \in H$ the element $x' \in G$ such that $x * x' = e$ also belongs to H

(in other words, H with the same operation $*$ is also a group).

Theorem 1. *Let $(G, *)$ be a finite group and let H be a subgroup of this group. Then the cardinality of H divides the cardinality of G. In particular, if $H \neq G$, then $|H| \leq |G|/2$.*

Corollary 1. *Let $(G, *)$ be a finite group and let H be a subgroup of this group. If $H \neq G$, then $|H| \leq |G|/2$.*

Sketch of the direct proof of the corollary: Let

$$H = \{h_1, h_2, \ldots, h_k\}$$

be the list of all elements of H. Let $a \in G \setminus H$ (any element of the group G that does not belong to H). We consider the list of elements

$$H' = \{a * h_1, a * h_2, \ldots, a * h_k\}.$$

All elements $a * h_i$ are pairwise distinct since the operation of multiplication by a is invertible: for every $g \in G$ there exists the unique h such that $a * h = g$ (or, equivalently, $h = a' * g$, where a' is the inverse to a).

Non of the elements $a * h_i$ belongs to H. Indeed, if $a * h_i = h_j$, then

$$a = h_i' * h_j, \text{ where } h_i' \text{ is is the inverse to } h_i,$$

which implies that $a \in H$, and we get a contradiction.

Thus, if H consists of k elements, then we can find at least k distinct elements in $G \setminus H$. This concludes the proof.

We will use the proven Corollary in the next lecture, when we prove soundness of a primality test.

Exercise 1. Prove Theorem 1.